4.1.22

Network security → measure to protect data during transmission.

Internet Security → " over collection of interconnected networks

Healthcare, Education, Banking, s/w, Marketing, shopping.

Banking → user credentials → DBC 123 → encrypted version → Database

↳ cryptography.

* Gmail information → encrypted information. (Google data center)

* Whatsapp → encrypted mode of sharing.

Cryptography:

→ method of transmitting secured data communication in such a way that only the destinated person knows about the actual information which is transmitted.

Ex:

person1 —"help"→ person2 ✓

1-1 U

x P4 x P5 P6 x P3 x

h → 1
e → -
l → 1
p → U

only person2 can decrypt the message.

Flow:

Plain text → Encryption → Cipher text → decryption → Plain text

Readable

h → 1
e → -
l → 1
p → U

Non-readable

1 → h
- → e
1 → l
U → p

readable

06th Jan, 2022:

→ Cipher → algorithm for transforming PT to CT

→ Key → Information used in cipher that is only known by sender & reciever

→ Encipher → (encryption) process of converting PT to CT

→ Decipher → (Decryption) process of converting CT to PT

→ Cryptanalysis → Study of methods of deciphering CT without knowing actual key.

→ Cryptology → Domain of cryptography & cryptanalysis.

→ Cryptography → Study of encryption principles & methods

Types:

i) Symmetric cryptography
ii) Asymmetric cryptography
iii) Hash functions

Sym: Same key used by both sender & reciever.
also called as private key cryptography.
Algorithms: * DES
* AES
* IDEA

Asym: (PKCrypt) different keys. (private & public key)
Algorithms: * RSA
* Eliptic curve

If private for Encryp → then public is for Decryption (vice-versa)

Hash: Once Encrypted, can't get original message
used for checking whether message is sent/not.
Algorithms: * SHA
* MD5 (message Digest)

main Application → (maintain secracy in the message transformations) of Cryptographies

Ex: whatsapp: end-to-end encrypted (Asymetric cryptography)

crypt in: (real life usages)

→ secure communication

* HTTPS (secured hyper text)

* Bluetooth, GSM (Global sys for mobile communication), 802.11i WPA2 (WEP)

→ User authentication

→ Encrypting files on Disk (EFS, Truecrypt)

→ Content protection (CSS, AACS → Alg for protection Blueray movies to get encrypted)

Secure Socket Layers/TLS:

* Handshake protocol: Establishing shared secret key using Public-key cryptography (Generation)

* Record Layer: Transmit data using shared secret key (transmission)

→ Ensuring confidentiality & Integrity.

Crypt follows CIA traid: confidentiality, Integrity, Availability

11th Jan 2022:

→ confidentiality: Person → personal details → company → need to maintain confidentiality.

→ Data confidentiality:
Assuring private/confidential is not made available.

→ privacy:

→ Integrity:

→ Data Integrity: Assuring info & pgm are changed only in a specified manner.

→ System Integrity:

→ Availability: system works promptly

OSI Security Architecture:

→ used to provide security services.

→ focuses on:

i) Security attack (Action that compromises security)

→ diff attacks takes place on data during transmission

→ tackling

ii) Security service (tech to overcome attack)

iii) security mechanism (implement those service we use mechanism)

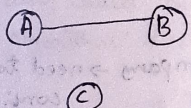
(Detect, prevent, recover from a security attack)

→ Security attack:

i) Passive attack

ii) Active attack

PA:



↓ unauthorised user / attacker

observe the data, how it is transfered & collect the information

(no modification will be done here)

AA: Here, C will modify data

Types of PA:

i) Release of message contents C → observer

Ex: phone tapping (just listening)

~~Traffic analysis~~

ii) Traffic Analysis

A → B (will be encrypted message)

Network may be public.

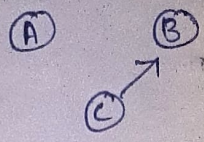
C → observe pattern of message, length, freq of message, location of the communication channel

Types of AA :

i) masquerade

Before A sends, C send to B as if A has sent.

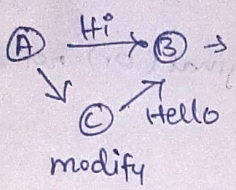
Instead of recieving original, recieved got from attacker



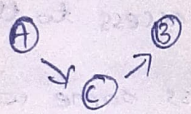
ii) Replay :

C observe & modify and send to reciever.

reciever will be in confused state.



