Section 1

What is Cryptography?

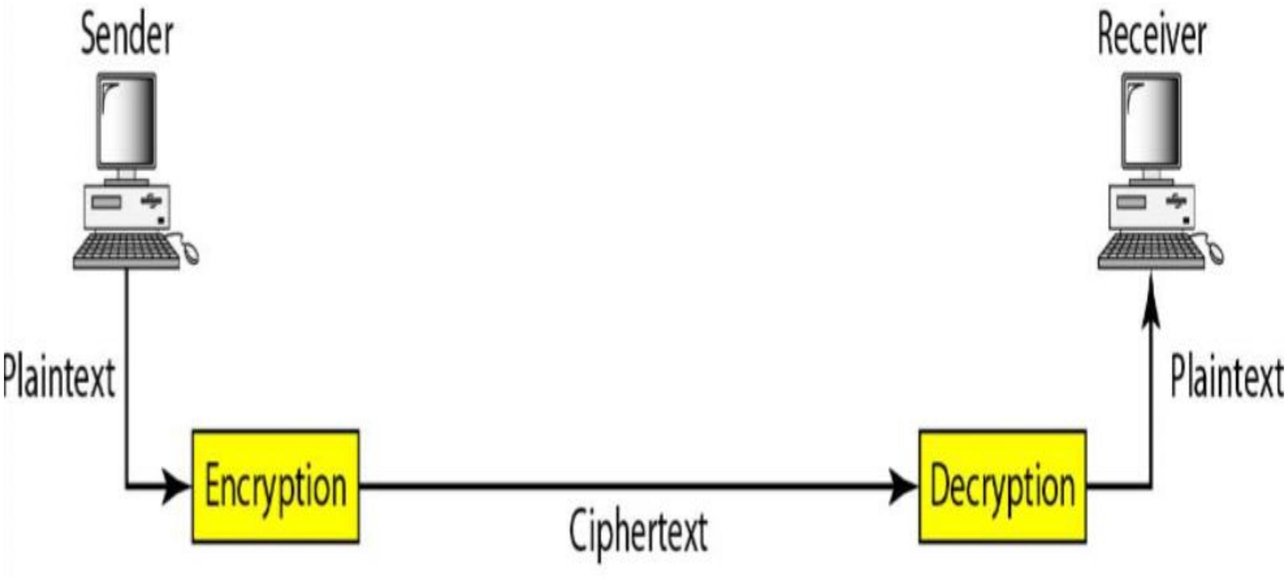
- Cryptography is the art of protecting information by transforming the original message, called plaintext into an encoded message, called a cipher or ciphertext.
- It provides Confidentiality, Integrity, Accuracy

- **1.Confidentiality or Privacy** : Service is used to save the information content of all persons except that told them to get acquainted with them.
  2.Data Integrity: This service is used to save the information of the change (delete or add or modify) by persons unauthorized to do so.
  3.Proof of identity **(Authentication):** This service is used to prove the identity of the data handling (authorized).

- **(Non-repudiation):** This service is used to prevent a person from denial to do something, Digital Signature

Basic Terms

- Plain Text: Message before encryption.
- Cipher Text: Message after encryption.
- Cipher: Encryption algorithm
- Encryption: the process of converting Plain text to Ciphertext
- Decryption: the process of converting ciphertext back to the original plaintext.
- Key: Sequence that controls the operation and behavior of the cryptographic algorithm.


