MOD-1

Cyber Attacks.

1] Motives

A Hacker is a successful name for Cyber attack. Hackers are youngsters/teenagers who use attack kits designed by other which are freely downloaded from internet.

Attackers include company insiders like unsatisfied employees.

Cyber terrorists who expose extreme religious & political cause.

Main motives for launching Cyber attacks are:

1] Theft of Sensitive Information.
2] Distruption of Services.
3] Illegal access to or use of Resources.

1] Theft of sensitive info.

Many organisation store & communicate sensitive info on new products to be designed.

Revenue service can be usually advantageous to a company competitors.

Military & Defence plan details of any nation.

pvt Bodies like Corps, Banks, etc & individual's personal info. like credit, cards, passwords, etc.

Taking this is called "Identity Theft".

2] Distruption of services.

Interruption of service against an organisation server which causes unavailable or inaccessible services.

Eg: attacks being launched by business rivals of e-commerce web-sites.

3] Illegal access to or use of resources.
The Goal is to use to obtain free access of services to paid resources.
Eg: Online digital products such as magazines, journal articles, free talk time, etc.

Common attacks.

Attempting to retrieve personal info. from individuals is one common attack which has 2 categories
1] Pharming attack. 2] Phishing attack.

1] It is a cyber attack intended to readirect a web-site's traffic to another fake site.
2] It is an attempt to obtain sensitive info. such as user name, password & credit card details by discussing it with a trust-worthy entity in an electronic communication.

One type of intruding into a system is through password guessing attack, side channel attack, skimming attack
All these forms are identity theft.

Password Guessing attack is done by guessing the keystrokes used by the user.

Dos [Denial of Services]
These attackers exhaust the computing power, memory capacity or communication bandwidth of their targets so they are unavailable.

Another important classes of attacks is caused by various types of malware.

-> Viruses -> Trojan.

-> Worm -> Spyware.

Virus typically infects a file. So, it spreads from one file to another.

Worms are usually stand-alone program that infects a computer so a worm spreads from one computer to another.

Trojan is a kind of malware which modifies the files, data theft, etc.

Spy-ware installed on a machine can be used to monitor user activities as a key logger to recover valuable info. such as passwords / user keystrokes.

Vulnerability.

Vulnerability in procedures, protocols, h/w or s/w within an organisation that will cause damage.

There are atleast 4 important vulnerability classes in the domain of security, they are

-> Human vulnerabilities. -> Software vulnerabilities.

-> Protocol vulnerabilities. -> Configuration vulnerabilities.

Human vulnerabilities includes human behaviour /action.

Eg: user clicking on the link in a e-mail received from the unknown resources. This type is kalled phishing.

Protocol vulnerabilities includes no. of ~~wor~~ networking protocols including ARP, ACMP, UDP, DNS and various protocols have been used in a anticipated way for attacks.

Eg: Pharming attack is an example. It also leads for man in the middle attack.

Software vulnerabilities is caused by weekly written system code or application s/w which normally happens at the time of user i/p's.

Configuration vulnerabilities relates to configuration settings on newly installed files, etc. By Read/Write executable permissions on files, etc providing privileges on the application, etc.

Different Strategies

Defence Strategies.

1] Access Control → Authentication.
→ Authorisation.

Authentication

Access control is to permit or deny the entry into the system which is called as authentication process. which can be implemented by some of the trusted third party appⁿs/s/w's & also it may be a part of OS to protect the s/m.

Authorisation.

Involves granting a specific entity the permission to access some restricted data or perform some restricted operations

2] Data Protection.

Data confidentiality. & Data Integrity.

Data confidentiality is the protection of data from disclosure to an unauthorised party or process.

Data Integrity, it is a assurance that data hasn't been modified, tampered with or made inconsistent in any way

To perform this data protection some of the cryptographic techniques are used. This is done by encryption & decryption of data for confidentiality & cryptography checksum is used for data integrity.

5] Prevention and detection.

Access control and message encryptions are all of preventing strategies.

Cryptographic checksum on the other hand detects tampering of messages.

The intrusion detection system also looks for certain patterns of behaviour.

Response, recovering, forensic.

Once an attack or infection has been detected response measure should be quickly taken like shutting down all the system or part of the system during a malware infection in which necessary actions should be taken like quarantined and necessary patches are applied.

Cyber forensic is an emerging discipline with a set of tools that helps trace back the criminals of cyber crime.

Guiding Principles.

1→ Security is as much a human problem than a technological problem & must be addressed at different levels.

2→ Security should be factored at inception not as an after thought.

3→ Security ~~by~~ being unknown is often bogus.

4→ Always consider the defult denial policy for adoption in access control.

5→ An entity should be given the least amount of permissions or privileges to accomplish a given task.

6→ Use defence in depth to ~~ens~~ enhance the security of an architectural design.

7. Identify vulnerabilities and respond appropriately.

8. Carefully study the trade of involving security before making any.

Co-prime, Congruency, Relative prime.

MODULO ARITHMETIC.

Let 'd' be an integer & let 'n' be a +ve integer. Let q and r be quotient & remainders obtained by dividing d by n.

Therefore, the relationship b/w d, n, q, r is

$d = (n * q) + r.$

$n = 10 \quad r = 3$

$q = \{0, 1, 2, 3\}$

the set of d values

$\{\ldots -27, -17, -7, 3, 13, 23, 33, \ldots\}$

Congruency modulo.

represented by $r \equiv d \pmod n$

If 2 integers are congruent modulo n then they differ by an integral multiple of n.