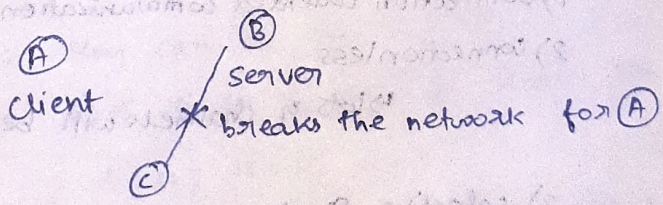
iii) Modification of message :



Get from sender & modified it to B

iv) Denial of service :

C break the network of the server providing service



AA :

→ Hard to prevent
→ physical, S/w and network vulnerabilities
→ Detect and recover from any disruptions/delays.
→ If detection has deterrent effect, it may also contribute to prevtn.

PA :

→ Neither sender nor reciever can know
→ hard to detect.
→ Encryption can reduce.
→ more emphasis on prevention than detection.

Security Service : implements security policies.

i) Authentication

→ to ensure that communication is authentic b/w sender & reciever.

→ two types:

* peer to peer authn.

* Data origin authn.

PP:

Peer → Entity

Authn each entity before transmission. Checking Ⓐ, Ⓑ

DO :

check data first, whether it is original (or) not.

checking source of data

ii) Access control:

→ ability to limit & control the access to the system.

Ex: Bank Manager can access some where employees can't

iii) Data confidentiality

more useful to prevent passive attack.

Sevices provided for

1) connection oriented communication Ⓐ —— Ⓑ

2) connectionless

↳ lots of channels will be there

Ⓐ Ⓑ

3) selective field

4) Traffic field/flow (observe source of data & provide security)

iv) Data Integrity: (Assure Reciever gets the sender's message)

v) Non repeadiation

Ⓐ Ⓑ

Ⓐ → should prove as actual sender.

Ⓑ → should prove as actual reciever.

Characteristics:

→ type of operations used for encrypt, decrypt

i) substn: Each element in plain text is mapped into another element.

ii) transposition: Each element in plain text are rearranged.

→ No. of key used

i) Symmetric (1 key)

ii) Assymetric (2 key → Priv, Pub)

→ way in which plain text is processed

i) block cipher

ii) stream

Substn: Caesar cipher, Monoalphabetic, playfair, Hill, polyalphabetic, one-Time pad

Transposition: Rail Fence, Row column Transposition

Caesar cipher:

→ Each alphabet replaced with alphabet + 3

a => D

b => E

Plain text → a p p l e

Cipher text → d s s o h

Key => 3

Monoalphabetic: Key can be any number.

Both Sender & reciever knows the key.

K = 3 ; K = 4 ; K = 7 ; ...

Then alphabet + K => Cipher text.

Cryptanalyst will be watching.

Security mechanism: implement security policies by services.

→ process to detect/prevent the messages from unauthorized access.

protocol → X.500 standard

↙ Specific protocol layers

↘ non-specific protocol layer / pervasive security mechanism

Specific security mechanism:

→ Encipherment

→ Digital signature (information + signature of sender)

→ Access control

→ Data Integrity (Assurance for original data)

→ Authentication

→ Traffic padding (Gaps in the data will be filled, while Ⓒ doesn't know which is real data, but Ⓑ does)

→ Routing control

→ Notarization (selecting a 3rd trusted party to control communication b/w two entities)
(keeps record of requests made by sender to reciever for later denial)

Pervasive security mechanism:

→ Trusted functionality

→ Security label

→ Event deduction (security related issues should be detected)

→ Security recovery

→ security audit trail (Periodic review of transmissions in data, about data → personal, security reasons)

Hill cipher : 1929, Lester Hill

a → 0
b → 1
⋮
z → 25

→ select a message to encrypt.

i) welcome

let n = 2 ; we|lc|om|ea

→ select a key.

