UNIT - II

BLOCK CIPHERS & PUBLIC KEY CRYPTOGRAPHY:-

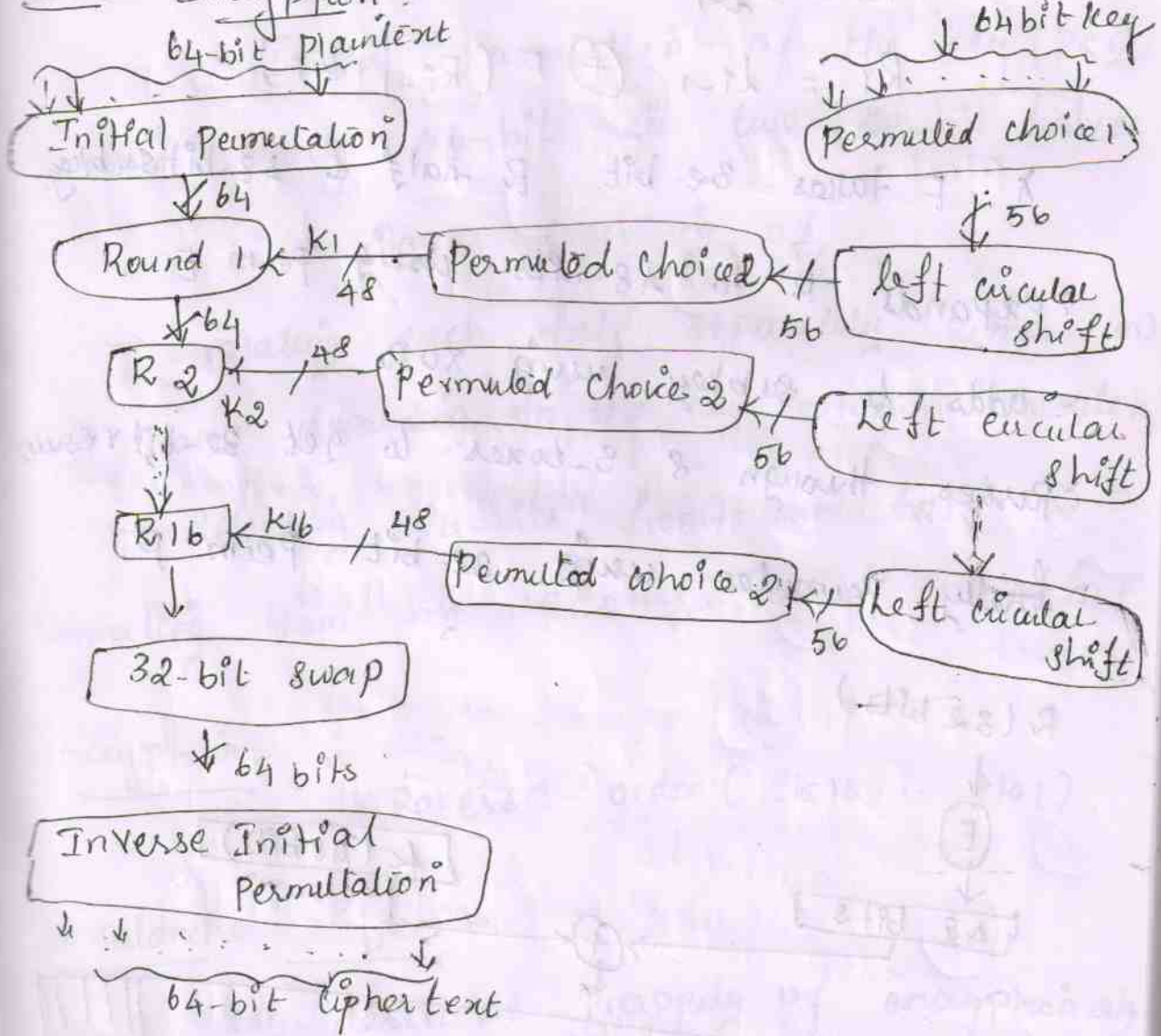
UNIT-II

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 i/p data bits.
  > Even bits to LH half, odd bits

Ex: IP (675a6967 5e5a6b5a)

= (ffb2194d 004dfbfb).

DES Round Structure:

* uses two 32-bit L & R halves.
* Feistel Cipher,

$L_i = R_{i-1}$

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

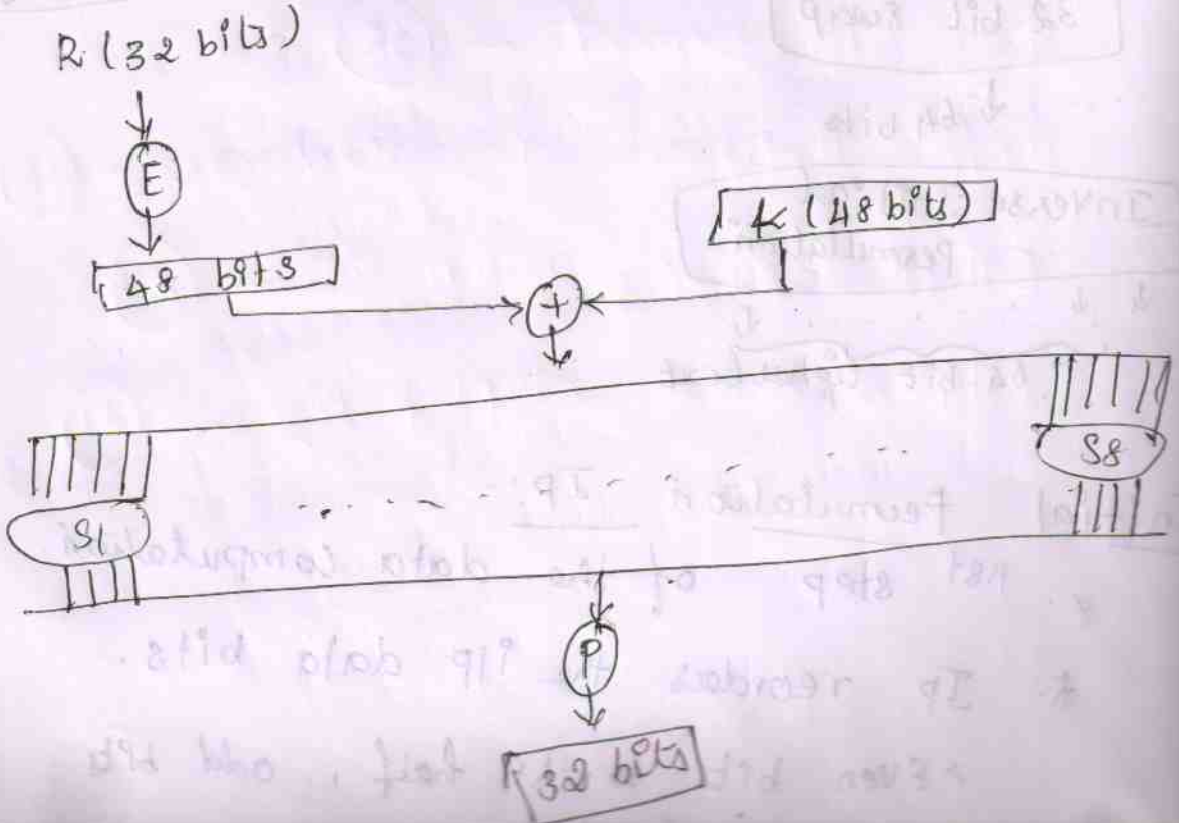
* F takes 32-bit R half & 48-bit subkey.

> 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.



Substitution Boxes S:-

* 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 confusion 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 k,
    - → selecting 24-bits from each half &. Permuting them by PC2 for use in round fn F.

Decryption:

* Reverse order (SK16 ... SK1).

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.

> 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 Feistels 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

> complex subkey creation, key avalanche

Block cipher modes of operation :-

* Block ciphers 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) }
- Cipher Feedback (CFB) } stream
- output Feedback (OFB) }
- 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.

Encryption : P_i → K → [Encrypt] → C_i

Decryption : C_i → K → [Decrypt] → P_i

Adv & limitations of ECB:-

* Msg repetitions may show in ciphertext.
  > If aligned with msg blk.
  > Particularly with data such graphics (or) with msg that change very little, which become a code-book analysis pblm.

* Weakness, is ~~dtcs~~ independent.

* ~~Vlstu~~ vulnerable to cut-and paste attack

* Main use is sending a few blks of data.

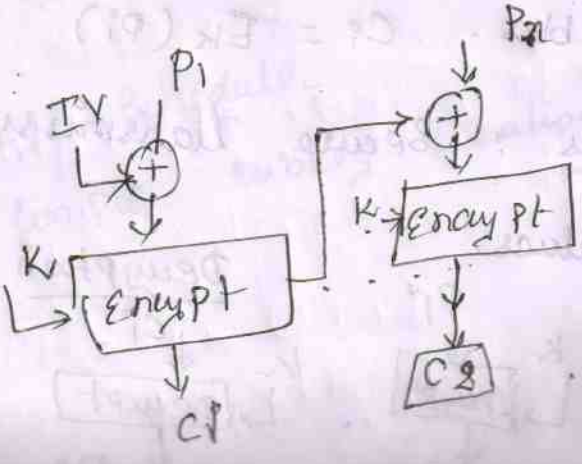
Cipher Block chaining (CBC):-

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

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

$$C_{-1} = IV$$

uses: bulk data Encryption, authentication.



