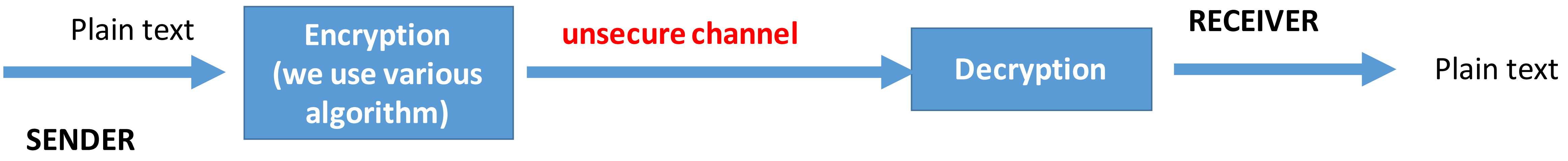
TYPES OF CRYPTOGRAPHY

1. **Symmetric key cryptography (Private/Secret Key Cryptography)**
2. **Asymmetric Key Cryptography or (Public Key Cryptography)**

Symmetric key cryptography (same key) / (Private/Secret Key Cryptography)
Symmetric key methods:DES,3DES,AES)



Plain text

SENDER

Encryption (we use various algorithm)

unsecure channel

Decryption

RECEIVER

Plain text

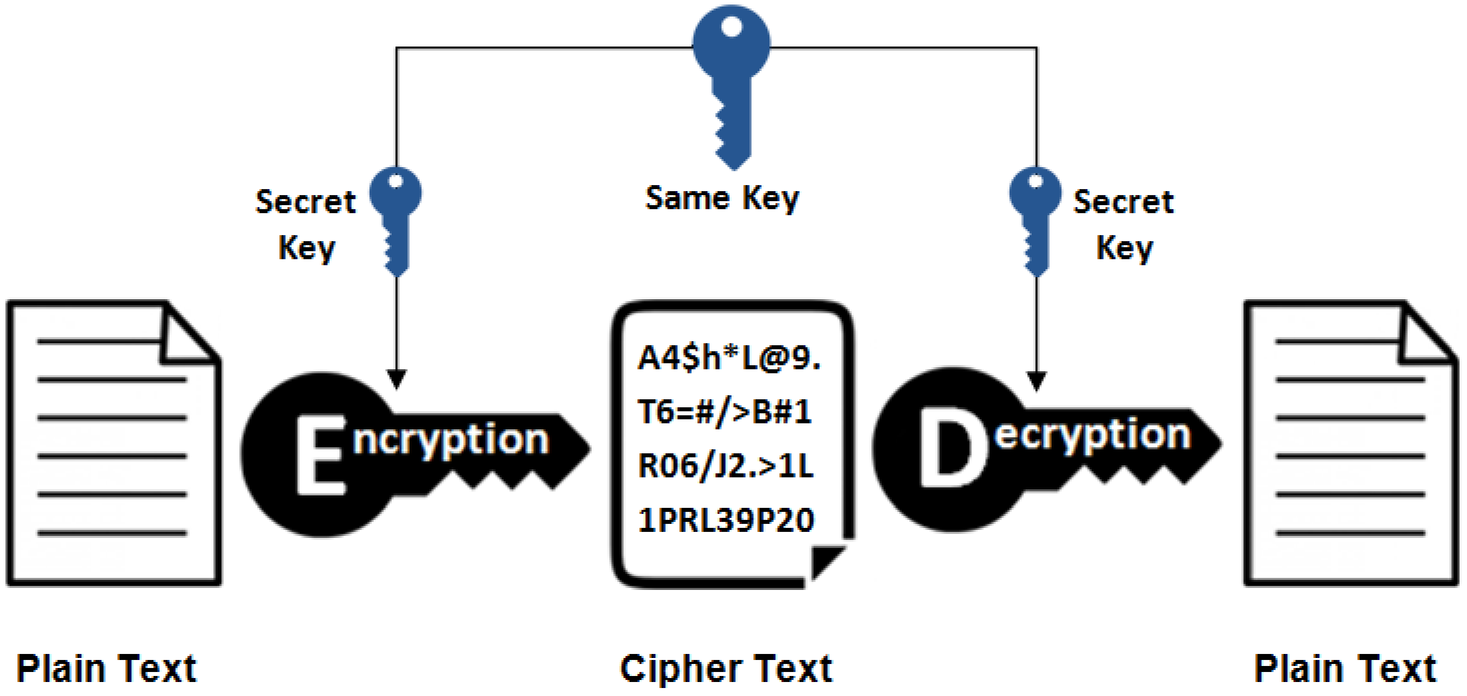
$$C=[K1[M]] \xrightarrow{\hspace{6em}} M=[K1[C]]$$