Sender
Receiver
Plaintext
Plaintext
Encryption
Ciphertext
Decryption

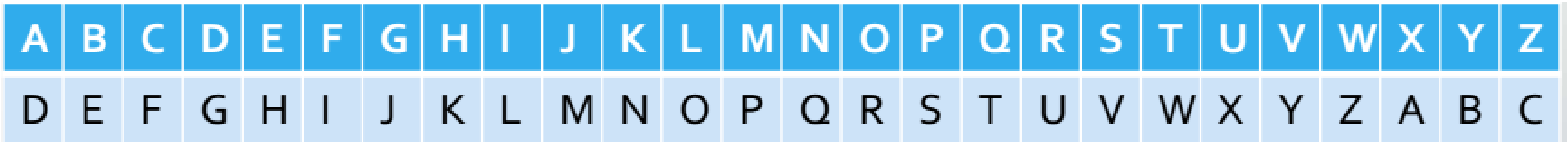
Techniques for Cryptography

1. **Substitution Technique**: In substitution cipher technique, the characters of a plain text message are replaced by other Characters, Characters, Number or Symbols.

Example: Caesar Cipher.

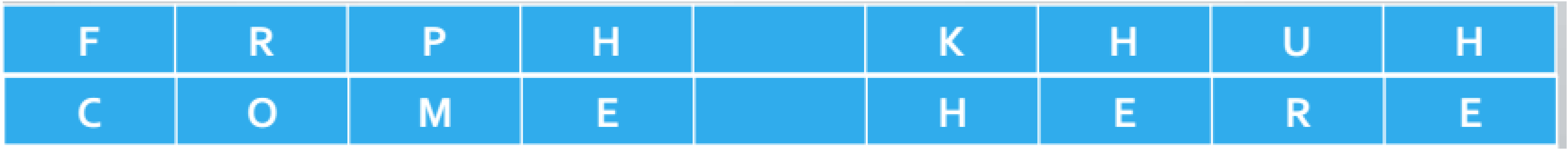
- Caesar Cipher is a special case of substitution technique wherein each message

message is replaced by an alphabet three place down the line.



A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

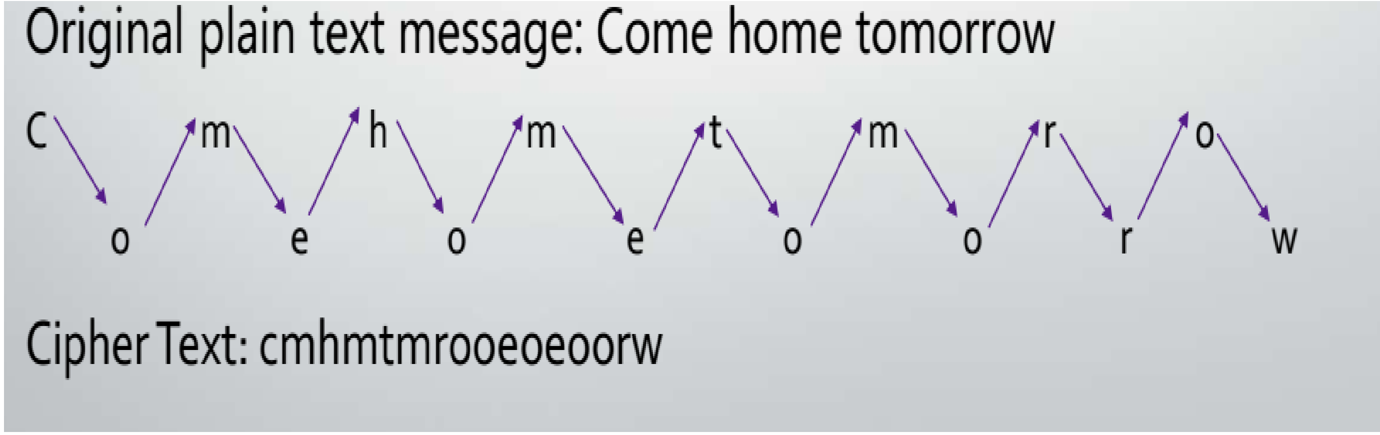
- To decrypt Caesar Cipher we have to replace each alphabet in cipher text.



F	R	P	H		K	H	U	H
C	O	M	E		H	E	R	E

Techniques for Cryptography (Contd..)