$a \bmod n = r \quad b \bmod n = r.$

then, $a = n * q_1 + r.$

$b = n * q_2 + r.$

$a - b = n * q_1 + r - (n * q_2 + r).$

$a - b = n(q_1 - q_2).$

Since q_1 & q_2 are integers a & b differ by an integral multiple of n.

1] $(a+b) \bmod n = ((a \bmod n) + (b \bmod n)) \bmod n$.
2] $(a-b) \bmod n = ((a \bmod n) - (b \bmod n)) \bmod n$.
3] $(a*b) \bmod n = ((a \bmod n) * (b \bmod n)) \bmod n$.

Properties of modulo arithmetic.

→ Verify property-1 for $n = 8$, $a = 27$, $b = 34$.

$(27+34) \bmod 8 = 61 \bmod 8 = \underline{\underline{5}}$.

$(27 \bmod 8) + (34 \bmod 8) = 5 \bmod 8 = \underline{\underline{5}}$.
$\quad 3 + 2$

$\therefore$ LHS = RHS.

GCD

If two integers a & b, if a divides b and a divides c & their exists number $a' > a$ such that a'/b and a'/c, then a is referred to the greatest common divisor of b and c denoted as
$a = \gcd(b, c)$.

If gcd of b, c i.e $\gcd(b,c) = 1$.
(b, c) can be a prime or co-prime or relatively prime.
$\gcd(b,c) = 1$.

Euclid's formula.

$d = (n*q) + r$.

d	n
161	120

$161 = 120(1) + (41)$.
$120 = 41(2) + (38)$.
$41 = 38(1) + (3)$.
$38 = 3(12) + (2)$.
$3 = 2(1) + \boxed{1}$.
$2 = 1(2) + (0)$.
$\gcd = \underline{1}$.

Eg: (56, 15)

$56 = 15(3) + (11)$.
$15 = 11(1) + (4)$.
$11 = 4(2) + (3)$.
$4 = 3(1) + \boxed{1}$.
$3 = 1(3) + (0)$.

Eg: gcd (161, 112)

$161 = 112(1) + 49$
$112 = 49(2) + 14$
$49 = 14(3) + \boxed{7}$ gcd.
$14 = 7(2) + 0$.

Extended Euclid's Algorithm

GCD theorem.

Given integers b and c there exists two integers x & y such that $\boxed{bx + cy = \gcd(b,c)}$

$bx + cy = 1$, if b and c are relatively prime or co prime numbers.

$7 = 49 - 14 * 3$.
$7 = (1)49 - (112 - 49 * 2) * 3$.
$7 = 49 * 7 + 112 * (-3)$. $49 \; (-112 - 1*2)*3$
$= (161 - 112 * 1) * 7 + 112 * (-3)$. $1*49*3*2 - (112*3)$ ($3*2+1$)
$= (161 * 7) + 112 * (-10)$. $49*7 + 112*(-3)$.

$x = 7$.
$y = -10$.

gcd (79, 12)

12 mod 79 = 12.

79 mod 12 = 7.

$79 = 12(6) + (7)$

$12 = 7(1) + (5)$

$7 = 5(1) + (2)$

$5 = 2(2) + \boxed{(1)}$ gcd.

$2 = 1(2) + 0.$

$2 = 5 - 2 * (2).$

$2 = 5 - 2 * 2$

$= (5 - (7 - 5 * 1) * 2.$

$= 5 * (3) + 7 * (-2)$

$= (12 - 7 * 1) * 3 + 7 * (-2).$

$= 12 * 3 + 7 * (-5).$

$= 12 * 3 + (79 - 12 * 6) * (-5).$

$= 12 * 33 + 79 * (-5) *$

$= x = -5$

$y = 33.$

In cryptography, we often need to compute multiplicative inverse modulo prime no's i.e

$b * x + c * y = 1$, Since $c * y$ differs from 1 by an integral multiple of b.

$c * y \equiv 1 \bmod b.$

It follows that y is actually the inverse of c mod b.

To obtain inverse of c mod b we use extended Euclidean algorithm.

The inverse c % b cx mod b. 12 mod 79.

12 mod 79.

12^{-1} mod 79.

$12 * y \equiv 1 \bmod 79.$

$12 * y = 1 * 5 * 79 \bmod 79.$

$12 * y \equiv 1 \bmod 79.$

or.

$* 33 = 1 + 5 * 79 \equiv 1 \pmod{79}$

$33 = 1 \bmod 79.$

$35^{-1} \bmod 6.$

$35 y \equiv 1 \bmod 6.$

$5 y \equiv 1 \bmod 6.$

$25 y \equiv 5 \bmod 6.$

$1 y = 5 \bmod 6.$

$\underline{y = 5}.$

$30^{-1} \bmod 7.$

$30 y \equiv 1 \bmod 7.$

$2 y \equiv 1 \bmod 7$

$8 y \equiv 4 \bmod 7.$

$\boxed{y = 4}.$

$42^{-1} \bmod 5.$

$\cancel{4y}\,2y \equiv 1 \bmod 5.$

$8 y \equiv 1 \bmod 5.$

Chinese Remainder Theorem. [CRT]

Used to solve a set of congruent with one variable but with different modulus which are relatively prime as shown below.

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$\vdots$$
$$x \equiv a_k \pmod{m_k}$$

$$x \equiv 2 \pmod{3}$$
$$x \equiv 3 \pmod{5}$$
$$x \equiv 2 \pmod{7}$$

To solve set of equations, there are few steps

1] Find $M = m_1 \times m_2 \times m_3 \ldots\ldots m_k.$

This is to find the common modulo.

