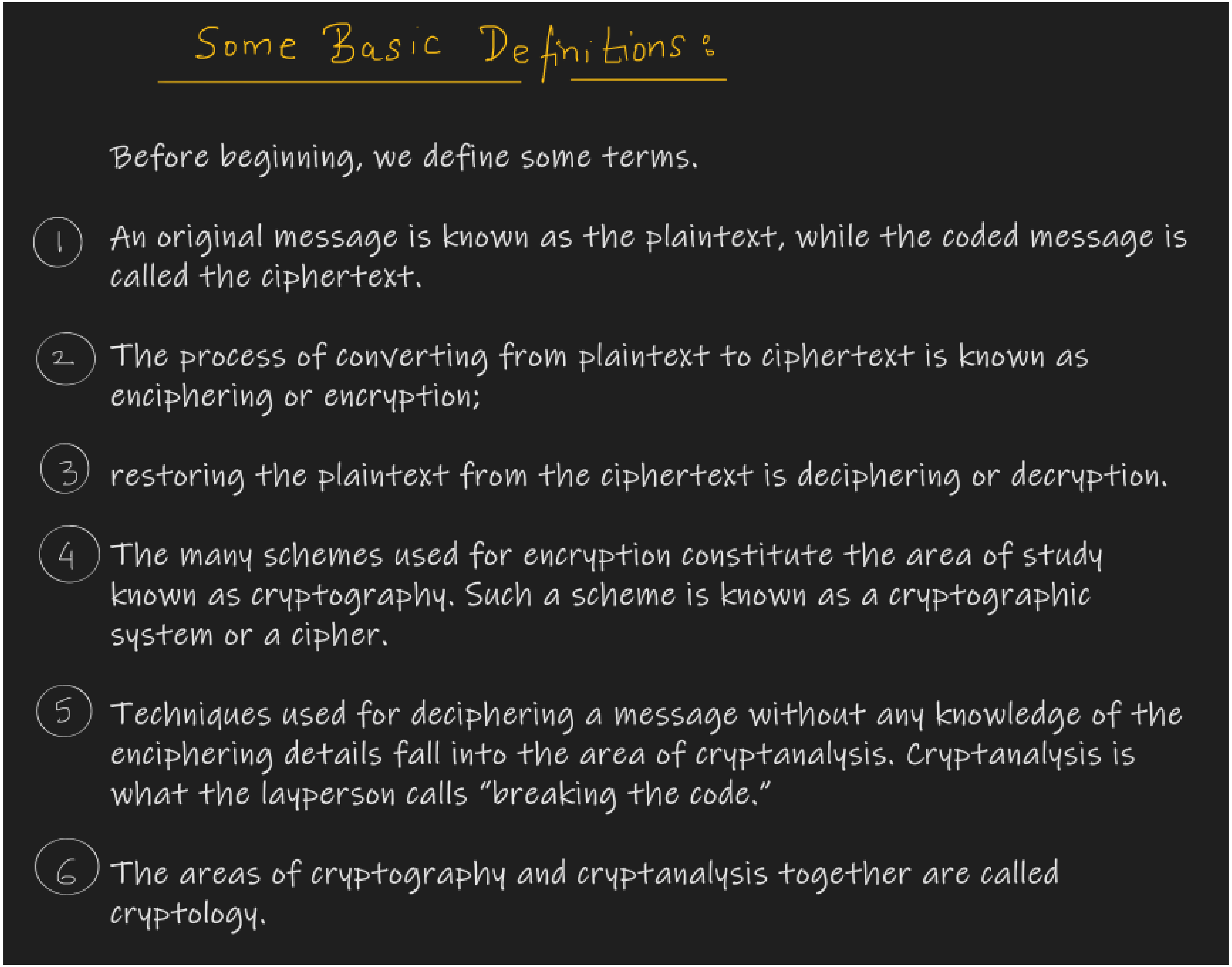
## Symmetric Cipher Model



### Some Basic Definitions :

Before beginning, we define some terms.

1. An original message is known as the plaintext, while the coded message is called the ciphertext.

2. The process of converting from plaintext to ciphertext is known as enciphering or encryption;

3. restoring the plaintext from the ciphertext is deciphering or decryption.

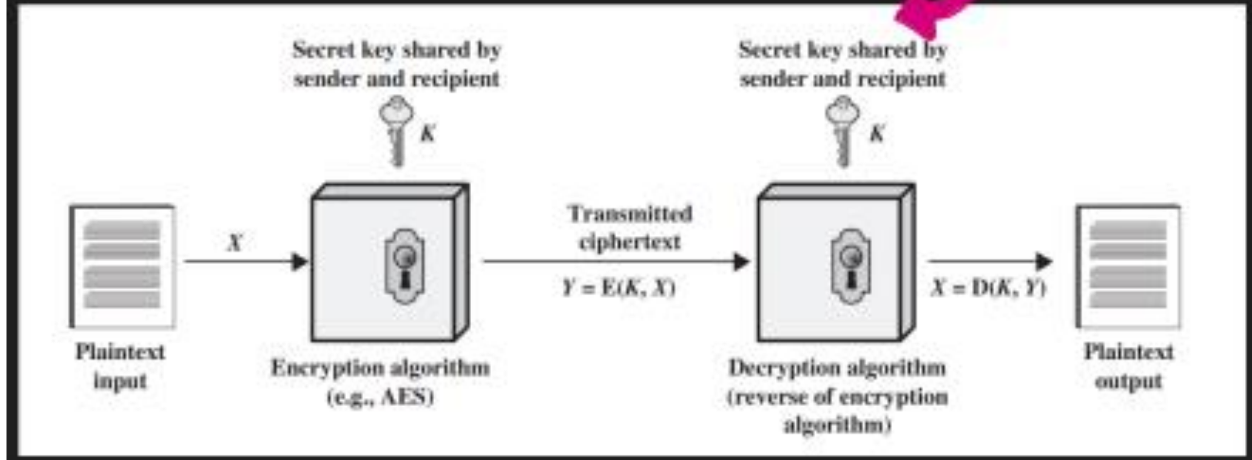
4. The many schemes used for encryption constitute the area of study known as cryptography. Such a scheme is known as a cryptographic system or a cipher.

