* Cryptography Technique:

NESO PART 1

CT-1 Theory.

CT-2 Computer Security: The protection afforded to an automated information system in order to attain the applicable objectives of preserving CIA of information system resources (includes hardware, software, firmware, info / data and telecommunication).

CIA Triad Confidentiality, Integrity, Availability.

(i) private keys, encryted data

(ii) sent = receive, no modification should occur.

(iii) Availability of services, reliable on service.

CT-3 Threats v/s Attacks.

OSI security Architecture

→ Security Attack | Mechanism | Services.

LT-4 Security Attack

→ Passive Attack (Hard to Detect) → learn or make use of info from data

↳ Release of msg content ↳ Traffic Analysis.

→ Active Attack (Hard to Prevent) Modification of data stream.

↳ masquerade (login someone account and pretends to be him)

↳ Replay (send same msgs)

↳ Modification. (change in msgs)

↳ DoS (Denial of service) (overloading servers)

LT-5 **Security Services**

- ↳ Authentication (Peer entity , Data origin.
- ↳ Access Control (Not all users have same access)
- ↳ Data confidentiality (encryption)
- ↳ Integrity (no modification)
- ↳ Non repudiation (Assurance that someone can't deny the validity of smth.)

LT-6 **Security Mech.**

- ↳ Specific
  - → Encipherment
  - → Digital Signature (Authentication, Integrity)
  - → Access control.
  - → Data Integrity)
  - → Traffic Padding (dummy data)
  - → Routing control
  - → Notarization.
- ↳ Pervasive.

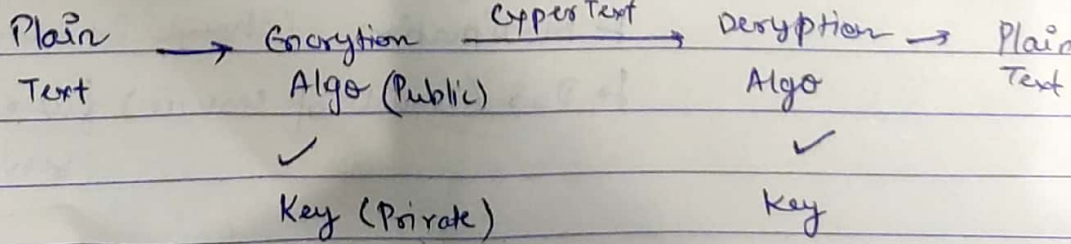
See video Theory

LT-7 **Network Security model** Theory.

4 major tasks:

- Algorithm
- Generate secret info
- methods for distribution and sharing info.
- Specify a protocol.

LT-8 **Cryptography**



If same key is used → symmetric.
(Private key cryptography)

* Symetric Cryptography: Same key is used for encryption and decryption. (Private key eg)
eg DES (Data Encryption systems), AES, RC4.

* Asymmetric eg: Different keys. One key is Public and another is Private.
(Public key cryptography)
↳ RSA, DSA, Elliptic Curve. / Deffie Hellman

Encryption scheme.
→ Unconditionally secure
→ computationally secure.

CT-9 Theory

CT-10 Crytanalysis:
→ Based on info know to the cryptanalyst.
Types of crytanalyst → Theory.

CT-11 Brute-force attack → Trying all possibilities key
Avoided using captcha

CT-12 Encryption Techniques:
(1) Substitution (2) Transposition.

(1) Letters of plain text are replaced with other letters or symbols.
eg: a → M
g → 9

(2) Applying some sort of permutation of plain text.
eg → NESO : ENSO, ENOS, SONE etc.

Substitution	Transposition
→ Ceasar Cipher	→ Rail Fence
→ Monoalphabetic Cipher	→ Row Column Transposition
→ Playfair Cipher	
→ Hill Cipher	
→ Poly alphabetic	
→ One-Time Pad	

CT-13 **Ceasar Cipher.**

→ letter are replaced by other letter or symbols.

→ k = 3

$$C = E(p, k) \bmod 26$$
$$= (p + k) \% 26$$

$$p = D(C, k)$$
$$= (C - k) \% 26$$

CT-14 **Shift Ciphers**

K = 2, 3, 4, 5 . . . . .

CT-15 **Monoalphabetic Cipher**

'Cipher' line can be permutation of 26 Alphabetic characters.

Character can be mapped to any character unlike shift cipher (no uniform difference)

CT-16 Play fair Cipher.

→ Manual symmetric technique.
→ First Lateral diagram substitution diagram.
→ Multiple letter encryption technique.
→ 5×5 Matrix constructed using a keyword.
→ I/J are together

Rules for encryption:

(1) Diagrams
(2) Repeating letters → Filler letter
(3) Same column |↓| Wrap around
(4) Same Row |→| Wrap around
(5) Rectangle |⇆| swap.

attack → at ta ck

academy → ac ad em gx
↑ fillers

balloon → ba ll oo n
ba lx lo on.
↑ filler.

CT-17 Generate cipher text from plain text

Given key = MONARCHY

attack

at ta ck
RS SR DE

mosque

mo sq ue
ON ts ML

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

Eg: 7, 9

CT-19 Hill cipher.

- Multi-letter cipher
- can encrypt 2 letter, 3 letter or more letters (gp of letters)

$C = E(k, P) = P \times k \mod 26$

$P = D(k, C) = C \times k^{-1} \mod 26 = P \times k \times k^{-1} \% 26$

Convert string to number $a \to 0$ $z \to 25$

group would be determined by $(M \times M)$

Then perform encryption. and Integers to string.

CT-20

Decryption of Hill cipher.

$$k^{-1} = \frac{1}{|k|} adj(k).$$

$$k^{-1} = (adj\ k) \times |k|^{-1} \quad \text{(Extended Euclid)} \quad \% 26.$$

CT-21 Polyalphabetic cipher (Vigenère cipher)

→ A set of related monoalphabetic subst. rule is used

→ A key determines which particular rule is chosen for a given transformation.