2] Finding $M_1 = \frac{M}{m_1}$, $M_2 = \frac{M}{m_2}$, $M_k = \frac{M}{m_k}$.

3] Finding the multiplicative inverse of ~~$M_1, M_2, \ldots$~~ $M_1, M_2, M_3, \ldots\ldots M_k$ using the corresponding $(m_1, m_2, m_3, \ldots\ldots m_k) = m_1^{-1}, m_2^{-1}, \ldots\ldots m_k^{-1}$.

$$M_1^{-1} \bmod m_1, \quad M_2^{-1} \bmod m_2 \ \ldots\ldots \ M_k^{-1} \bmod m_k.$$

4] $x = (a_1 \times M_1 \times M_1^{-1} + a_2 \times M_2 \times M_2^{-1} + \ldots\ldots + a_k * M_k \times M_k^{-1}) \bmod M$.

$x \equiv 2 \pmod 3$ —— (1)
$x \equiv 3 \pmod 5$ —— (2)
$x \equiv 2 \pmod 7$ —— (3)

$M = 3 \times 5 \times 7 = 105$.

$M_1 = \frac{M}{m_1} = \frac{105}{3} = 35$.

$M_2 = \frac{M}{m_2} = \frac{105}{5} = 21$.

$M_3 = \frac{M}{m_3} = \frac{105}{7} = 15$.

Rough

$35y \equiv 1 \bmod 3$
$2y \equiv 1 \bmod 3$
$y = 2$ $M_1^{-1} = 2$.

$21y \equiv 1 \bmod 5$.
$y = 1$ $M_2^{-1} = 1$.

$15y \equiv 1 \bmod 7$.
$y = 1$ $M_3^{-1} = 1$.

$x = (2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1) \bmod 105$.
$x = (140 + 63 + 30) \bmod 105$.
$x = 233 \bmod 105$.
$x = 23$. —— (1) —— (2) —— (3).

TE Let ~~N~~ $N = 210$ & $n_1 = 5$ $n_2 = 6$, $n_3 = 7$, Compute $f^{-1}(3, 5, 2)$ $x_1 = 3$ $x_2 = 5$ $x_3 = 2$.

$\begin{array}{l} 46 \\ 233 \\ \hline 105 \\ 21 \end{array}$

$x_1 = 3$ $\quad n_1 = 5$ $\quad N = 210$ $\quad f^{-1}(3,5,2).$

$x_2 = 5$ $\quad n_2 = 6$

$x_3 = 2$ $\quad n_3 = 7$

$N_1 = \frac{210}{5} = 42.$

$N_2 = \frac{210}{6} = 35.$

$N_3 = \frac{210}{7} = 30.$

$42y \equiv 1 \bmod 5.$

$35y \equiv 1 \bmod 6.$

$30y \equiv 1 \bmod 7.$

$42y \equiv 1 \bmod 5.$

$2y \equiv 1 \bmod 5.$

$\underline{\underline{y=3}}$ $\quad \underline{\underline{N_1^{-1}=3}}.$

$x = (3 \times 42 \times 3 + \overset{175}{5 \times 35 \times 5} + \overset{120}{2 \times 30 \times 4}) \bmod 210.$

$x = (378 + 875 + 240) \bmod 210.$

$x = 1493 \bmod 210.$

$35y \equiv 1 \bmod 6.$

$5y \equiv 1 \bmod 6.$

$\underline{\underline{y=5}}$ $\quad \underline{\underline{N_2^{-1}=5}}.$

$9^{-1} \bmod 26.$

$9y \equiv 1 \bmod 26.$

$\underline{\underline{y=3}}$ $\quad (27)-(26) = \underline{\underline{1}}$

$30y \equiv 1 \bmod 7.$

$2y \equiv 1 \bmod 7.$

$8y \equiv 4 \bmod 7.$

$\underline{\underline{y=4}}$ $\quad \underline{\underline{N_3^{-1}=4}}.$

Find an integer that have remainder of 3 when divided by 7 and 13. and divisible by 12. using CRT solve.

$x \equiv 3 \bmod 7$

$x \equiv 3 \bmod 13$

$x \equiv 0 \bmod 12$

$M = 7 \times 13 \times 12 = 84 \times 13 = 1092.$

$M_1 = \frac{1092}{7} = 156.$

$M_2 = \frac{1092}{13} = 84.$

$M_3 = \frac{1092}{12} = 91.$

$156y \equiv 1 \bmod 7.$

$2y \equiv 1 \bmod 7.$

$8y \equiv 4 \bmod 7.$

$\underline{y=4}$ $\quad \underline{\underline{M_1^{-1}=4}}$

$84y \equiv 1 \bmod 13$ $\quad\quad$ $91y \equiv 1 \bmod 12$.

$6y \equiv 1 \bmod 13$. $\quad\quad$ $7y \equiv 1 \bmod 12$.

$y = 11$ $\quad\quad$ $\cancel{y=5}$ $\quad$ $\cancel{M_3^{-1}=5}$ $\quad$ $y = 7$ $\quad$ $M_3^{-1} = 7$.

$M_2^{-1} = 11$.

$$x = (3 \times \overset{156}{\cancel{1092}} \times 4 + 3 \times \cancel{1092} \times 84 \times 11 + 0 \times 91 \times 7) \bmod 1092.$$

$x = 4644 \bmod 1092$.