(CIPHER TEXT)

C=Cipher Text
K1=KEY
M=MESSAGE (PLAIN TEXT)

Example:

Symmetric Encryption



Symmetric Key Cryptography

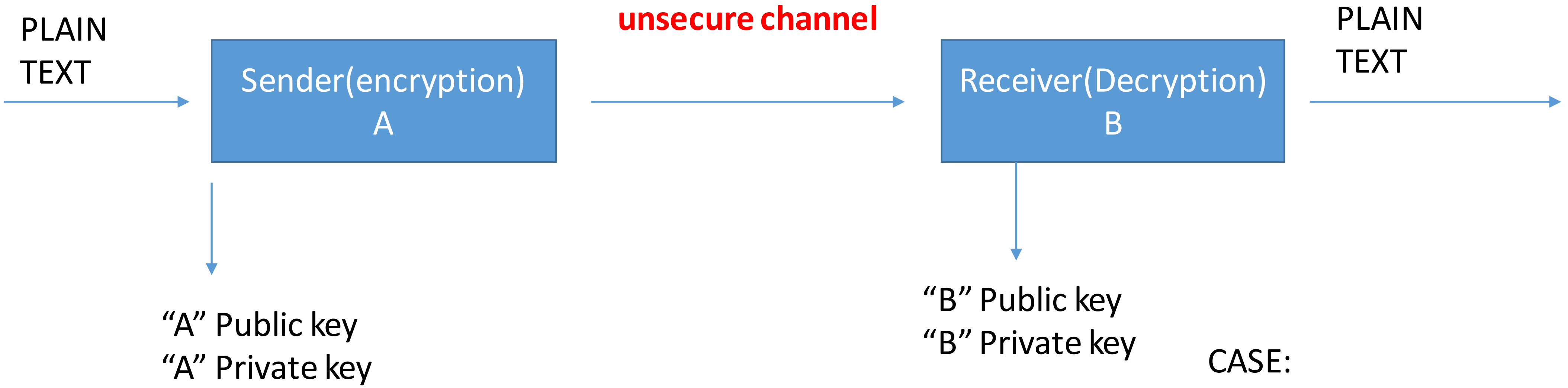
- Symmetric key cryptography is also known as **Private key** cryptography or secret key cryptography
- In symmetric key cryptography a single key is used for both encryption as well as decryption.
- **AES (Advanced Encryption System) is the most widely uses symmetric key cryptography.**

- The symmetric key system has one major drawback that the two parties must somehow exchange the key in a secure way as there is only one single key for encryption as well as decryption process.

It is represented as P=D(K,E(P))
Where K=Encryption and decryption key
P=Plain text
D=Decryption
E(P)=Encryption of plain text

Asymmetric Key Cryptography or (Public Key Cryptography)