Vigenère cipher)

consists of 26 Caesar cipher with shift 0 – 25

one to many mapping.

$C_i = (P_i + k_{i \bmod 26}) \mod 26.$

$P_i = (C_i - k_{i \% 26}) \% 26.$

7

key is repeated

Auto key system.

Vigenere Cipher – Cryptanalysis.

→ Determine the length of the keyword.

→ Key and the plain text share the same frequency distribution of letters, a statistical techniques can be applied.

CT-22 Vernam Cipher.

→ Systems works on binary bits rather that letter.

$$C_i = P_i \oplus K_i$$

$$P_i = C_i \oplus K_i$$

CT-23 One Time pad:

→ ~~Key~~ Key is random, as long as message.

→ The key is not repeated.

→ The key is used to encrypt and decryt a single message and then discarded.

→ For each new message → a new key is required.

→ 2 Fundamental Difficulties

→ Practically making larger quatities of random keys.

→ Key distribution and protection.

→ used for low-bandwidth channels requiring very high security.

Perfect secrecy.

Perfect secrecy is the notion that given an encrypted message (or cypter text) from a perfectly secure encryption system (or cipher), absolutely nothing will be revealed about the unencrypted message (or plain text) by the cipher text.

CT-24 Transposition technique:

Rail fence:

→ Plain text is written down as sequence of diagonals and then read of as a sequence of rows

eg:

P → nsa academy is the best

Depth = 2.

→ n s a a e y s h b s t
e o c d m i t e e t.

CT → nsaaeyshbseocdmiteet.

CT-25 Row Column Transposition

→ Rectangle.

→ Write → Row by Row → Read : column by column.

→ Key : Order of the column.

CT-26 Steganography:

→ conceal the existence of message.

→ Hiding the message.

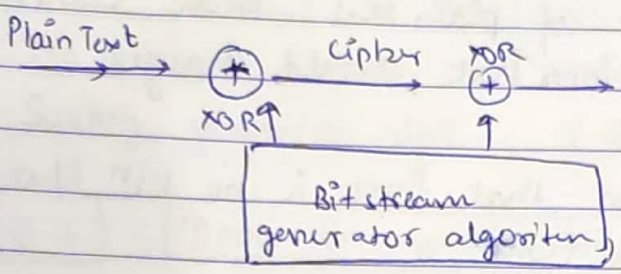
→ Not an encryption scheme.

→ Ex: Boy Is Terribly Caught Haunting

→ Character marking, Invisible Ink, Pin Punctures Typewriter color ribbon.

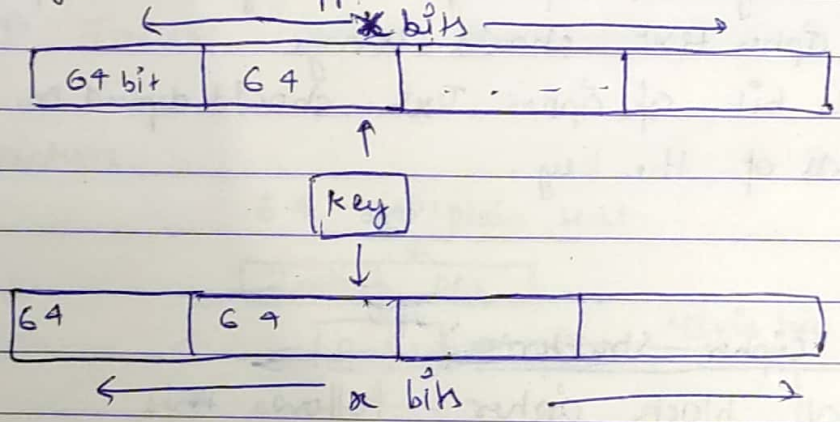
→ LSB steganography.

* Stream Cipher: Encrypts digital data stream one bit or one byte at a time. Symmetric key encryption.



only confusion concept

* Block Cipher :- A block of plain text is treated as a whole and used to produce cipher text of equal length. Symmetric cipher.
→ Typically block size of 64 and 128 bits is used.
→ key will be applied on each block.



eg: → DES (64 bit block size)

confusion & diffusion concept

---

2 methods for preventing cryptanalysis.
(1) Diffusion
(2) Confusion.

(1) Diffusion: If a symbol in plain text is changed, several or all symbols in cipher text should change.

→ The idea of diffusion is to hide the r/n b/w the ciphertext and plain text.

→ So if we change 1 bit of plain text, then statistically half of the bits in cipher text should change. and also viceversa.

Hence it should seem that there is no r/n b/w plain text and cipher text.

→ So each symbol in cipher text is dependent on some or all symbols in plain text.

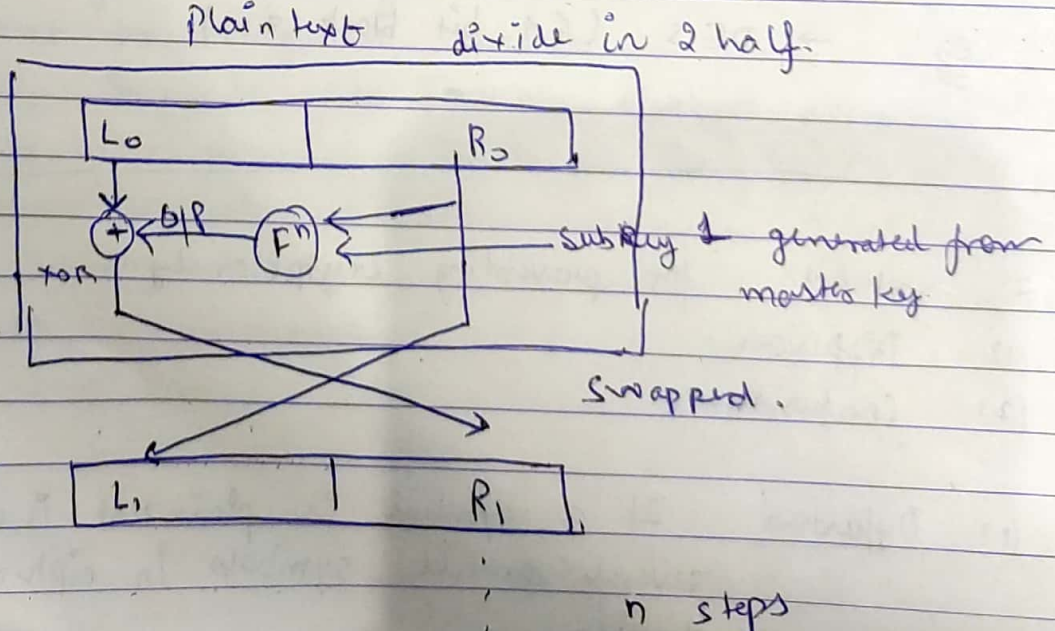
(2) Confusion: Hides r/n b/w ~~cipher~~ cipher text and the key.