$x = 276$.

Basics of Cryptography.

Cryptography is the science of hiding messages so that only the intended recipient can decipher the received message.

The original msg to be transferred is called plain text. & its hidden version is cipher text.

The process of hiding the original plain text is called encryption.

The process of recovering the original plain text from the cipher text is called decryption.

Encryption involves the use of encryption functions or algorithms denoted by E.

Encryption key (e).

Decryption involves the use of decryption functions or algorithms denoted by D.

Decryption key (d).

$C = E_e(P)$. $\quad$ C = cipher text.

$P = D_d(C)$. $\quad$ P = Plain text.

Secret vs. Public key Cryptography.

The two types of cryptography techniques used are secret key & public key.

Secret key Cryptography.

Both sender & receiver share a common secret for encryption & decryption of message.
i.e (e=d)

This is also referred as symmetric key algorithm.

Public key Cryptography.

Two distinct keys are used i.e encryption key is called public key & decryption key is called private key.

The pub key of a receiver is used for encryption & at the receiving end the private key is used for decryption of message.
i.e pub key & prt key ~~has no any~~ doesn't have any relationship also known as asymmetric key algorithm.

$$C_1 = E_{e.Bpu}(P).$$

$$P = D_{d.Bpr}(C_1).$$

[Later] Types of attacks

The attacker is known as cryptanalysts.

Substitutional Ciphers.

→ **Monoalphabetic Cipher**

The m cipher is used for substituting the alphabets with different alphabets which shifts the letters of one alphabets ~~with~~ against another alphabet to create the secret message which is called as "Caesar Cipher", which was found by an Roman Emperor Julius Caesar.

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 for key = 5

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

The shifting is done by key no. of positions i.e encryption process is cipher text = m+e mod 26.

$C_i = m + e \bmod 26$ m = message.

Decryption process is $m = C_i + d \bmod 26$.

if e=3.

$d = -3 \bmod 26$.

$d = 23$.

Eg: Perform Caesar cipher for a key=3 m = what is the population of Mars?

key = 3.

C =

What is the population of MARS

ZKDW LV WKH SRSXODWLRQ RI PDUV

k=5.

This is a secret message

YMNX NX F XJHWJY RJXXFLJ.

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

→ Polyalphabetic Cipher.

In p cipher the cipher text corresponding to a particular character in the plain text is not fixed.

I] ~~Vigenere Cipher~~.

The plain text is broken into blocks of keyword size (m), the key length or the keyword uses a multidigit key i.e $k_1, k_2, k_3, \ldots, k_m$ on each integers.

The first letter of each block is replaced by the letter k_1 position to its right.
The 2^{nd} letter is replaced by the letter k_2 position to its right & so on.

Eg:

(1) Vigenere Cipher.

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
0	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

Key (MATH)
key :(12,0,19,7)

MAKE IT HAPPEN.
12,0,19,7 12,0 19,7,12,0,19,7.

* MATH MA TH MATH

YADL UAT AHBPAU

Key (04, 19, 3, 22, 7, 12, 5, 11)

WISHING YOU MUCH SUCCESS.

~~ABYD~~

ABYDPZL JSN

To decrypt a vegenere cipher we need to use the key in backward direction to the left.

W	I	S	H	I	N	G	Y	O	U	M	U	C	H	S	U	C	C	E	S	S
4	19	3	22	7	12	5	11	4	19	3	22	7	12	5	11	04	19	3	22	7

ABYDPZL JSN PQJT XFGVHOZ

(2) Hill Cipher.

It is a p cipher, as vegenere cipher the plain text ~~ca~~ is broken into blocks of size m.
where m is a linear eq^n.
the key in hill cipher is an $(m \times m)$ matrix of integers 0 to 25.

Each alphabet is assigned with a numeric value
$A=0, B=1, \ldots \ldots Z=25$.

The relationship b/w block of plain text & its cipher text is expressed by $C_1 = P_1 K_{11} + P_2 K_{21} + \ldots \ldots + P_m \cdot K_{m1}$ mod 26.

~~$C_2 = P_2 k_{21} +$~~

$C_2 = P_1 K_{12} + P_2 K_{22} + \ldots \ldots P_m K_{m2}$ mod 26.

$C_m = P_1 K_{1m} + P_2 K_{2m} + \ldots \ldots P_m K_{mm}$ mod 26.

i.e = $C = P \cdot K$. $K = (m \times m)$ matrix.

K represents a key comprising of $(m \times m)$ square matrix.

At the receiver end, the plain text can be recovered from cipher text using "$P = C \cdot K^{-1}$".

Note : $K \cdot K^{-1}$ = Identity Matrix.
Every time the inverse of matrix doesn't exist if the matrix is random value.

Calculation of Inverse of Matrix.

Consider a in cipher using a block of 2 (m=2) where key = ~~(3, 7, 15, 12)~~ $\begin{bmatrix} 3 & 7 \\ 15 & 12 \end{bmatrix}$.

Perform encryption of plain text HI.
The numerical equivalent of HI is 78.