- 2. Transposition Technique: Transposition techniques differ from substitution techniques in the way that they do not simply replace one alphabet with another; they also perform some permutation over the plain text alphabets.



Original plain text message: Come home tomorrow

C m h m t m r o

o e o e o o r w

Cipher Text: cmhmtmrooeoeoorw

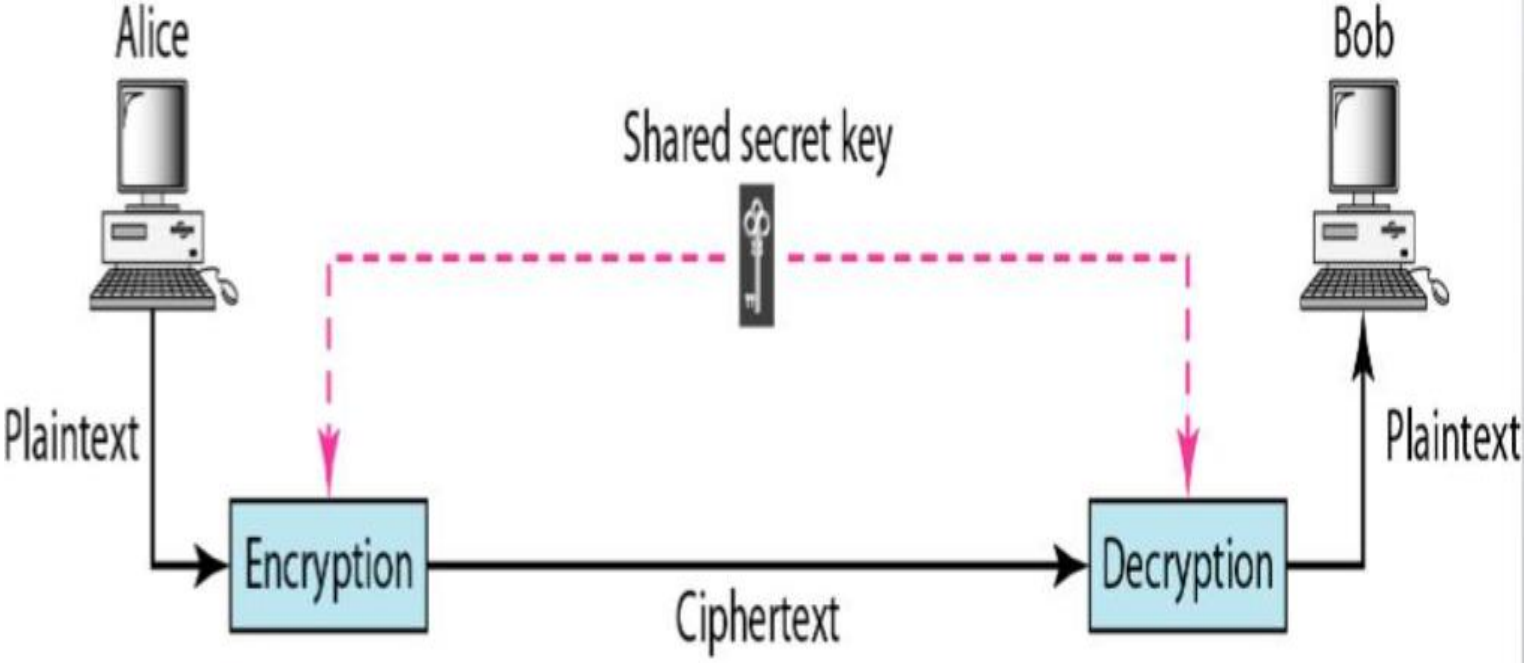
Types of Cryptography

- **1.Symmetric Key Cryptography**:

Symmetric key cryptography involves the usage of the same key for encryption and decryption.

Both sender and receiver must know the common key.