→ If single bit of key is changed, most/all bits of cipher text should change.

→ Each bit of cipher Text should depend on several parts of the key.

* Fiestel Cipher Structure:

→ Most of block cipher follows this.



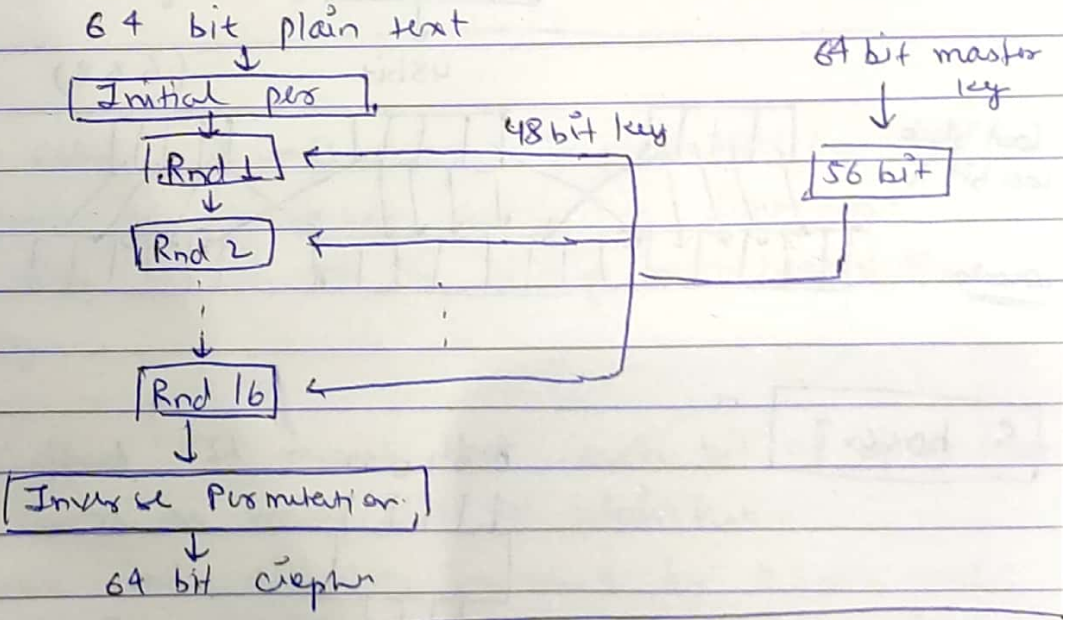
(1) Block size : large block size, more security
(2) key size : large key size large security but may decrease the speed of enc/decr
(3) No of ~~rnds~~ rounds : ↑ rnds ↑ secure.
(4) Subkey generation algo : ↑ complex, harder to break.

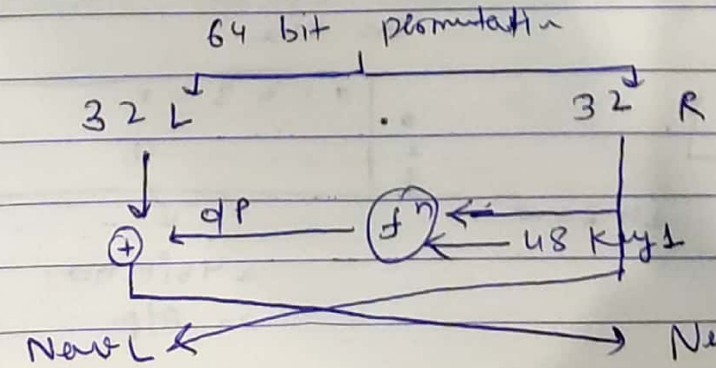
DES | Data Encryption Standard

→ Block cipher : , symmetric
→ 64 bit plain text
→ 16 rnds , each rnd is fiestal rnd.

