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

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

Principle behind DH

DH key exchange assumes first that there exists:

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

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

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

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

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