2 KEY:
PUBLIC KEY
PRIVATE KEY



PLAIN TEXT

Sender(encryption)
A

unsecure channel

Receiver(Decryption)
B

PLAIN TEXT

“A” Public key
“A” Private key

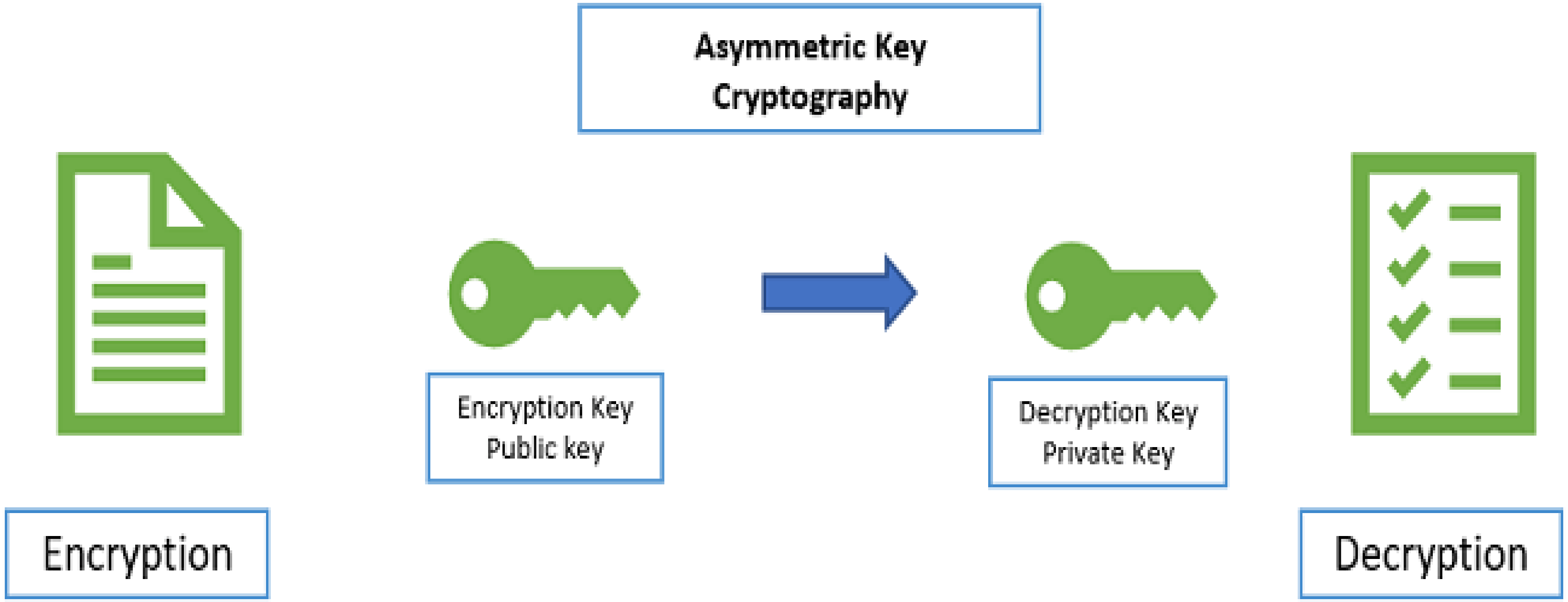
“B” Public key
“B” Private key

CASE:

1) A=E[“A” Public key[M]] send to B
2) A=E[“B” Private key[M]] send to B
3) A=E[“A” Private key[M]] send to B
(Confidentiality not achieved)
4) **A=E[“B” Public key[M]] send to B**

NOTE: Always use Receiver Public key to encrypt the message.

Example:



Asymmetric Key Cryptography

Encryption Key
Public key

Decryption Key
Private Key

Encryption

Decryption

Asymmetric Key Cryptography or (Public Key Cryptography)

- Asymmetric key cryptography is also called as public key cryptography or conventional cryptographic system.
- In asymmetric key cryptography two keys are used, our encryption and other is for decryption.
- **It is represented as:**

P=D(Kd,E(Ke,P))

Where Ke=Encryption key

Kd=Decryption key

D=Decryption

E(Ke,P)=Encryption of plain text using encryption key

P=Plain text

For Example: RSA Algorithm and Diffie Hellman key exchange algorithm.

Advantage /disadvantage of Symmetric Key Cryptography

Advantages of Private key cryptography:

a. It is faster than asymmetric key cryptography.

b. Symmetric key achieves the authentication principle, because receivers identity is checked here

c. As a common key is used for both encryption and decryption, the receiver must have the sender's key in order to decrypt the message.

d. AES and DES techniques are implemented using symmetric key cryptography

Disadvantages of Private key cryptography:

a. If the common key is stolen, then the data can be easily decrypted as same key is used for both encryption and decryption

b. In private key cryptography, the key is transmitted first and later the message is transmitted. If the attacker intercepts the initial communication between the sender and the receiver, he can intercept and decrypt the message before it reaches the intended receiver

Advantage /disadvantage of Asymmetric Key Cryptography

Advantages of Asymmetric key cryptography :

a. In Asymmetric key cryptography key cannot be distributed among sender and receiver as both have their own key so there is no problem of key distribution while transmitting the data over insecure channel.

b. The main advantage of asymmetric key cryptography is that two separate keys are used for encryption and decryption; even if encryption key is stolen by the attacker he/ she cannot decrypt the message as decryption key is only available with the receiver.

c. **RSA algorithm** and **Diffie Hellman** key exchange are implemented using asymmetric key cryptography.

Disadvantages of Asymmetric key cryptography :

a. Because of different key used between sender and receiver more time is required to get the transmission done as compared to symmetric key cryptography

b. Asymmetric key cryptography utilizes more resources as compared to symmetric Key cryptography.

Conclusion

Encryption of data is much needed in our modern time and the latest schemes may necessarily be the best fit. There are the latest algorithms and techniques being developed as hackers and eavesdroppers have made it tough to secure data to the best possible way. Cryptography is going to enhance more methods in the coming years to make personal data more secure and it’s standards more reliable.