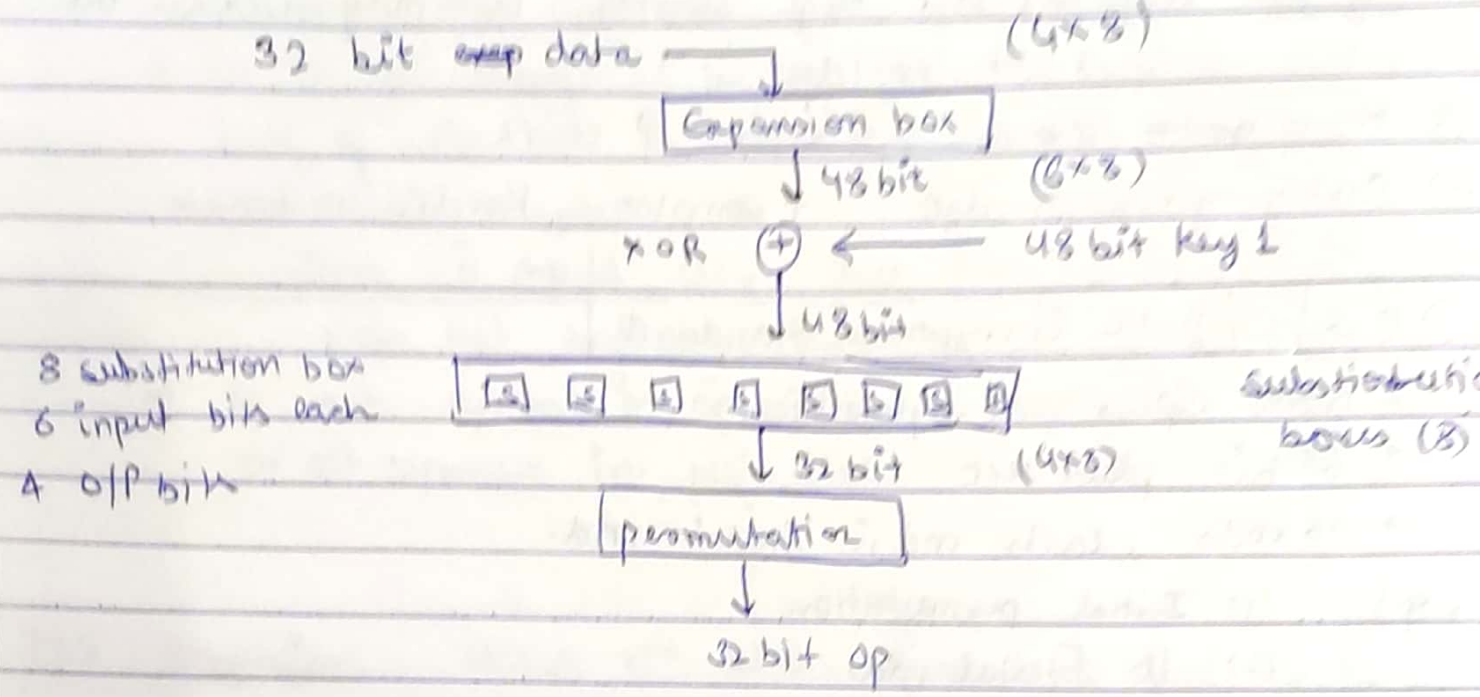
Steps (1) Initial permutation
(2) 16 Fiestal rnds.
(3) Swapping
(4) Inverse initial Permutation.

Basic Structure :

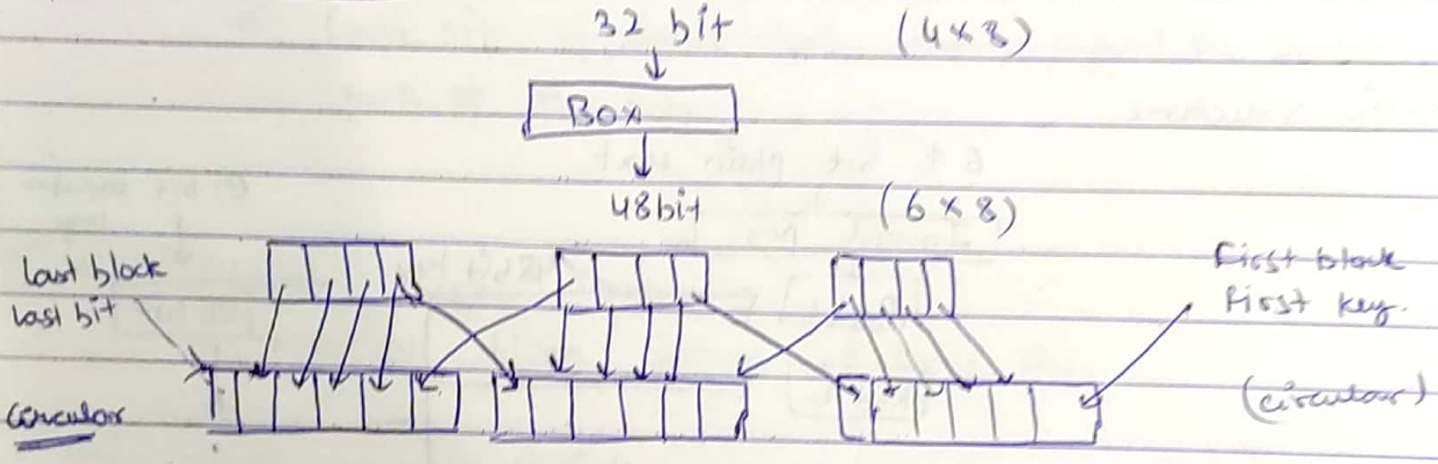




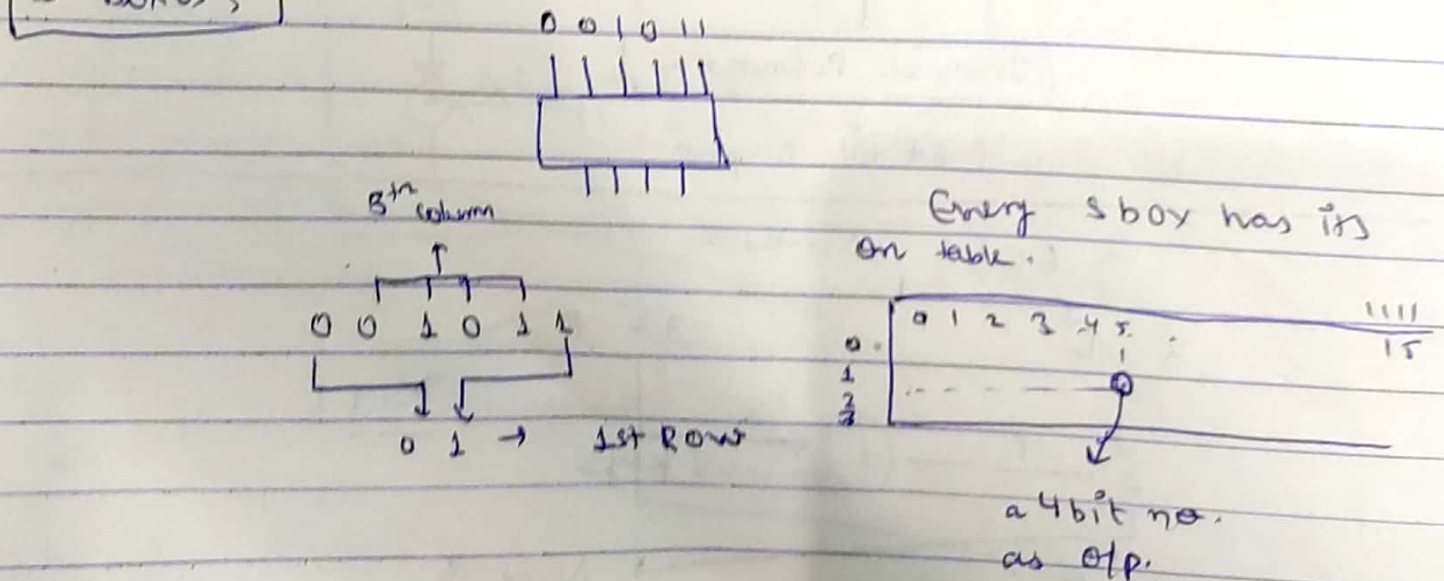
What's the function?