$C = p.K.$

$$C = \begin{bmatrix} 7 & 8 \end{bmatrix} \begin{bmatrix} 3 & 7 \\ 15 & 12 \end{bmatrix}$$

$$C = \begin{bmatrix} \cancel{15}\,21+120 & 49+96 \end{bmatrix}$$

$$C = \begin{bmatrix} 141 & 145 \end{bmatrix} . \bmod 26.$$

$$(11 \quad 15)$$

$$C = \begin{bmatrix} L & P \end{bmatrix}$$

Decryption process.

$$\cancel{P = C.P.K^{-1}} \qquad K^{-1} = \begin{bmatrix} 10 & 5 \\ 7 & 9 \end{bmatrix}$$

$$P = C.K^{-1}.$$

$$P = \begin{bmatrix} 11 & 15 \end{bmatrix} \begin{bmatrix} 10 & 5 \\ 7 & 9 \end{bmatrix}$$

$$P = \begin{bmatrix} 110+105 & 55+135 \end{bmatrix}$$

$$P = \begin{bmatrix} 215 & 190 \end{bmatrix} \bmod 26.$$

$$P = \begin{bmatrix} 7 & 8 \end{bmatrix}.$$

$$P = \begin{bmatrix} H & I \end{bmatrix}.$$

[OTP] One Time Pad.

It is an encryption technique in which each character of the plain text is combined with a character from a random set of key.

In The (OTP) One Time Pad is that the encryption key has atleast the same length as the actual msg (plain text) & consists of truly random numbers and is not reused.

There are some rules mandatory for OTP

1] The OTP shd consist of truly Random chars.
2] The OTP (key) shd have the same length of the plain text.
3] Only 2 copies of OTP should exist.
4] The OTP shd be used only once
5] Both copies of OTP are destroyed immediately after use.

6]

The key is prior sent to the receiver and the encryption is done.

To encrypt plain text data the sender uses keystream by mixing bit by bit [XOR operation]. Again It is XOR operation performed on decryption to get plain text.

Eg:

A	0 1 1 0 0 1 0 1
key	1 1 0 1 0 1 0 1
	XOR
CT	1011 0000
key	1101 0101 (XOR) Decryption
PT	0110 0101

Hill cipher prob

Perform for a plain text HELP where the block of 2

HELP $m=2$. $\begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}$. H E L P. 7 4 11 15.

$C = p \cdot K$

$= \begin{bmatrix} 7 & 4 \\ 11 & 15 \end{bmatrix}_{2\times2} \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}_{2\times2}$

$= \begin{bmatrix} 7 & 4 \end{bmatrix} \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix} = \begin{bmatrix} 21+8 & 21+20 \end{bmatrix}$

$= \begin{bmatrix} 29 & 41 \end{bmatrix} \bmod 26$.

$= \begin{bmatrix} 3 & 15 \end{bmatrix} = \begin{bmatrix} D & P \end{bmatrix}$

$$\begin{bmatrix} 11 & 15 \end{bmatrix} \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}$$

$$= \begin{bmatrix} 33+30 & \cancel{45}\ 33+75 \end{bmatrix}$$

$$= \begin{bmatrix} 63 & 108 \end{bmatrix} \bmod 26.$$

$$= \begin{bmatrix} 11 & 4 \end{bmatrix}$$

$$= \begin{bmatrix} L & E \end{bmatrix}$$

$= D \quad P \quad L \quad E$

<u>Decryption</u>

$P = CK^{-1}$ $\qquad K^{-1} = \begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix}$

$$= \begin{bmatrix} 3 & 15 \end{bmatrix} \begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix}$$

$$= \begin{bmatrix} 45+300 & 51+135 \end{bmatrix}$$

$$= \begin{bmatrix} 345 & 186 \end{bmatrix} \bmod 26.$$

$$= \begin{bmatrix} 7 & 4 \end{bmatrix}$$

$= H \quad E.$

$\therefore$ H E L P

$$= \begin{bmatrix} 11 & 4 \end{bmatrix} \begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix}$$

$$= \begin{bmatrix} 165+80 & 187+36 \end{bmatrix} \bmod 26.$$

$$= \begin{bmatrix} 245 & 223 \end{bmatrix} \bmod 26.$$

$$= \begin{bmatrix} 11 & 15 \end{bmatrix}$$

$= L \quad P$

Difference b/w Substitution & Transposition Cipher.

In substitution cipher each letter retains its position but changes its identity.
In transposition cipher each letter retains its identity but changes its position.

Transposition Cipher.

TCipher shuffles, rearranges or permutes the bits in a block of plain text.

Row transposition Cipher

In Rt Cipher the plain text is arranged in the form of matrix for a particular fixed column value.
Eg: "Begin operation at NOON".

$$\begin{array}{cccc} 1 & 2 & 3 & 4 \\ \end{array}$$
$$\begin{bmatrix} B & e & g & i \\ n & o & p & e \\ r & a & t & i \\ o & n & a & t \\ N & O & O & N \end{bmatrix} \Rightarrow \begin{bmatrix} r & a & t & i \\ n & o & o & n \\ n & o & p & e \\ b & e & g & i \\ o & n & a & t \end{bmatrix}$$

Now, let's rearrange the rows as follows:
The 1st row is 3rd row.
The 2nd row is 5th row.
The 3rd row is 2nd row.
The 4th row is 1st row.
The 5th row is 4th row.

Now, rearranging the column as follow:
1st - 4th
2nd - 3rd.
3rd - 1st
4 - 2nd

$$\begin{bmatrix} i & t & r & a \\ n & o & n & o \\ e & p & n & o \\ i & g & B & e \\ t & a & o & n \end{bmatrix}$$

. it ra nono epno igBe taon.