If n = 2, then key should be 2×2 matrix, leng(key) = 4

If n = 3, then key should be 3×3 matrix, len(key) = 9

Ex: key = test [4 in length]

$$\text{key} = \begin{bmatrix} t & e \\ s & t \end{bmatrix} \Rightarrow \text{key} = \begin{bmatrix} 19 & 4 \\ 18 & 19 \end{bmatrix}$$

a → 0
b → 1
c → 2
d → 3
e → 4
f → 5
g → 6
h → 7
i → 8
j → 9
k → 10
l → 11
m → 12
n → 13
o → 14
p → 15
q → 16
r → 17
s → 18
t → 19
u → 20
v → 21
w → 22
x → 23
y → 24
z → 25

→ each pair into component vector, then numerical value

$$\begin{pmatrix} w \\ e \end{pmatrix} \Rightarrow \begin{pmatrix} 22 \\ 4 \end{pmatrix} \quad \begin{pmatrix} l \\ c \end{pmatrix} \quad \begin{pmatrix} o \\ m \end{pmatrix} \quad \begin{pmatrix} e \\ a \end{pmatrix}$$

$$\downarrow \qquad \downarrow \qquad \downarrow$$

$$\begin{pmatrix} 11 \\ 2 \end{pmatrix} \quad \begin{pmatrix} 14 \\ 12 \end{pmatrix} \quad \begin{pmatrix} 4 \\ 0 \end{pmatrix}$$

cipher text ⇒ K * P mod 26 ⇒ $k * \begin{pmatrix} w \\ e \end{pmatrix} \bmod 26$

$$\begin{bmatrix}19 & 4\\ 18 & 19\end{bmatrix}\begin{bmatrix}22\\ 4\end{bmatrix} \bmod 26 \Rightarrow \begin{bmatrix}434\\ 472\end{bmatrix} \bmod 26 \Rightarrow \begin{bmatrix}18\\ 4\end{bmatrix}$$

$$\Rightarrow \begin{bmatrix}18\\ 4\end{bmatrix} = \begin{bmatrix}s\\ e\end{bmatrix}$$

$$\begin{bmatrix}19 & 4\\ 18 & 19\end{bmatrix}\begin{bmatrix}11\\ 2\end{bmatrix} \bmod 26 \Rightarrow \begin{bmatrix}217\\ 236\end{bmatrix} \bmod 26 \Rightarrow \begin{bmatrix}9\\ 2\end{bmatrix} \Rightarrow \begin{bmatrix}j\\ c\end{bmatrix}$$

$$\begin{bmatrix}19 & 4\\ 18 & 19\end{bmatrix}\begin{bmatrix}14\\ 12\end{bmatrix} \bmod 26 \Rightarrow \begin{bmatrix}314\\ 480\end{bmatrix} \Rightarrow \begin{bmatrix}2\\ 12\end{bmatrix} \Rightarrow \begin{bmatrix}c\\ m\end{bmatrix}$$

$$\begin{bmatrix}19 & 4\\ 18 & 19\end{bmatrix}\begin{bmatrix}4\\ 0\end{bmatrix} \bmod 26 \Rightarrow \begin{bmatrix}76\\ 72\end{bmatrix} \Rightarrow \begin{bmatrix}24\\ 20\end{bmatrix} \Rightarrow \begin{bmatrix}y\\ u\end{bmatrix}$$

cipher => sejcmyu

Decryption:

Plain text => $K^{-1} C \bmod 26$

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

$|K| \Rightarrow 289$

Finding multiplicative inverse:

$289x \bmod 26 = 1$ $\qquad$ $289 \bmod 26 \Rightarrow 9$

$\Rightarrow 3x \bmod 26 = 1$

$\Rightarrow 3 \times 9 \bmod 26 = 1$ (condition satisfied)

$\therefore x = 9$ $\qquad$ when $x = 9 \Rightarrow 27 - 1 \cdot 26 = 1$

$$\frac{1}{|K|} = 9$$

compute adj(K)

$K = \begin{bmatrix} 19 & 4 \\ 18 & 19 \end{bmatrix} \Rightarrow adj(K) = \begin{bmatrix} 19 & -4 \\ -18 & 19 \end{bmatrix}$

$K^{-1} = 9 \begin{bmatrix} 19 & -4 \\ -18 & 19 \end{bmatrix} \Rightarrow 9 \begin{bmatrix} 19 & 22 \\ 8 & 19 \end{bmatrix} \Rightarrow \begin{bmatrix} 171 & 198 \\ 72 & 171 \end{bmatrix}$

$\begin{bmatrix} 171 & 198 \\ 72 & 171 \end{bmatrix} \begin{bmatrix} 18 \\ 4 \end{bmatrix} \bmod 26 \Rightarrow \begin{bmatrix} 3960 \\ 1980 \end{bmatrix} \bmod 26 \Rightarrow \begin{bmatrix} 22 \\ 4 \end{bmatrix}$

