02/07/2025 Cyber security

Data Encryption Standard (DES):

Block Ciphers feature → file, data. → high security

→ largest block size, thats why greater security

→ Larger key size " "

→ multiple round " "

→ each round
→ substitution
→ Permutation
→ XOR

Stream ciphers features: → voice, vedio → Real-time

→ encrypt data one bit or byte at a time

→ low memory use

→ fast & efficient

when used:

→ Real-time communication (vedio, voc)

→ When low latency & ~~speed~~ need

→ low processing power

Feistel Network:

Encryption Decryption

NIST: National institute of Standard & Technology

Cipher Suite: set of algo for secure communication (Like HTTP, SSL etc)

~~Example~~

9 components:

	Algo
→ key exchange	RSA, ECDHE
→ Authentication	RSA, DSA,
→ Encryption Algo	AES, 3DES
→ MAC/Hash function	SHA-256, SHA-384

TLS protocol

Replacement or alternative 3DES or AES

DES feature:

Type : symmetric key block cipher

block cipher size : 64 bit

key size : 56 bit

round : 16

Structure: Feistel Network

Work Step:

(i) Input 64-bit plaintext

(ii) IP (Initial Permutation)

(iii) 16 round feistel Network

each round
- → sub
- → perm
- → XOR

(iv) FP (Final ...)

(v) Output 64-bit ciphertext

P box:

1.	20	27	9	28	5	21	93
26	91	25	12	92	13	45	62
19	11	51	31	10	30	29	94
90	6	99	57	50	58	3	60
18	52	69	14	56	15	46	16
39	24	55	98	2	32	63	59
53	7	17	54	61	22	47	33
38	23	36	35	8	37	34	9

→ Expansion function DES (32bit → 48bit)

→ Compression " DES

S box

Permutation box

Expansion function

↓

S-box

↓

Permutation box (P-box) / compression function

DC-2

Is S-box is compression box?