

43

UNIT - II

①

Block CIPHERS & PUBLIC KEY CRYPTOGRAPHY

Data Encryption Standard (DES) - ②

Block cipher Principles - ⑤

Block cipher modes of opn - ⑥

Advanced Encryption Standard (AES) - ⑫

Triples DES - ⑭

Blowfish - ⑰

RC5 algorithm - ⑳

Public-key cryptography - ㉓

Principles of public key crypto systems - ㉕

The RSA algorithm - ㉗

Key management - ㉚

Diffie-Hellman Key Exchange - ㉞

Elliptic curve arithmetic - ㉟

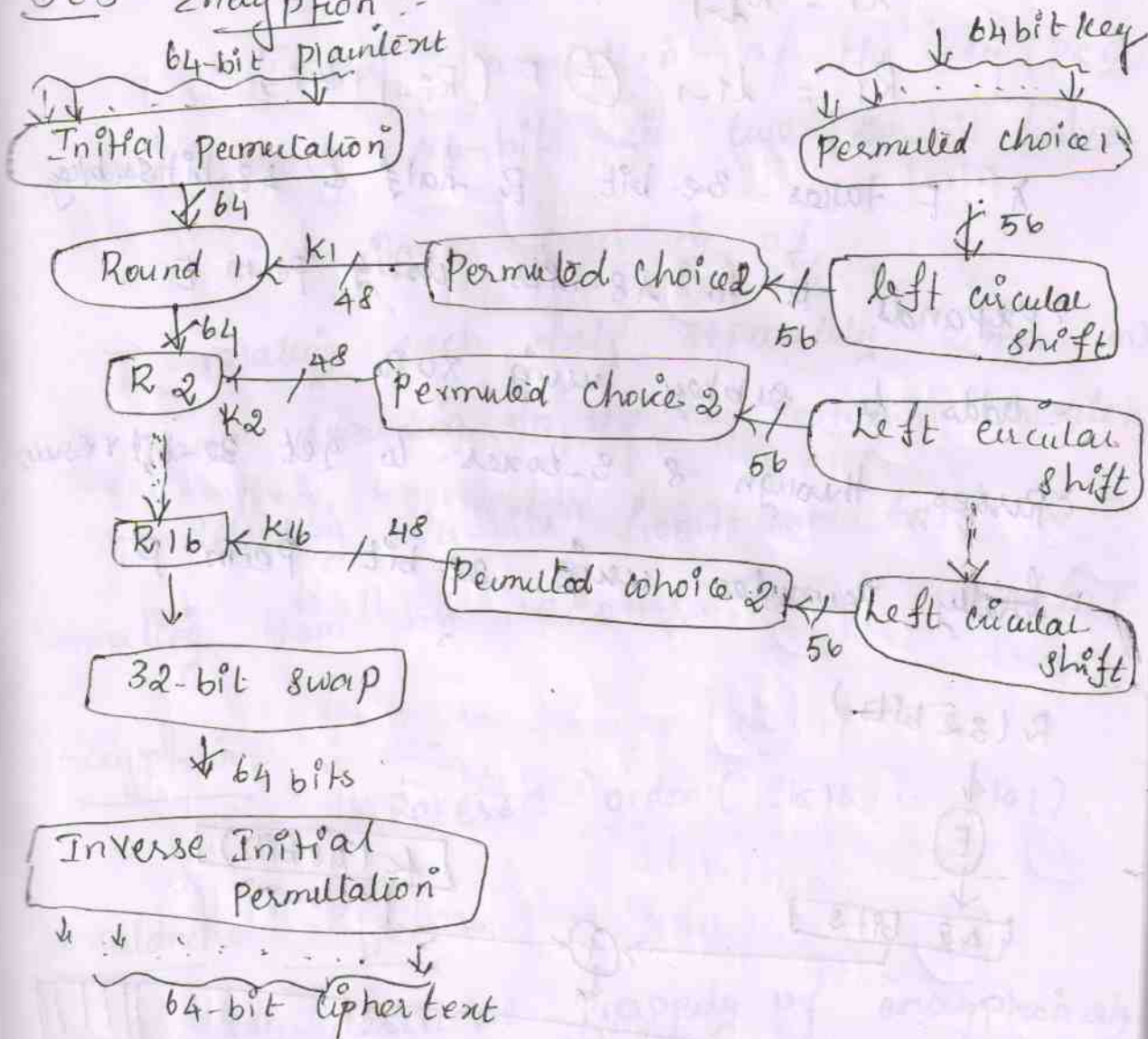
Elliptic curve Cryptography - ㊱

Block CIPHERS

Data Encryption Standard (DES):-

- * Proposed by NIST adopted in 1977.
- * It is a block cipher & encrypts 64-bits data using 56-bit key.