$\begin{bmatrix} 171 & 198 \\ 72 & 171 \end{bmatrix} \begin{bmatrix} 11 \\ 2 \end{bmatrix} \bmod 26 \Rightarrow \begin{bmatrix} 2277 \\ 1134 \end{bmatrix} \bmod 26 \Rightarrow \begin{bmatrix} 15 \\ 16 \end{bmatrix}$

$\begin{bmatrix} 171 & 198 \\ 72 & 171 \end{bmatrix} \begin{bmatrix} 14 \\ 12 \end{bmatrix} \bmod 26 \Rightarrow \begin{bmatrix} 4770 \\ 3060 \end{bmatrix} \bmod 26$

$\begin{bmatrix} 171 & 198 \\ 72 & 171 \end{bmatrix} \begin{bmatrix} 4 \\ 0 \end{bmatrix} \bmod 26 \Rightarrow \begin{bmatrix} 684 \\ 72 \end{bmatrix} \bmod 26$

22 Jan :

$15x + 26y = \gcd(15, 26)$

$a = bq + r$

$26 = 15 \times 1 + 11 \Rightarrow 26 = 1 \times 15 + 11$

$15 = 1 \times 11 + 4$

$11 = 2 \times 4 + 3$

$4 = 1 \times 3 + 1$

$3 = 3 \times 1 + 0$

$\gcd(15, 26) = 1$

Step : 2

$\Rightarrow 4 = 1 \times 3 + 1 \quad \Rightarrow \quad 1 = 4 - 1 \times 3$

$= 4 - 1 \times (11 - 2 \times 4)$

$= 4 - (1 \times 11) + (2 \times 4)$

$= (1 * 4) - (1 * 11) + (2 * 4)$

$= (3 * 4) - (1 * 11)$

$= (3 * 4) + (-1 * 11)$

$= (3 * 15 - (1 * 11)) + (-1 * 11)$

$= 3 * (15 - (1 * 11) - 11$

$= (3 * 15) - (3 * 11) - 11$

$= (3 * 15) - (3 * 11) + (-1 * 11)$

$= (3 * 15) - (4 * 11)$

$= 3 * 15 - 4 * (26 - 1 * 15)$

$= (3 * 15) - (4 * 26) + (4 * 15)$

$= (7 * 15) - (4 * 26)$

$1 = (15 * 7) + (26 * -4)$

$15x + 26y$

$\therefore x = 7 \; ; \; y = -4$

① $1914x + 899y = \gcd(1914, 899) \rightarrow x = 33;\ y = -14$

② $93x + 219y = \gcd(93, 219) \rightarrow x = 8;\ y = -17$

①

$1914 = 899 \times 2 + 116$

$= 2 \times [899 + 116]$

$\Rightarrow 899 = 7 \times 8 [116 + 87]$

$116 = 1 \times 87 + 29$

$87 = 3 \times 29 + 0$

$\gcd(1914, 899) = 29$

$\Rightarrow 116 = 1 \times 87 + 29$

$\Rightarrow 29 = 116 - 1 * 87$

$= 116 - 1 * (899 - 7 * 116)$

$= 116 - 1 * 899 + (7 * 116)$

$= (8 * 116) - (1 * 899)$

$= 8 * (1914 - 2 * 899) - (1 * 899)$

$= 8 * 1914 - (16 * 899) - (1 * 899)$

$29 = 8 * 1914 - (17 * 899)$

$\Rightarrow 1914x + 899y = \gcd(1914, 899)$

$\boxed{x = 8;\ y = -17}$

$899 \overline{)1914} \quad 2$

1798

$116 \overline{)899} \quad 7$

812

87

② $93x + 219y = \gcd(93, 219)$

$$93 \overline{)219}\ 2$$
$$186$$
$$33$$

$\Rightarrow 219 = 93 \times 9 + r$

$\Rightarrow 219 = 2 \times 93 + 33$

$93 = 2 \times 33 + 27$

$33 = 1 \times 27 + 6$

$27 = 4 \times 6 + 3$

$6 = 2 \times 3 + 0$

$\boxed{\gcd(93, 219) = 3}$

$27 = 4 * 6 + 3$

$= 4 * (33 - 1 * 27) + 3$

$= (4 * 33) - (4 * 27) + 3$

$= (4 * 33) - 4 * (93 - 2 * 33) + 3$

$= (4 * 33) - (4 * 93) + (8 * 33) + 3$