5. Techniques used for deciphering a message without any knowledge of the enciphering details fall into the area of cryptanalysis. Cryptanalysis is what the layperson calls “breaking the code.”

6. The areas of cryptography and cryptanalysis together are called cryptology.

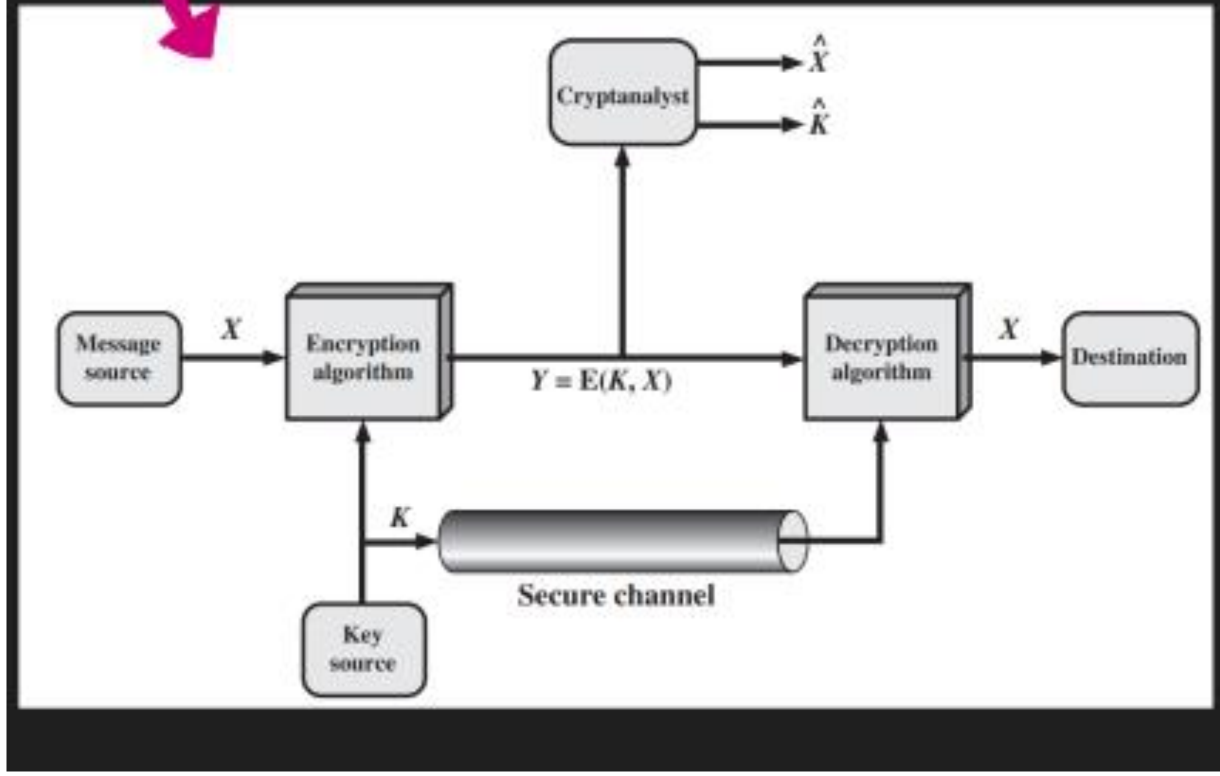
# Symmetric Cipher Model

Simplified Model of Symmetric Encryption



Secret key shared by sender and recipient
K
Secret key shared by sender and recipient
K
X
Transmitted ciphertext
$Y = E(K, X)$
$X = D(K, Y)$
Plaintext input
Encryption algorithm (e.g., AES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

Practical Model of Symmetric Encryption



A symmetric encryption scheme has five components:

- Plaintext:
This is the original intelligible message or data that is fed into the algorithm as input.

- Encryption algorithm:
The encryption algorithm performs various substitutions and transformations on the plaintext.

- Secret key:
The secret key is also input to the encryption algorithm. The key is a value independent of the plaintext and of the algorithm. The algorithm will produce a different output depending on the specific key being used at the time. The exact substitutions and transformations performed by the algorithm depend on the key.

- Ciphertext:
This is the scrambled message produced as output. It depends on the plaintext and the secret key. For a given message, two different keys will produce two different ciphertexts. The ciphertext is an apparently random stream of data and, as it stands, is unintelligible.

- Decryption algorithm: This is essentially the encryption algorithm run in reverse. It takes the ciphertext and the secret key and produces the original plaintext.