DES Encryption :-



Initial Permutation IP:-

- * 1st step of the data computation.
- * IP reorders the IP data bits.
- > Even bits to LH half, odd bits

Ex: IP (675a69b7 5e5a6b5a) ⁽³⁾

= (ff b 21 94 d 004 df6 fb)

DES Round Structure:

* uses two 32-bit L & R halves.

* Feistel cipher,

$$L_i = R_{i-1}$$

$$R_i = L_{i-1} \oplus F(R_{i-1}, k_i)$$

* F takes 32-bit R half & 48-bit subkey.

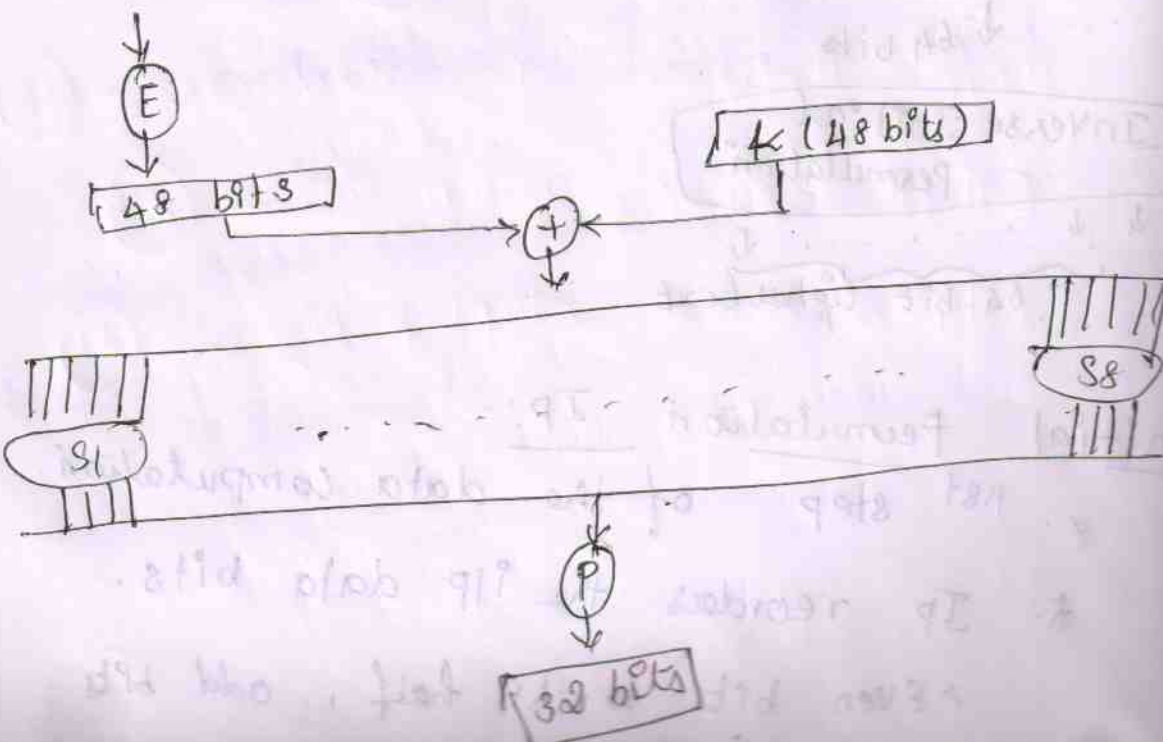
> expands R to 48-bits using Perm E

> adds to subkey using XOR

> passes through 8 S-boxes to get 32-bit result

> finally permutes using 32-bit Perm P.

R (32 bits)



③

Substitution Boxes 8:-

- * Each of the eight S-boxes is different.
- * Each S-box reduces 6 bits to 4 bits.
- * So, the 8 S-boxes implement the 48-bit to 32-bit contraction substitution.

DES Key Schedule:-

- * Forms subkeys used in each round.
 - > Initial permutation of the key (PC1) which select 56-bits in two 28-bit halves.
 - > 16 stages consisting of,
 - rotating each half separately either 1 (or) 2 places depending on the key rotation schedule.
 - selecting 24-bits from each half & permuting them by PC2 for use in round fn F.

Decryption:

- * Reverse order ($S_{k16} \dots S_{k1}$).

Avalanche Effect:-

- * Key desirable property of encryption alg.
- * where a change of one i/p (or) key bit results in changing approx half o/p bits.
- * Making attempts to "home-in" by guessing keys impossible.

Strength of DES - key size.

(5)

> 56-bit keys have $2^{56} = 7.2 \times 10^{16}$ values.

> brute-force search looked hard.

Analytic Attacks:-

> differential cryptanalysis

> linear cryptanalysis

> related key attacks.