$= (12 * 33) - (4 * 93) + 3$

$= 12 * (219 - 2 * 93) + 3 - (4 * 93)$

$= (12 * 219) - (24 * 93) + 3 - (4 * 93)$

$27 = 4*6 + 3$

$\Rightarrow 3 = 27 - 4*6$

$= 4*6 - 27$

$= 4*6 - (93 - 2*33)$

$= 4*6$

$\Rightarrow 27 = 4*6 + 3$

$3 = 27 - 4*6$

$= 27 - 4*(33 - 1*27)$

$= 27 - (4*33) + (4*27)$

$= (5*27) - (4*33)$

$= 5*(93 - 2*33) - (4*33)$

$= (5*93) - (10*33) - (4*33)$

$= (5*93) - (14*33)$

$= (5*93) - 14*(219 - 2*93)$

$= (5*93) - (14*219) + (28*93)$

$= -(14*219) + (33*93)$ $\Rightarrow x = 33$, $y = -14$

$\Rightarrow (93 - 2*33) - (4*33) + (4*27)$

$\Rightarrow (93 - 2*33) - (4*33) + 4*(93 - 2*33)$

25th Jan:

Congruence: If a, b are integers. And n > 0.

$a \equiv b \bmod n \Rightarrow n \mid (a-b)$

If $\frac{n}{a} \Rightarrow b$

Example: 15, 3 $\Rightarrow 15 \equiv 3 \bmod 12$

$\Rightarrow \frac{12}{15-3} \Rightarrow \frac{12}{12} \Rightarrow 1$

Modular arithmetic property:

i) $(a+b) \bmod n = [(a \bmod n) + (b \bmod n)] \bmod n$

(expand mod n until Left value is less than n)

ii) $(a-b) \bmod n = [(a \bmod n) - (b \bmod n)] \bmod n$

iii) $(a*b) \bmod n = [(a \bmod n) * (b \bmod n)] \bmod n$

Modular Exponentiation:

① Compute $3^{10} \bmod 5$

$3^2 \bmod 5 \Rightarrow 9 \bmod 5 = 4$

$3^4 \bmod 5 \Rightarrow 3^{2+2} \bmod 5$

$\Rightarrow 3^2 \cdot 3^2 \bmod 5 \Rightarrow [(3^2 \bmod 5) * (3^2 \bmod 5)]$

$\Rightarrow [4 * 4] \Rightarrow 16 > 5$

Perform mod 5

$\Rightarrow 16 \bmod 5 \Rightarrow 1 < 5$ //

$x^{a+b} = x^a \cdot x^b$

$(x^a)^b = x^{ab}$

$3^8 \bmod 5 \Rightarrow 3^4 \cdot 3^4 \bmod 5$

$\Rightarrow [(3^4 \bmod 5) * (3^4 \bmod 5)]$

$\Rightarrow [1 * 1] \Rightarrow 1 < 5$

$\Rightarrow 3^{10} \bmod 5 \Rightarrow 3^8 \cdot 3^2 \bmod 5$

$\Rightarrow [(3^8 \bmod 5) * (3^2 \bmod 5)]$

$\Rightarrow [1 * 4] \Rightarrow 4 < 5$

② $3^{20} \bmod 5$

③ $2^{34} \bmod 5$

Fermat's Theorem: (Fermat's little theorem)

→ used in public key cryptography.

→ Let p be prime number, 'a' is a +ve integer not divisible by p. and $\gcd(a, p) = 1$

then $a^{p-1} \equiv 1 \bmod p$

(a, p) → relatively prime (no common factors other than 1) [coprime]

$$\Rightarrow \frac{a^p}{a} \equiv 1 \bmod p \Rightarrow a^p \equiv a \bmod p$$

→ Acc. to congruence rule, $a \equiv r \bmod b$ [b/a, rem = r]

$$a^{p-1} = 1 \bmod p \Rightarrow 1$$

$$a^p = a \bmod p \Rightarrow a$$

① $3^{20} \bmod 5$

$\Rightarrow 3^2 \bmod 5 \Rightarrow 9 \bmod 5 = 4$

$3^4 \bmod 5 \Rightarrow 3^2 \cdot 3^2 \bmod 5 \Rightarrow [(3^2 \bmod 5) * (3^2 \bmod 5)]$