Expansion box?



S boxes?

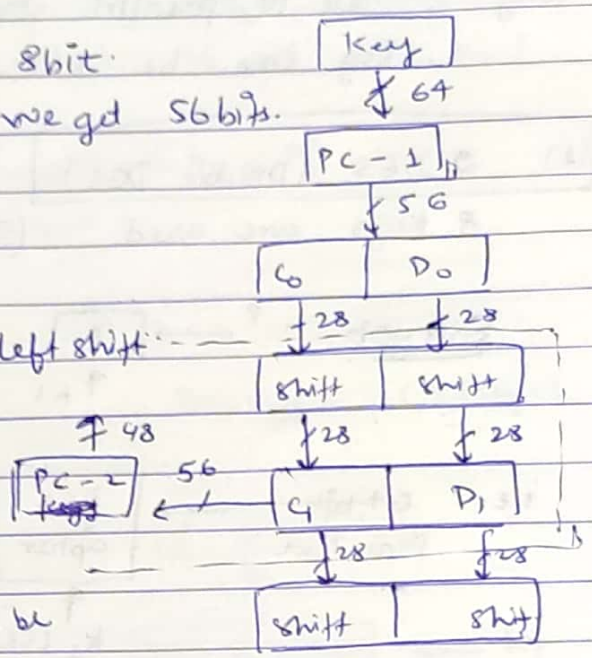


Master key 64 bit.

Have 16 ~~key~~ subkey generated ? 48 bit each

Inside PC-1 8 parts each of 8bit.
last bit is discarded. so we get 56 bits.
(8, 16, 24, 32, 40, 48, 56, 64)

→ 56 bits divided in 2 parts.
↳ in Rnd i = 1, 2, 9, 16 ← 1 bit left shift
other → 2 left shifts.



So $C_0 = 28$
$(4 \times 1) + (9 \times 12) = 28$
Hence all 16 keys generated would be unique.

→ Inside PC-2 using a predefined table we eliminate 8 bits.

DES Analysis

(1) Avalanche effect : A small change in plain text (or key) should create a significant change in cipher text.
→ DES has been proved to be strong with regard to this property.

(2) Completeness effect : It means that each bit of cipher text needs to depend on many bits of plaintext.
→ The confusion and diffusion produced by D-boxes and s-boxes in DES, show a very strong completeness effect.

Multiple DES

Why? Due to parallel computing 2^{56} (brute-force attack) key can be known.

(1) 2 DES (Double DES)

2 keys are used (56+56) 112 bit key.

Encrypt : P → E (↑ K_1) → X → E (↑ K_2) → C

i.e. 64 bit Plain Text → DES cipher (↑ K_1 (56)) → 64 bit Middle Text → DES cipher (↑ K_2 (56)) → Cipher Text

$$P \rightarrow e(K_1, P) \rightarrow E(K_2, E(K_1, P)) \rightarrow \text{Cipher}.$$

Decrypt: 1 decrypt using K_2, we get middle text, then using K_1

$$P = D(K_1, D(K_2, C))$$

→ Meet-in-the-middle attack (MITM)

Encrypt from 1 end
Decrypt from other
} meet in middle

Some pairs of plain Text encrypt pairs for 2^{56} values of K_1

	Plain	Cipher	Middle
K_1 = 1			
2			
.			
2^{56}			

Cipher Text decrypt pairs for 2^{56} values of K_2

K_2	Cipher	Middle
2^{56}		

work to do → $2^{56} + 2^{56} = 2^{57}$

i.e twice than 1-DES.

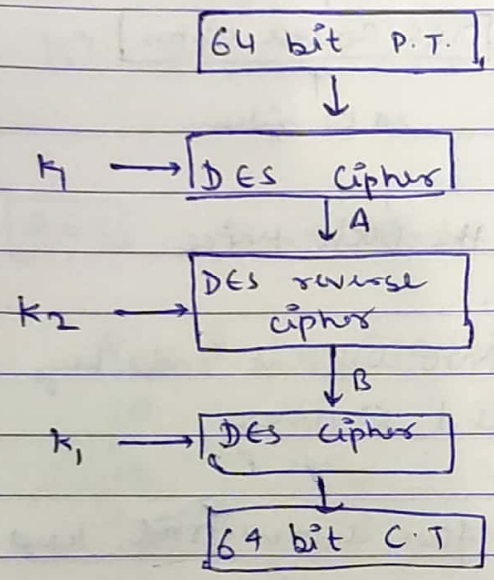
Some pairs would match in both tables.
Hence we get some pairs of $\{k_1, k_2\}$, then we can do brute-force attack to get (k_1, k_2).

Decrypt (k_2, C) = Encrypt (k_1, P).