Block cipher principles:-

* Basic principles still like Feistel in 1970's.

x. Number of Rounds.

↳ more is better, Exhaustive search best attack.

x. Function f :

↳ provides "confusion" is non-linear, avalanche.

> have issues of how S-boxes are

selected.

* key schedule

> complete subkey creation, key avalanche

Block cipher modes of operation :- (6)

* Block cipher encrypts fixed size blocks.

Ex: DES encrypts 64-bit blocks.

* NIST SP 800-38A defines 5 modes.

↳ block & stream modes.

Modes of Opn:-

> Electronic code book (ECB) } Blk

> Cipher Block chaining (CBC) } Blk

> Cipher Feedback (CFB) } Stream

> output Feedback (OFB) } Stream

> Counter (CTR).

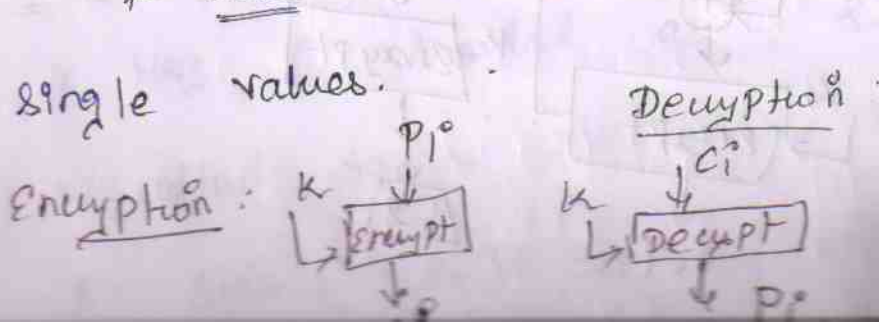
Electronic codebook Book (ECB):-

* Msg is broken into independent blks that r encrypted.

* Each blk is a value which is substituted like a codebook, hence name.

* Each blk is encoded independently of the other blks. $C_i = E_k(P_i)$.

* Uses: Secure transmission of single values.



Adv & limitations of ECB:- (7)

- * Msg repetitions may show in ciphertext.
 - > If aligned with msg blks.
 - > Particularly with data such graphics or with msg that change very little, which become a code-book analysis pbm.
- * Weakness, is ~~also~~ independent.
- * ~~Vulnerable~~ vulnerable to cut-and-paste attack.
- * Main use is sending a few blks of data.

Cipher Block Chaining (CBC):-

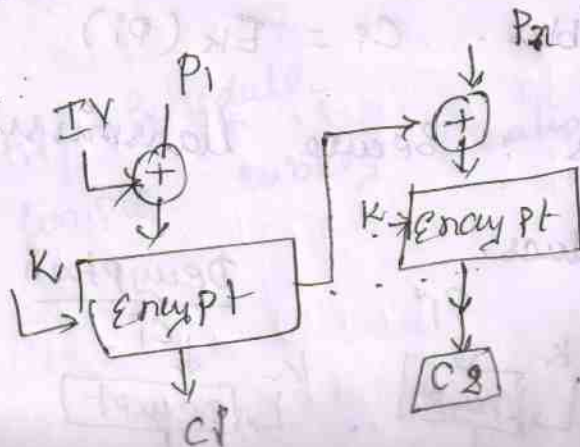
- * Msg is broken into blks.
- * Each previous cipher block is chained with current plaintext blk.

$$C_i = E_k (P_i \oplus C_{i-1})$$

$$C_1 = IV$$

uses: bulk data encryption, authentication.

Encryption:



Adv & dis adv:-

* A ciphertext blk depends on all blks before it. any change to a blk affects all following ciphertext blks ... avalanche effect.

Disadv:

- * need Initialization vector (IV)
 - > which must be known to sender & receiver
 - > Integrity must be checked.

Stream modes of opn:-

- * blk modes encrypt entire blk.
- * May need to operate on smaller units
 - ↳ Real-time data.
- * Convert blk cipher into stream cipher
 - > cipher feedback (CFB) mode
 - > output " (OFB) "
 - > counter (CTR) "
- * Use blk cipher as some form of

Pseudo-random no generator ... Vernam cipher

Cipher Feedback (CFB):-

- * msg is treated as a stream of bits
- * added to the o/p of the blk cipher

* stds [128, 192, 256, 512, 1024]