$\Rightarrow [4 * 4] \Rightarrow 16 > 5$

$\Rightarrow 16 \bmod 5 \Rightarrow 1$

$3^8 \bmod 5 \Rightarrow 3^4 \cdot 3^4 \bmod 5 \Rightarrow [(3^4 \bmod 5) * (3^4 \bmod 5)]$

$\Rightarrow [1 * 1] \Rightarrow 1$

$3^{10} \bmod 5 \Rightarrow (3^8 \cdot 3^2 \bmod 5) \Rightarrow [(3^8 \bmod 5) * (3^2 \bmod 5)]$

$\Rightarrow [1 * 4] \Rightarrow 4$

$3^{20} \bmod 5 \Rightarrow 3^{10} \cdot 3^{10} \bmod 5 \Rightarrow [(3^{10} \bmod 5) * (3^{10} \bmod 5)]$

$\Rightarrow [4 * 4] \Rightarrow 16 \bmod 5$

$\Rightarrow 1$

② $2^{34} \bmod 5$

$\Rightarrow 2^4 \bmod 5 \Rightarrow 16 \bmod 5 \Rightarrow 1$

$\Rightarrow 2^8 \bmod 5 \Rightarrow 2^4 \cdot 2^4 \bmod 5 \Rightarrow [(2^4 \bmod 5) * (2^4 \bmod 5)] \Rightarrow [1 * 1] \Rightarrow 1$

$\Rightarrow 2^{16} \bmod 5 \Rightarrow [(2^8 \bmod 5) * (2^8 \bmod 5)] \Rightarrow [1 * 1] \Rightarrow 1$

$\Rightarrow 2^{32} \bmod 5 \Rightarrow 2^{16} \cdot 2^{16} \bmod 5 \Rightarrow [(2^{16} \bmod 5) * (2^{16} \bmod 5)]$

$\Rightarrow [1 * 1] \Rightarrow 1$

$\Rightarrow 2^{34} \bmod 5 \Rightarrow 2^{32} \cdot 2^2 \bmod 5 \Rightarrow [(2^{32} \bmod 5) * (2^2 \bmod 5)]$

$\Rightarrow [1 * 4] \Rightarrow 4$

$2^2 \bmod 5 \Rightarrow 4 \bmod 5 \Rightarrow 4$

29th Jan

compute $5^{18} \bmod 19$

19 → Prime number

g(5,19) should be equal to 1

Finding whether 5 divides 19 $\Rightarrow 19/5$

$\Rightarrow a^{p-1} \bmod p$

$a^{p-1} = 1 \bmod p \Rightarrow \boxed{a^{p-1} \bmod p = 1}$ → fermet's theorom

$\Rightarrow 5^{19-1} \bmod 19$

$\Rightarrow 5^{18} \bmod 19 \Rightarrow 1$

$a^p = a \bmod p \Rightarrow \boxed{a^p \bmod p = a}$ → fermet's theorom

$5^{19} \bmod 19 \Rightarrow 5$

$5 = 5$

$5^{20} \bmod 19$

write power in multiples of P.

$20 \Rightarrow 19 * 1 + 1 \quad \rightarrow a = bq + r$

$5^{20} \bmod 19 \Rightarrow 5^{19*1+1} \bmod 19$

$\Rightarrow ((5^{19})^1 * 5^1) \bmod 19$

$\Rightarrow (5^{19} \bmod 19) * 5 \bmod 19$

$\Rightarrow [5 * 5] \bmod 19$

$\Rightarrow 25 \bmod 19 \Rightarrow 6$

ompute $9^{794} \bmod 73$

3 → prime number

cd(9,73) should be 1

794 > 73

$794 \bmod 73 \Rightarrow 9^{73*10+64} \bmod 73$

$\Rightarrow (9^{73})^{10} \times 9^{64} \bmod 73$

$\Rightarrow (9^{73} \bmod 73)^{10} * (9^{64} \bmod 73)$

$\Rightarrow$ ~~$(9^{1 \text{ to } 10}) * 64$~~ $\Rightarrow 9^{10} * (9^{64} \bmod 73)$

$\Rightarrow 9^{74} \bmod 73$

$\Rightarrow 9^{73*1+1} \bmod 73$

$\Rightarrow (9^{73})^1 . 9^1 \bmod 73$

$\Rightarrow (9^{73} \bmod 73) * (9 \bmod 73)$

$\Rightarrow 9 * 9 \Rightarrow 81 \bmod 73 \Rightarrow 8 //$

1st Feb

use of Symmetric : older method.