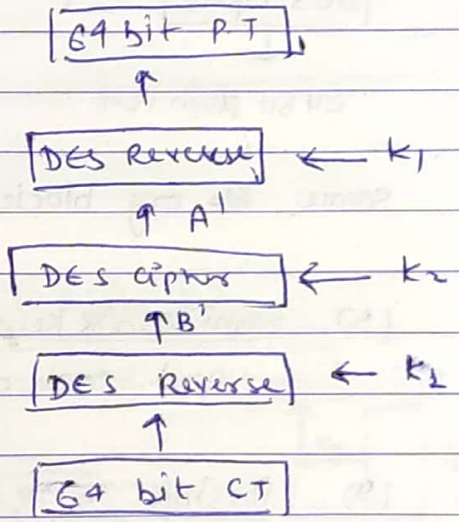
$\therefore (k_1, k_2)$ are used.

Triple DES Much stronger than 2-DES.

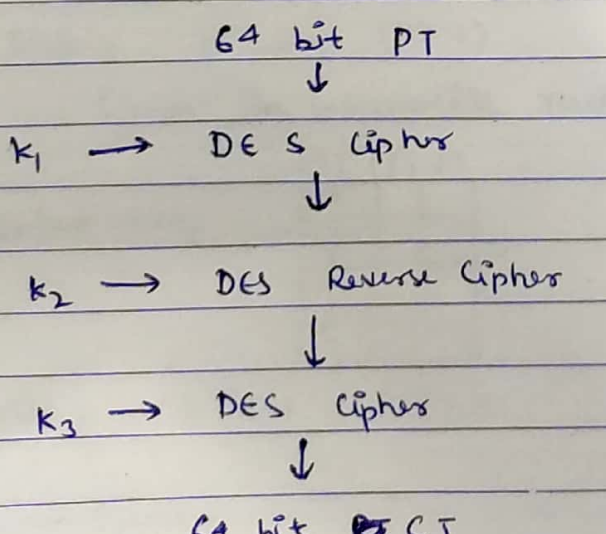
Encrypt (2keys)

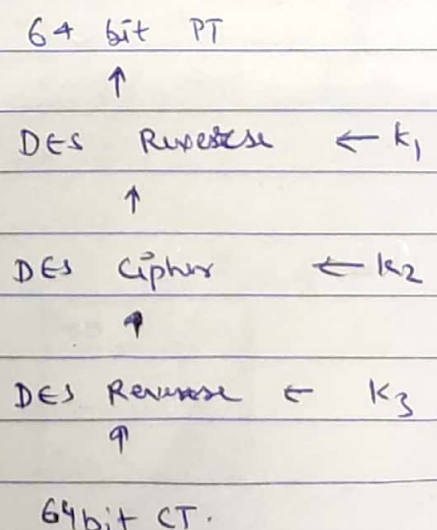


Decrypt (2keys)



(3 keys)

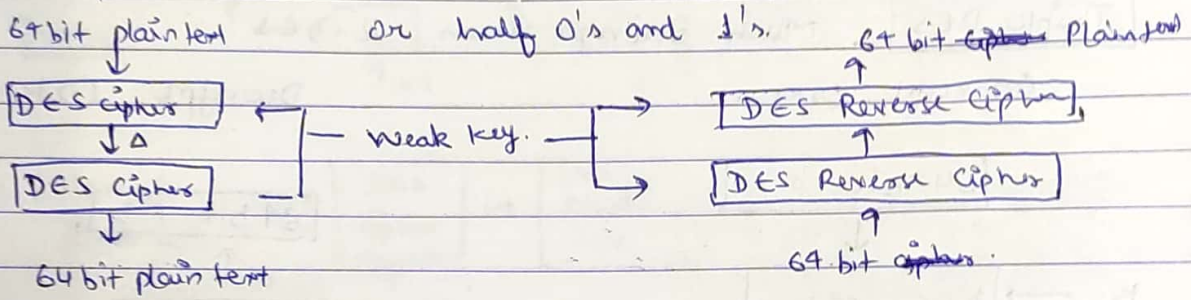




DES Weakness:

(1) Key size → 56 bits → 2^{56} combination (4)
→ easy to break by parallel processing.
So 3-DES is more secure
(112 & 168 bits)

(2) Weak keys: one which consist of all 0s, 1's or half 0's and 1's.



same ~~blo~~ org block if we decrpt the block twice.

(3) Semi weak keys: creates only two different rnds keys and each of them is repeated 8 times

(4) Possible weak keys (48) four different rnd keys

(5) Key clustering → means 2 or more d/f keys can create same cipher text from plain text.

Missing values
Inform the given entry?
Data preprocessing techniques
cause of dimensionality
Terms and concepts.

Distances Mon
Type of Attribute
Simil / Dis
Types of Data
Noise Outlier

Data Tran

PCA ✗

Intro.
Data
step
Applic

Association
Anomaly
Noise &

AES Advanced Encryption standard.

→ Symmetric key block cipher

→ Block size = 128 bits.

1 word = 32 bits
4 bytes

See video.

Block cipher Modes of operation:

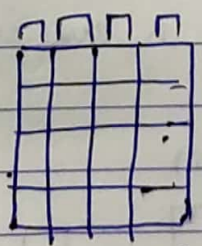
(1) ECB Electronic codeBook mode
(2) CBC Cipher block chaining.
(3) CFB Cipher Feedback.
(4) OFB output feedback
(5) CTR counter mode.

AES fixed block size = 128 bits.

