# Unit 2

## Index



## Cryptography

Why? To achieve the CIA triad i.e. Confidentiality, Integrity, Availability and Non - Repudiation.

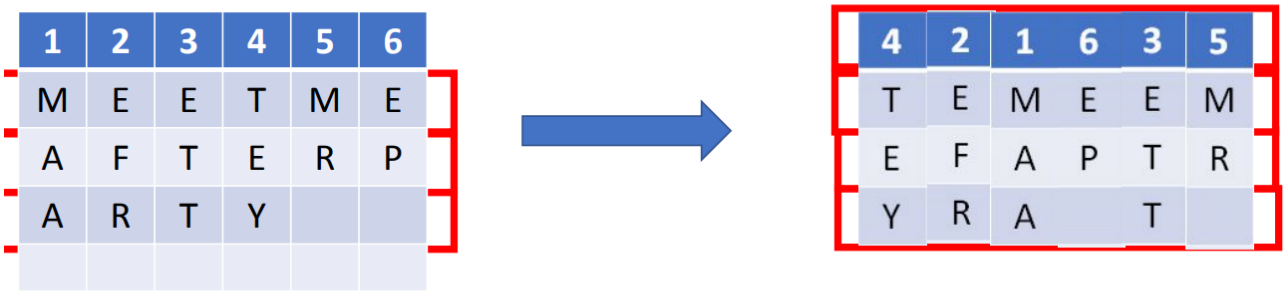
2 basic types of ciphers. Symmetric and non symmetric.

### Symmetric Cipher

Common problem is scaling. We need nC2 keys for n participants.

- Transposition Cipher

  - Plain Text: MEET ME AFTER PARTY
  - Key: 421635




  - Cipher Text= TEMEEMEFAPTRYRAT

- Substitution Cipher

- Plain Text : `Data Encryption`
  - Key word : 4

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 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 |

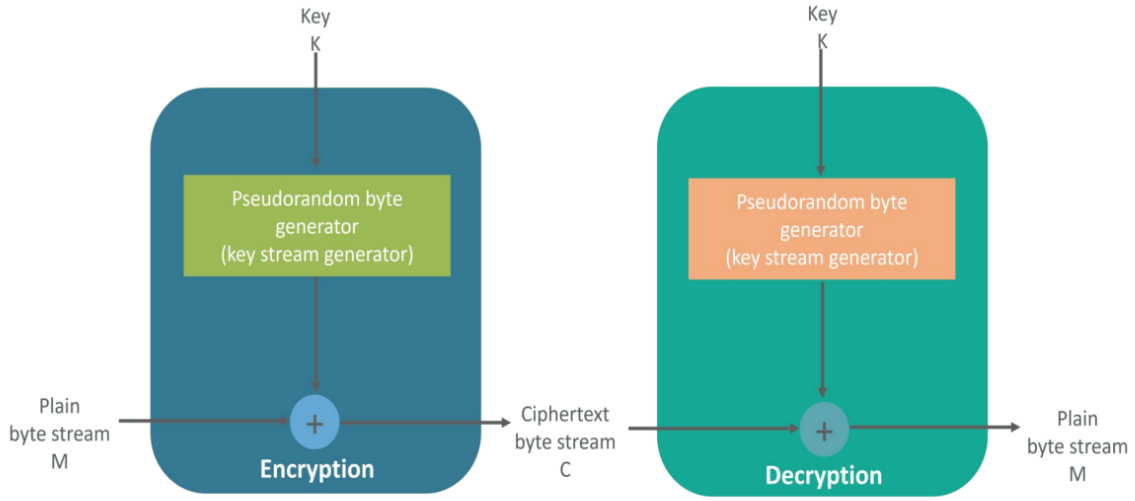
"D" will be replaced with the next 4th alphabet "H" in cipher text