→ faster & more efficient, takes toll on network due to perf

→ Examples :

* DES (Data Encryption Standard)
* AES (Adv. Enc. Std)
* RC4, RC5, RC6
* IDEA (Internation Data Enc. A)
* Blowfish

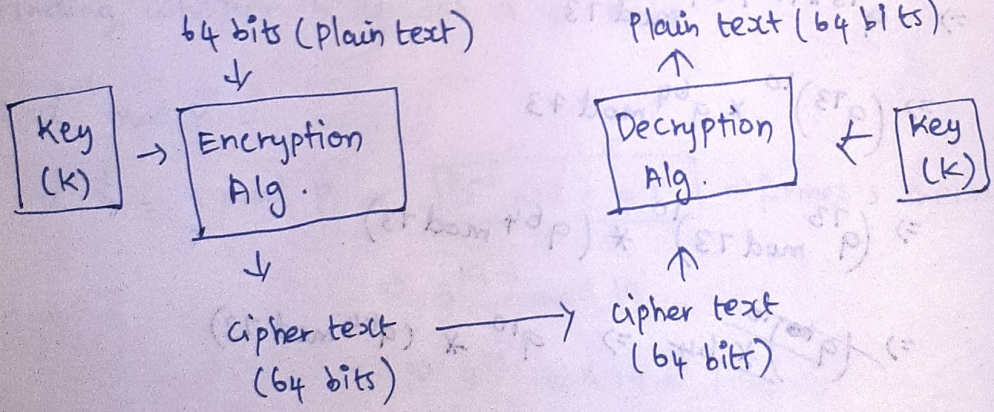
RC4 → Stream cipher
others → Block cipher

Public key → Known to everyone.

private key → only to the reciever.

BLOCK CIPHER :

→ data blocks from plain text.
↳ same size (fixed)
↳ 64 bits / 128 bits



Ex:

HelloVITwelcome!

1st 8 bit → HelloVIT

2nd 8 bit → welcome!.

Step 2: convert to hexadecimal character of 16. (8 X 2) → L4A1F3F...)

Step 3: Each hexadecimal value to binary (in 4 bits)

Ex: A → 1010

1 → 0001

4 → 0100

F → 1111

So totally, 64 bits will be generated (16 X 4)

↳ Single ~~bits~~ block.

↳ input to encryption algorithm.

Ex: WelcomeToVIT

8 bits → 16 bit Hexad → 64 bit binary

4 bits → 8 bits Hexad → 32 bit binary + 32 bit binary zeros → 64 bit binary.

Principles:

→ # of rounds

→ Design of Funution F

→ key schedule Algorithm

Modes of operation:

ECB (Electronic codebook)