Rnd	Key size (bits)	
10	128	AES-128
12	192	AES-192
14	256	AES 256

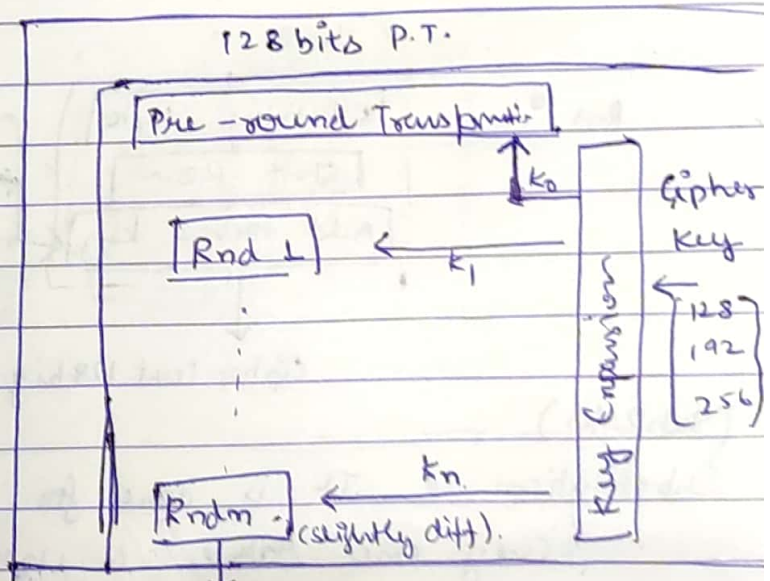
No of subkeys (k_i) = ($Rnd^s + 1$)

State → 16 bytes (4×4)
Stores the intermediate result.



Input array

16byte = 4 word = 128 bits.



S byte of word.

State Array

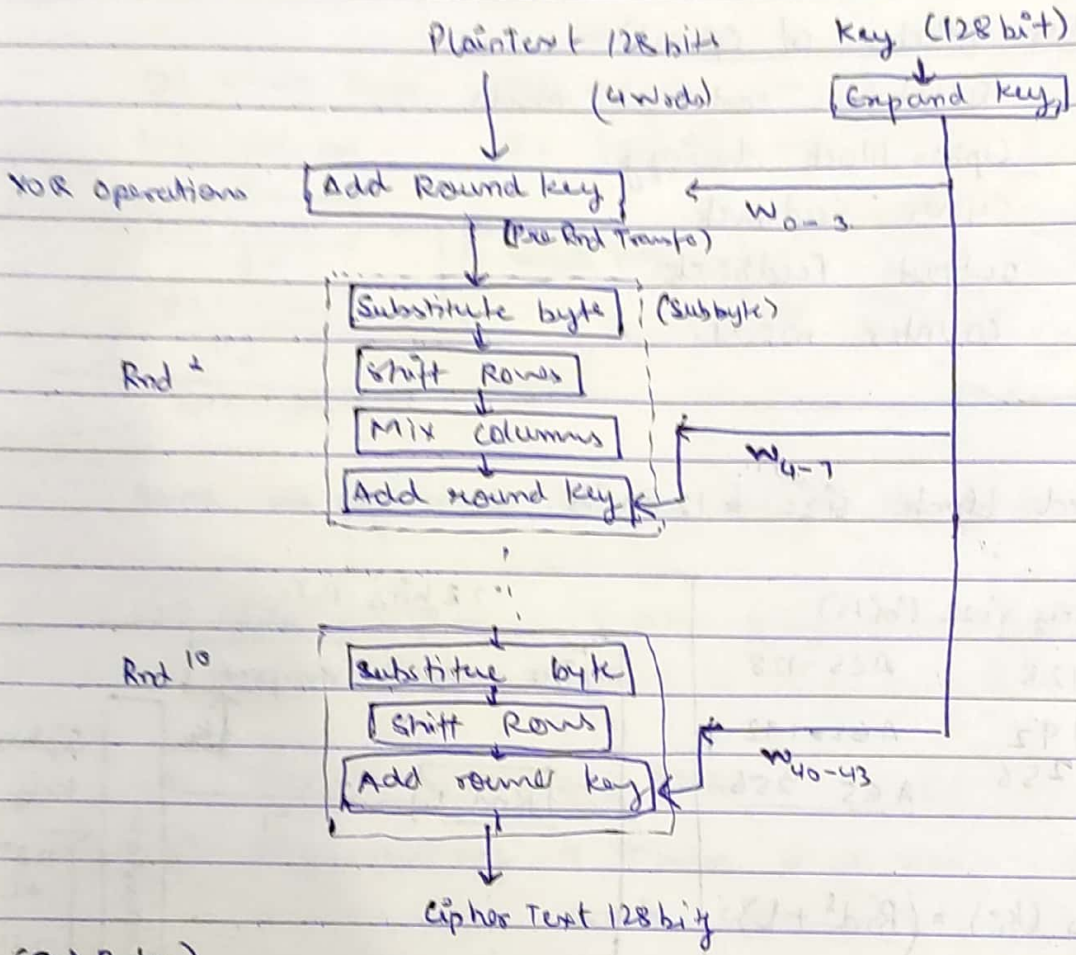
s_{00}	s_{03}
s_{30}	s_{33}

$= [W_0\ W_1\ W_2\ W_3]$

Key 128 bits | 4 words

$[W_0\ W_1\ W_2\ W_3] \xrightarrow[\text{key Algo}]{\text{expand}} [W_0\ W_1\ \ldots\ \ldots\ W_{43}]$

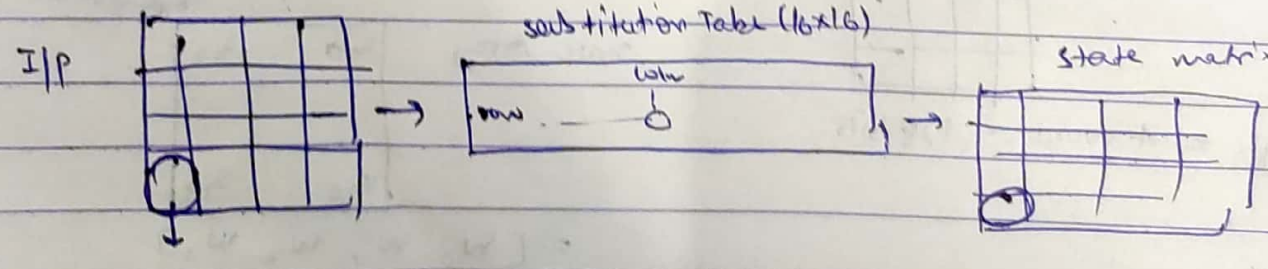
44 Words.