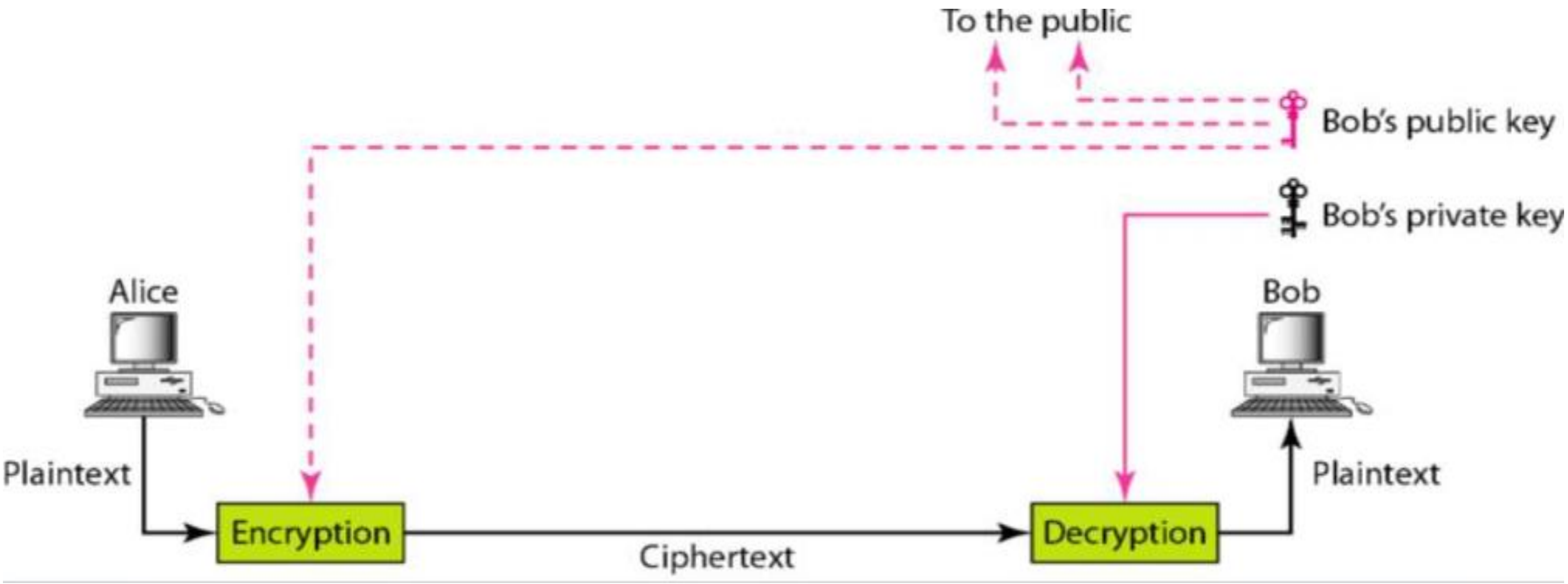
The common key need to be exchanged before hand by some other secure method.