Decipher 1

$$\begin{array}{c} \begin{array}{cccc} 1 & 2 & 3 & 4 \end{array} \\ \begin{bmatrix} i & t & r & a \\ n & o & n & o \\ e & p & n & o \\ i & g & B & e \\ t & a & o & n \end{bmatrix} \end{array} \Rightarrow \begin{array}{c} \begin{array}{cccc} 1 & 2 & 3 & 4 \end{array} \\ \begin{bmatrix} i & g & B & e \\ e & p & n & o \\ i & t & r & a \\ n & o & n & o \\ t & a & o & n \end{bmatrix} \end{array}$$

To decrypt the message the recipient would have to cast the cipher text in (5x4) matrix and reverse the column & row shuffle.

In the above technique, the message can be changed by identifying some interesting keywords

Decipher 2.

$$\begin{array}{c} \begin{array}{cccc} 1 & 2 & 3 & 4 \end{array} \\ \begin{bmatrix} i & g & B & e \\ e & p & n & o \\ i & t & r & a \\ n & o & n & o \\ t & a & o & n \end{bmatrix} \end{array} \Rightarrow \begin{array}{c} \begin{array}{cccc} 1 & 2 & 3 & 4 \end{array} \\ \begin{bmatrix} r & a & t & i \\ n & o & o & n \\ n & o & p & e \\ B & e & g & i \\ o & n & a & t \end{bmatrix} \end{array}$$

$$\begin{bmatrix} B & e & g & i \\ n & o & p & e \\ r & a & t & i \\ o & n & a & t \\ n & o & o & n \end{bmatrix}$$

Confusion.

Confusion seeks to make the relationship b/w the statistics of the CTxt and the value of encryption key as complex as possible.

Even if the attacker can get some handle on the statistics of CTxt, the way in which the key was used to produce that CTxt is so complex as to make it difficult to deduce the key.

This is achieved by complex substitution theorem.

Diffusion. [Rearrangement].

In diffusion, the statistical structure of the plaintext is dissipated into long-range statistics of the CTxt.

This is achieved by having each CTxt digit be affected by many Ptxt digits

$$y_n = \left(\sum_{i=1}^{k} m_{n+i}\right) \bmod 26$$

adding k successive letters to get CTxt letter y_n

In a binary block cipher, diffusion can be achieved by repeatedly performing some permutation on the data followed by applying a function to that permutation.

Block Cipher.

It is one in which a block of PTxt is treated as a whole and used to produce a CTxt block of equal length, a block of 64b or 128b is used. A block cipher can be used to achieve the same effect as a stream cipher.

They seem applicable to a broader range of app^ns than stream ciphers.

The majority of N/w based symmetric cryptographic applications make use of block ciphers.

Stream Cipher

It is one that encrypts a digital data stream one bit or one byte at a time.

Eg: Vigenere Cipher.

If the cryptographic keystream is random, then this cipher is unbreakable by any means other than acquiring the keystream.

~~Substitution - Perm~~

Product Cipher ~~combines~~
It is a combination of substitution-permutation box.

Substitution Box is a device that takes i/p string of length m & returns string of length n.
~~and~~ ~~the~~
where m = n is occasional not always.

Data Encryption Stds.
In DES, $\boxed{m > n}$

An S-Box is a easily implemented using a table or array of 2^m rows, each row contains n-bit value.
S-Box has no restrictions.

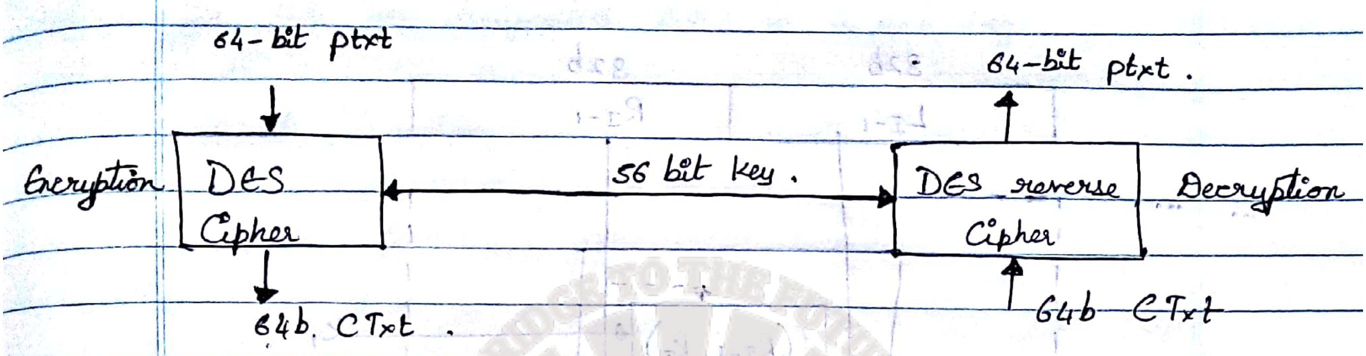
Permutation Box performs permutation or rearrangement of bits in the i/p.

Permutation is more restricted than ~~diffusion~~ substitution.

