The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

1.Alice and Bob exchange their public keys PA and PB.

2.Alice computes F(SA , PB)

3.Bob computes F(SB, PA)

4.The special property of the public key cipher system, and the choice of the function F, are such that F(SA , PB) = F(SB, PA). If this is the case then Alice and Bob now share a secret.

5.This shared secret can easily be converted by some public means into a bitstring suitable for use as, for example, a DES key.

Assume that Alice and Bob are the parties who wish to establish a shared secret, and let their public and private keys in the public key cipher system be denoted by (PA , SA) and (PB , SB) respectively.
The basic principle behind Diffie–Hellman key exchange is as follows:

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.

Principle behind DH

DH key exchange assumes first that there exists:

1.A public key cipher system that has a special property (we come to this shortly).

2.A carefully chosen, publicly known function F that takes two numbers x and y as input, and outputs a third number F(x,y) (for example, multiplication is such a function).

DH key exchange was first proposed before there were any known public key algorithms, but the idea behind it motivated the hunt for practical public key algorithms. DH key exchange is not only a useful and practical key establishment technique, but also a significant milestone in the history of modern cryptography.

The **Diffie–Hellman (DH) key exchange** technique was first defined in their seminal paper in 1976.

DH key exchange is a method of exchanging public (i.e. non-secret) information to obtain a shared secret.