(SubByte)

Substitution. It is done for each byte

Only one table is used for transformation. so if 2 bytes are same, transf. is also same.



XXXX XXXX

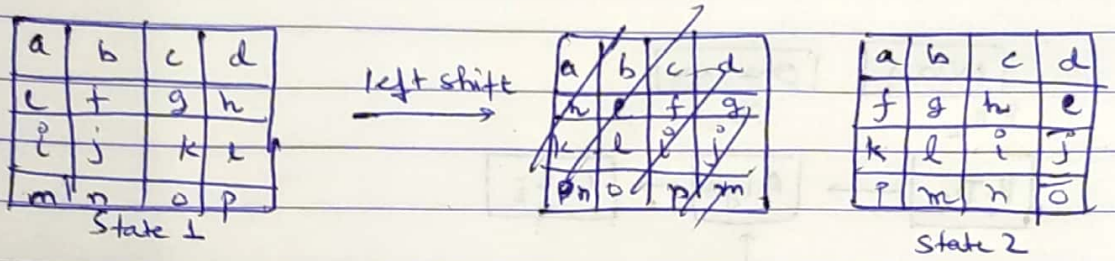
row column

State 1

Permutation (Shift Rows)

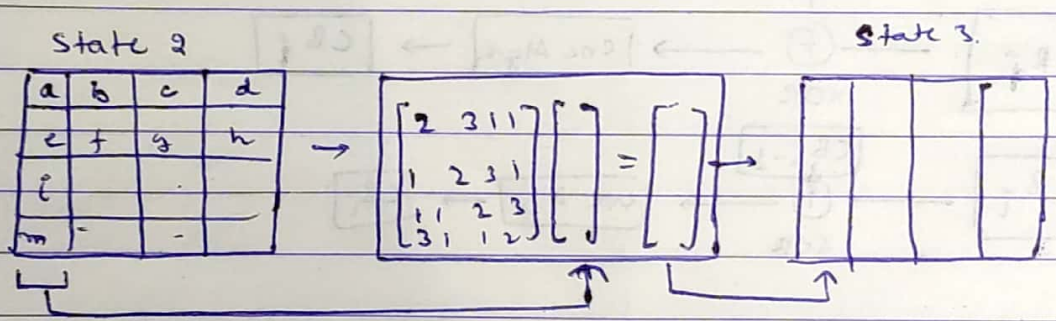
In DES it was done at bit level
AES ——— at byte level.

→ Shifting is done to left.
→ no. of shift = row no. of matrix.



In decryption Inverse shift (right).

Mixing columns



Add Rnd key.

State 3.

$$\begin{bmatrix} a & b & c & d \end{bmatrix} \oplus \begin{bmatrix} w_1 & w_2 & w_3 & w_4 \end{bmatrix} = \begin{bmatrix} \quad & \quad & \quad & \quad \end{bmatrix}$$

Words (4×4 matrix) (4×4 matrix) 4×4 matrix

goes for next rnd.

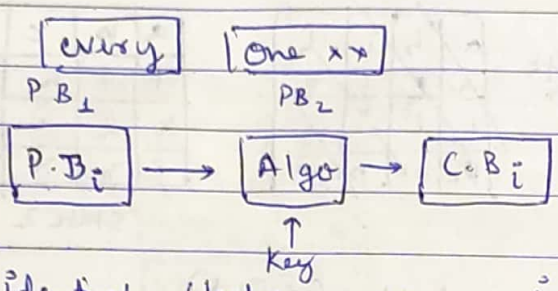
→ ECB

→ plain text is divided in fixed size block.

→ same key for enc and decr.

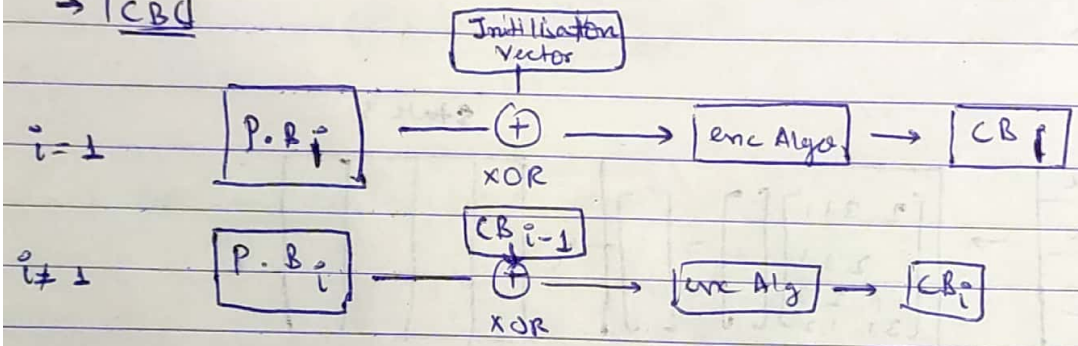
eg block size = 5

P.T. everyone.



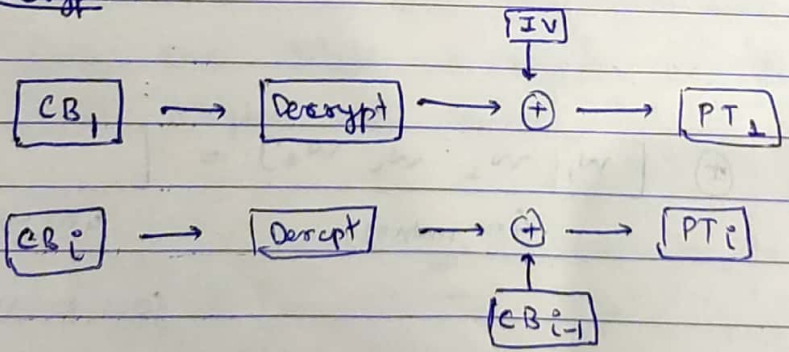
If identical blocks, same cipher Block will be produced.

→ CBC



So patterns are not repeated.

decrypt:



→ identical msgs and same IV is used, cipher Text will be same.