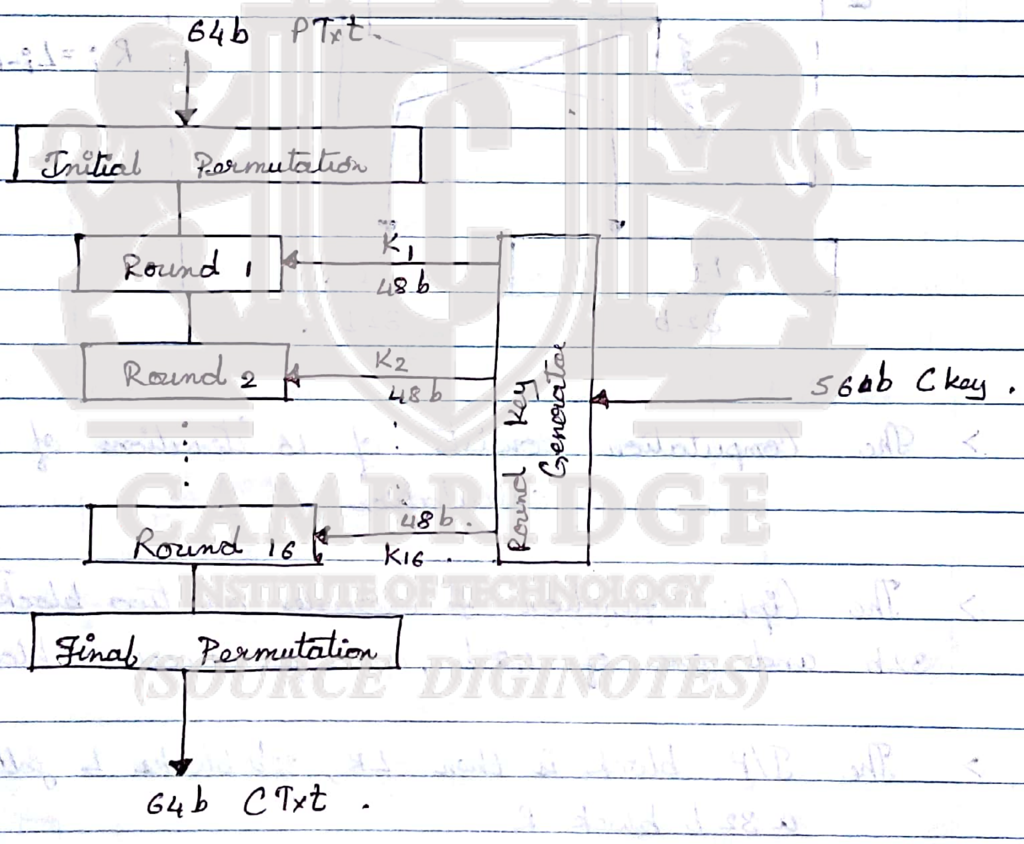
Cascading P-Box & S-Box alternatively the strength of the cipher can be greatly increased.
This concept is called product cipher.

DES.

Key: ~~64 bit~~ 56 bit key.



General Structure of DES.

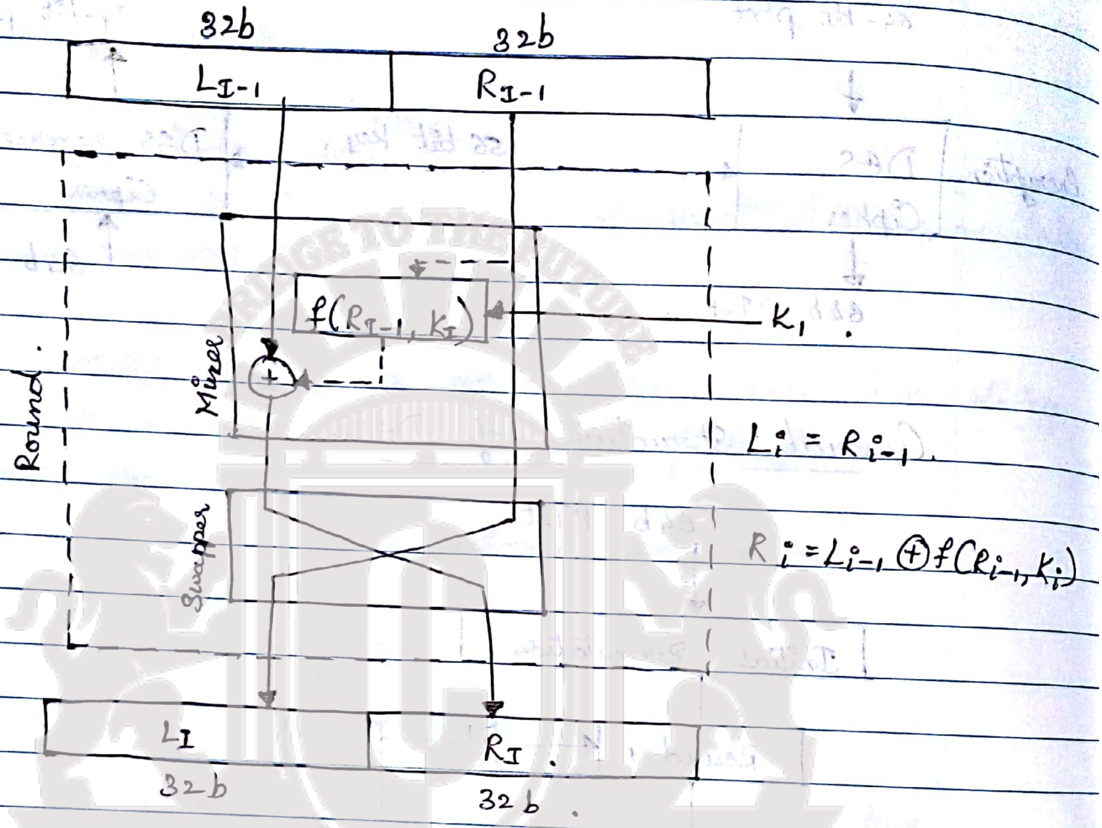


Feistel Cipher Structure.