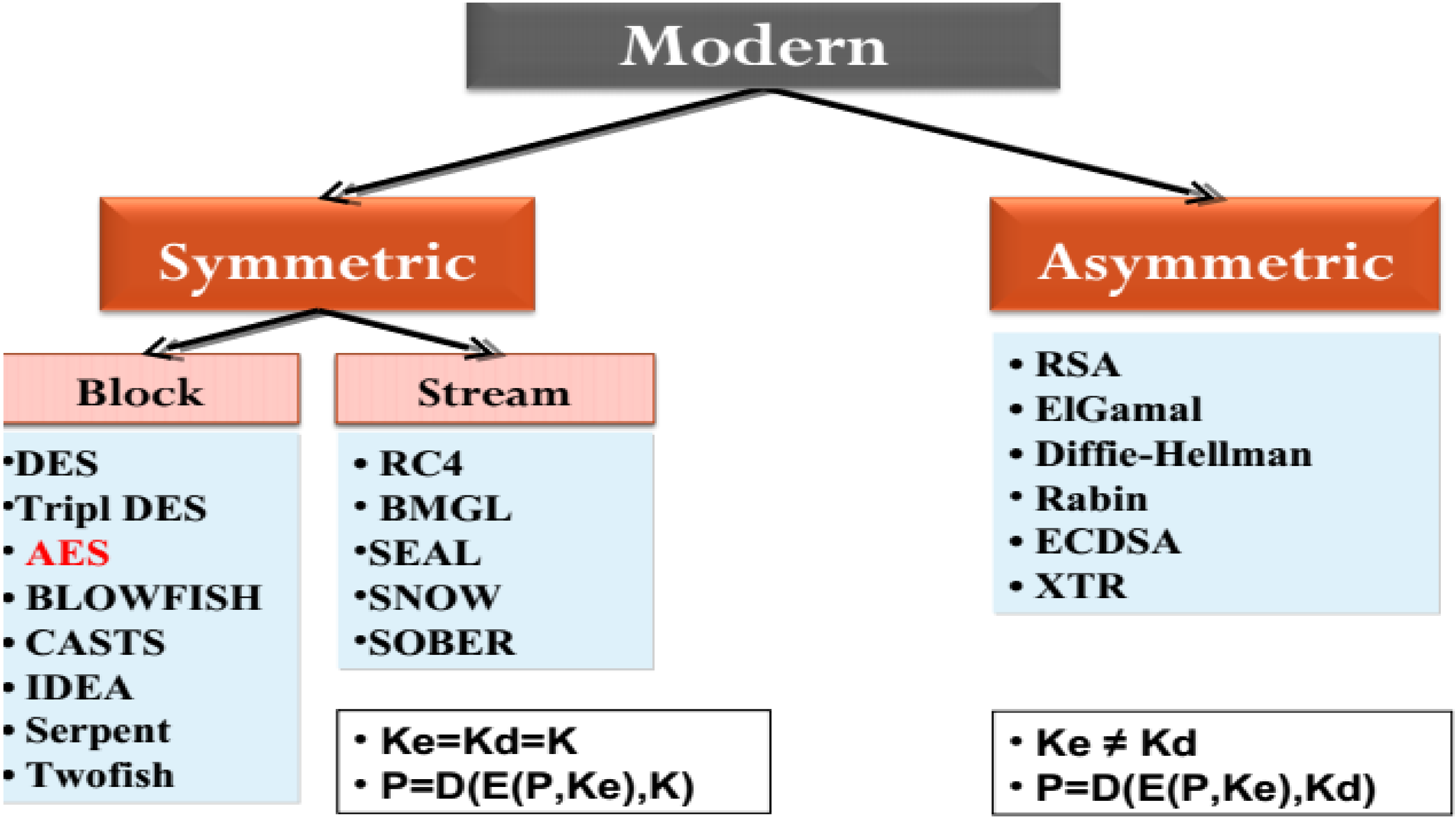

Alice
Bob
Shared secret key
Plaintext
Plaintext
Encryption
Ciphertext
Decryption

Types of Cryptography (Contd…)

2. Asymmetric Key Cryptography:

- Two different keys are used to encrypt and decrypt the message.
- Receiver generates a public and private key pair.
- Receiver broadcasts the public key
- Encryption is done by public key and private key is used for decryption.


To the public
Bob's public key
Bob's private key
Alice
Bob
Plaintext
Encryption
Ciphertext
Decryption
Plaintext



Modern

Symmetric

Block

- DES
- Tripl DES
- AES
- BLOWFISH
- CASTS
- IDEA
- Serpent
- Twofish

Stream

- RC4
- BMGL
- SEAL
- SNOW
- SOBER

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

Asymmetric

- RSA
- ElGamal
- Diffie-Hellman
- Rabin
- ECDSA
- XTR

- Ke ≠ Kd
- P=D(E(P,Ke),Kd)