Adv & disadv:-

* A ciphertext blk depends on all blks before it. any change to a blk effects 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):-

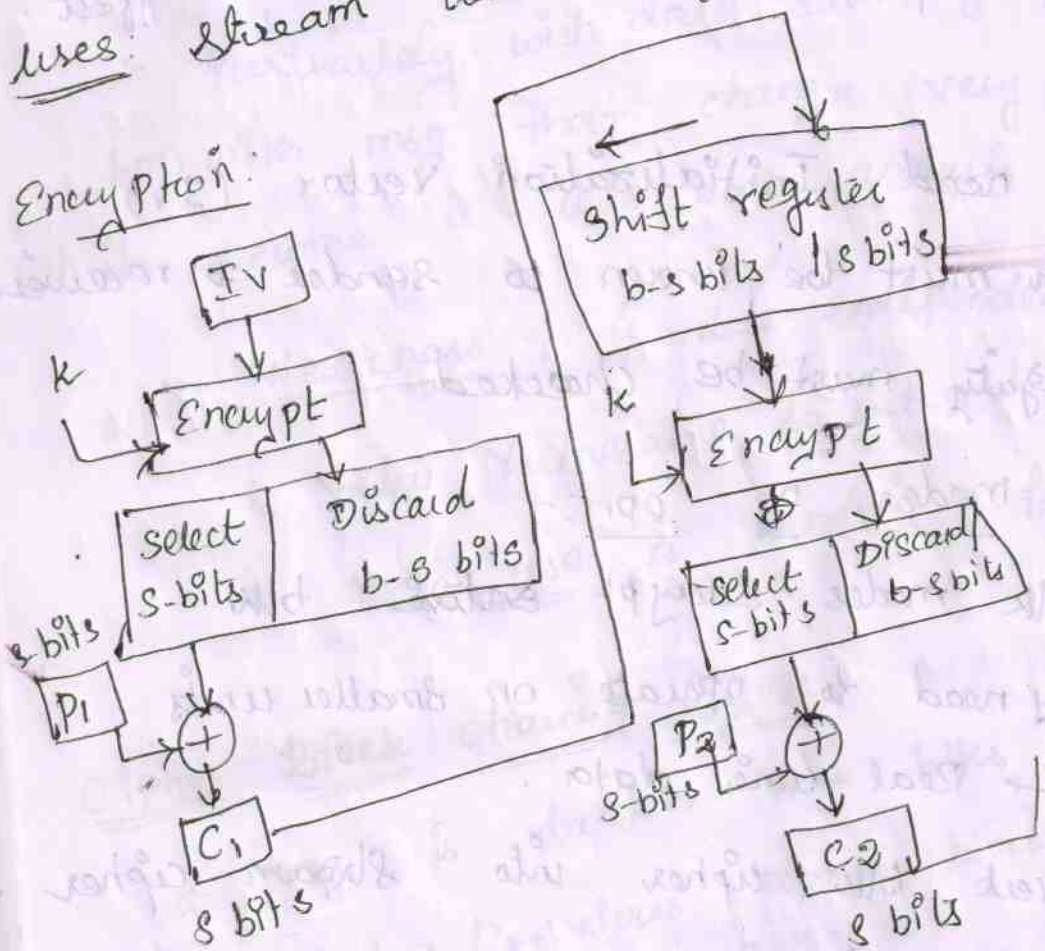
* Msg is treated as a stream of bits
* added to the o/p of the blk cipher
* sds [1, 8, 16 (or) 64 (or) 128].

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

$C_{-1} = IV$

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 blks after the error....

Output FeedBack (OFB):-

* O/P of cipher is added to msg.

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

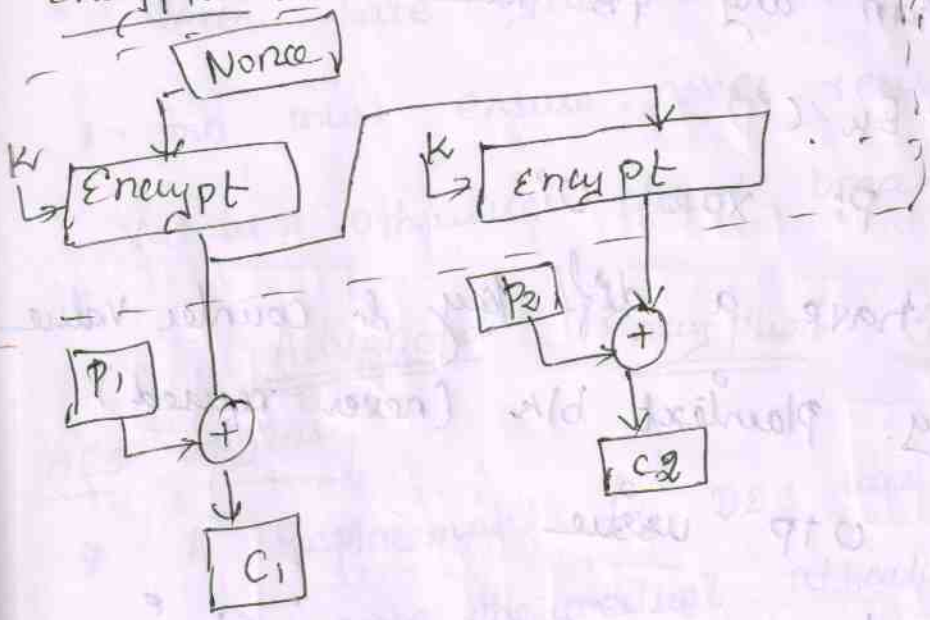
$C_i = P_i \text{ XOR } O_i$

* FB is independent of msg

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