Decryption- Go backwards and select

  - Cipher Text : `Hexe Irgvctxmsr`

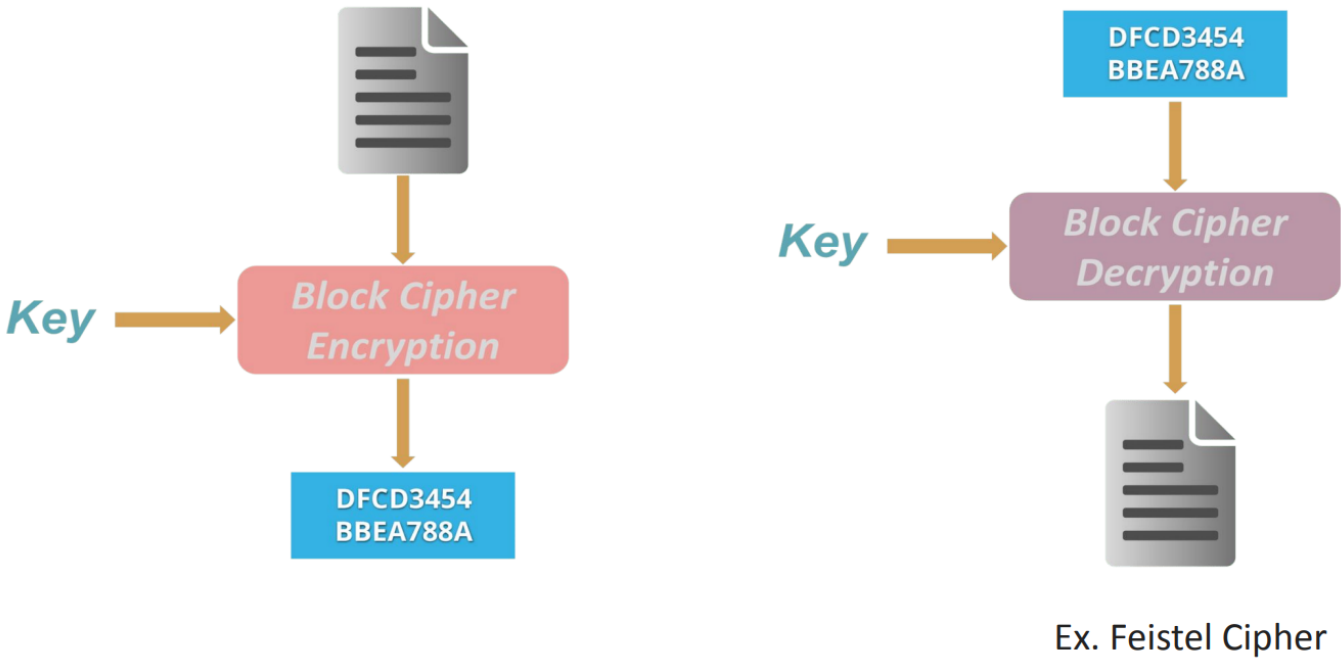
- Stream Ciphers

Bit by bit conversion




Ex: OTP/ RC4

- Block Cipher




Ex. Feistel Cipher

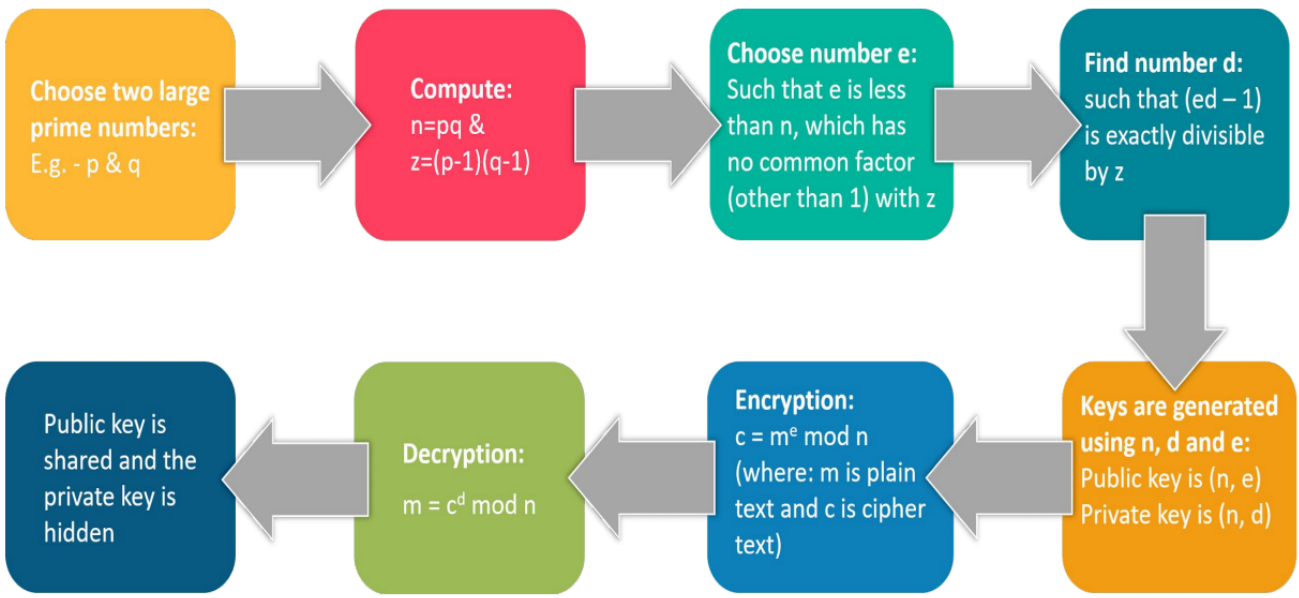
DES

This is a block cipher. A 64-bit key but effectively 56 bits. Not used as it weak as fuck.

## Asymmetric Cipher

This is the private and public keys.

RSA




Diffie Hellman

dunno

## Digital Signature

This is a digital fingerprint. They use the standard Public Key Infrastructure. We add the digital signature to the file after encryption. This does all the CIA and non repudiation.

## Hash

The usual. MD-5, SHA-1, SHA-256 (bitcoin), Keccak-256 (Ethereum).