Implements Shannon's S-P n/w concept where a single block of PTxt is transformed into CTxt after passing through the foll. stages.

- partitions i/p block into two halves.
- An initial permutation.

- 16 rounds of a given function.
- A 32b left-right swap and.
- A final permutation.



> The Computation consists of 16 iterations of a calculation

> The Cipher Function f operates on two blocks, one of 32b and one of 48 b, and produces a block of 32 b

> The I/P block is then LR, 32b blocks L followed by a 32 b block R

Let L_{i-1} & R_{i-1} be the left and right halves of the i/p to round i.

$$L_i = R_{i-1}.$$
$$R_i = L_{i-1} \oplus f(R_{i-1}, K_i).$$

> The function f is applied at each round is referred as the "Round Function".

> At each iteration a diff block of key K bits is chosen from the 64b key designated KEY to a 48b key.

Round Function.

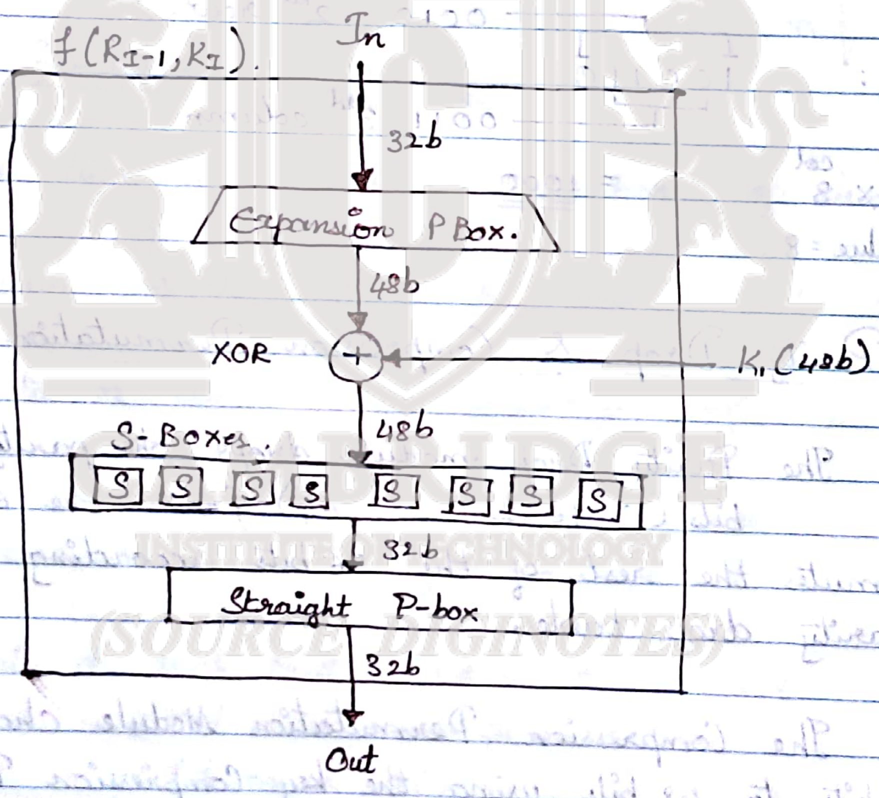
Four operations.

> Expansion.

> XOR with round key.

> Substitution.

> Permutation.



Each S box uses a corresponding 4 row x 16 column table i.e 8 tables. [n^{2n} array]. 2^4

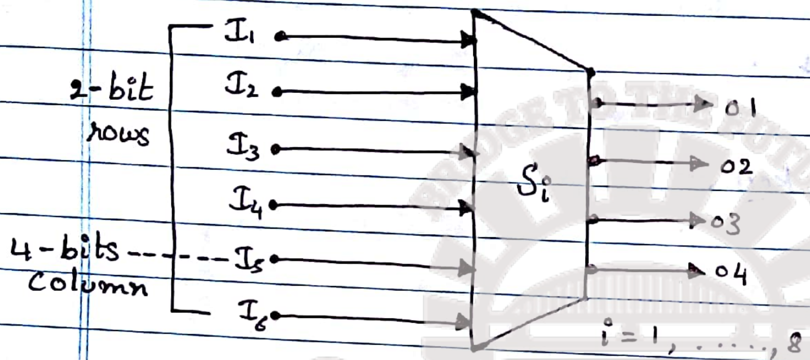
Given a 6 bit i/p, the 1^{st} and 6^{th} bits are used to address one of the rows and the remaining 4 bits are used to address one of the 16 columns.

Finally, the value found in the corresponding location of the table is the 4-bit o/p of the S box.

Substitution Box. [Substitution and Shrink]

48 bits ⇒ 32 bits. [$8 * 6 \Rightarrow 8 * 4$].

2 bits used to select amongst 4 substitutions for the rest of the 4 bit quantity.



Eg: 100110

0010 2^{nd} row.

0011 3^{rd} column.

row col
2 x 3

= $\underline{\underline{1000}}$

value = 8.

Parity Drop & Compression Permutation

The Parity Drop module drops the parity bits bits (8, 16, 24, ..., 64) from the 64-bit key & permutes the rest of the 56 bits according to the parity drop table.

The Compression Permutation Module changes the 56 bits to 48 bits using the key Compression Table, which are used as the key for a round.

~~Prbtis~~