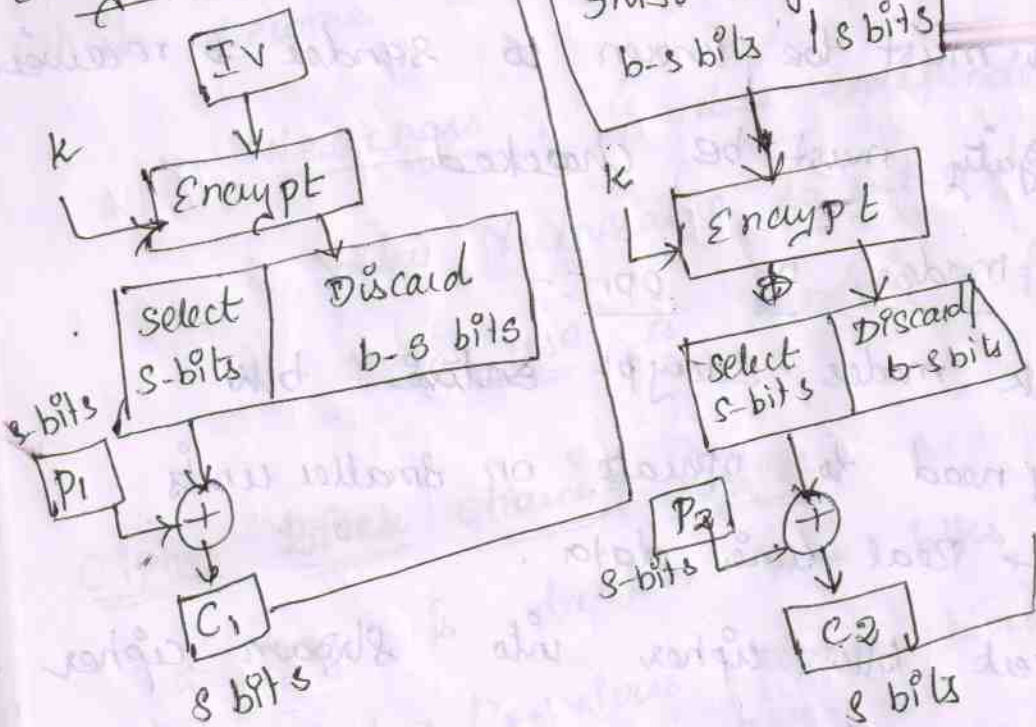
$$C_i = P_i \text{ XOR } E_k(C_{i-1})$$

(9)

$$C_{-1} = IV$$

uses: Stream data Encryption, authentication

Encryption:



Adv & Limitations:-

- * Data arrives in bits / bytes.
- * Limitation is need to stall while doing encryption after every s-bits.
- * Errors propagate for several bits after the error...

output Feedback (OFB) :-

- * O/P of cipher is added to msg.

$$O_i = E_k(O_{i-1})$$

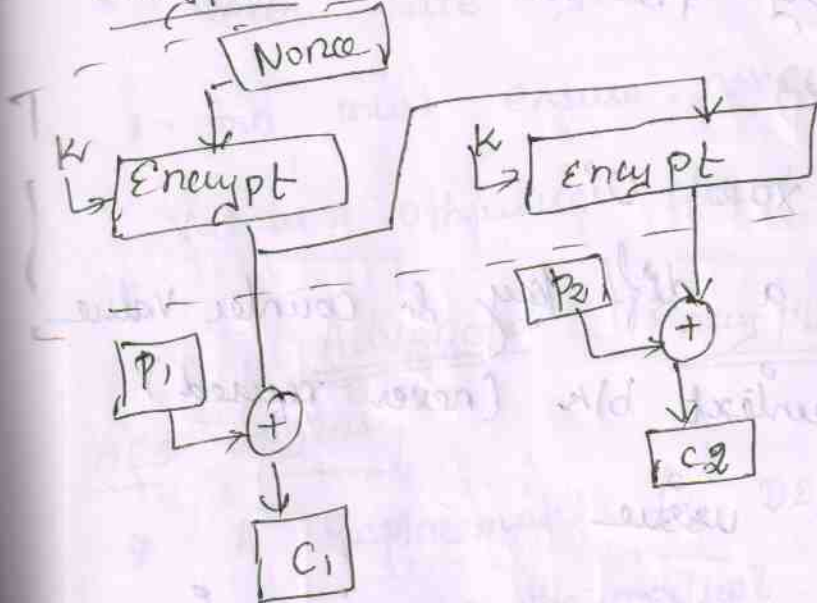
$$C_i = P_i \text{ XOR } O_i$$

* FB is independent of msg (10)

uses: Stream encryption on noisy channels.

why noisy channels?

Encryption:



Adv & limitation:

- * Needs an IV which is unique for each use.
 - ↳ If ever reuse attacker can recover o/p.
 - ↳ OTP
- * Can Pre-compute
- * Bit errors do not propagate
- * More vulnerable to msg stream modification.
 - ↳ change arbitrary bits by changing ciphertext.
- * Sender & receiver must remain in sync
- * only use with full blk FB.
 - ↳ CFB64 (or) CFB128.