CBC (cipher block

CFB

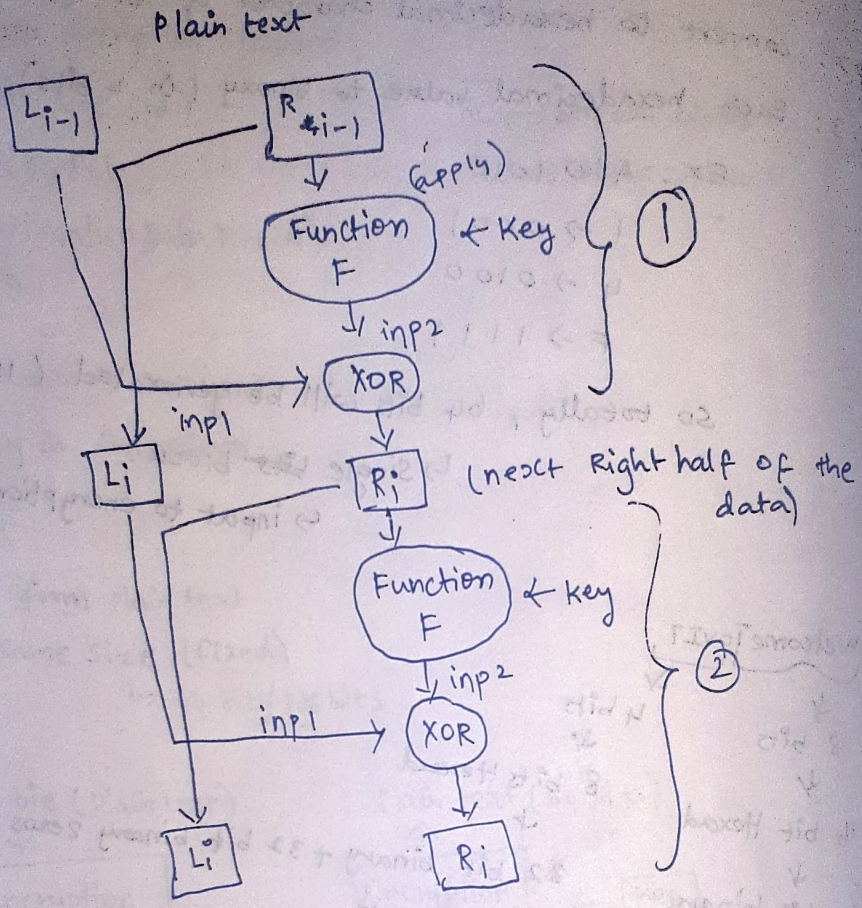
OFB

CTR

Feistel Block Cipher:

-) Structure that implements substitution & permutation.

↳ implements alternatively.



$L_i \Rightarrow R_{i-1}$

$R_i \Rightarrow L_{i-1}$ XOR (function (R_{i-1}, Key))

Parameters:

No. of rounds ↑ then complexity ↑ security also ↑

↳ Normally 16 rounds.

Block size ↑ then security ↑ but encryp & decryp ↓

Key size ↑ security ↑ complexity ↑

Subkey → differs round to round

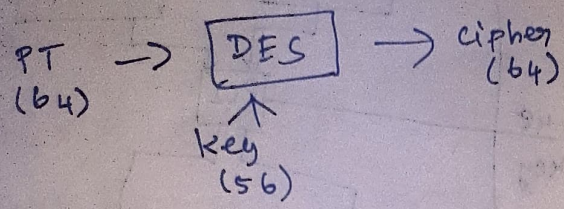
DES:

Block size → 64 bits

key size → 64 bits should be but 56 bits

rounds → 16

16 Intermediate keys each 48 bits



64 bit plain text

↳ gives to initial permutation. → 64 bit to Round 1

First bit of output → 58th of inp

50th of inp

7th of inp

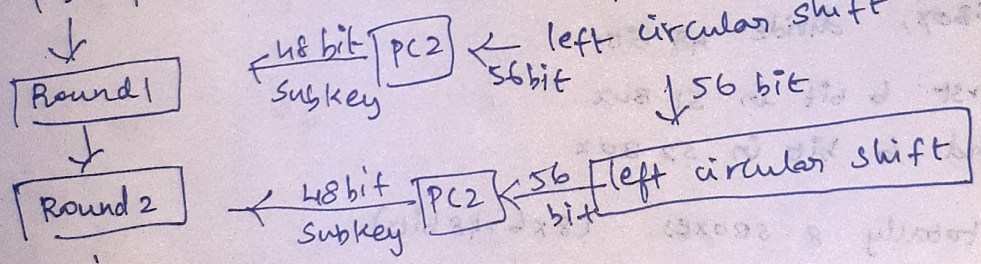
64 bit Key → input to → permutated choice - 1

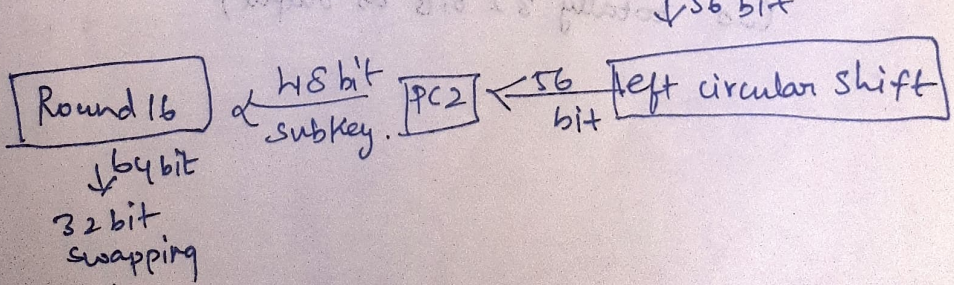
PC 1

↓

56 bit key

64 bit plain text after PC



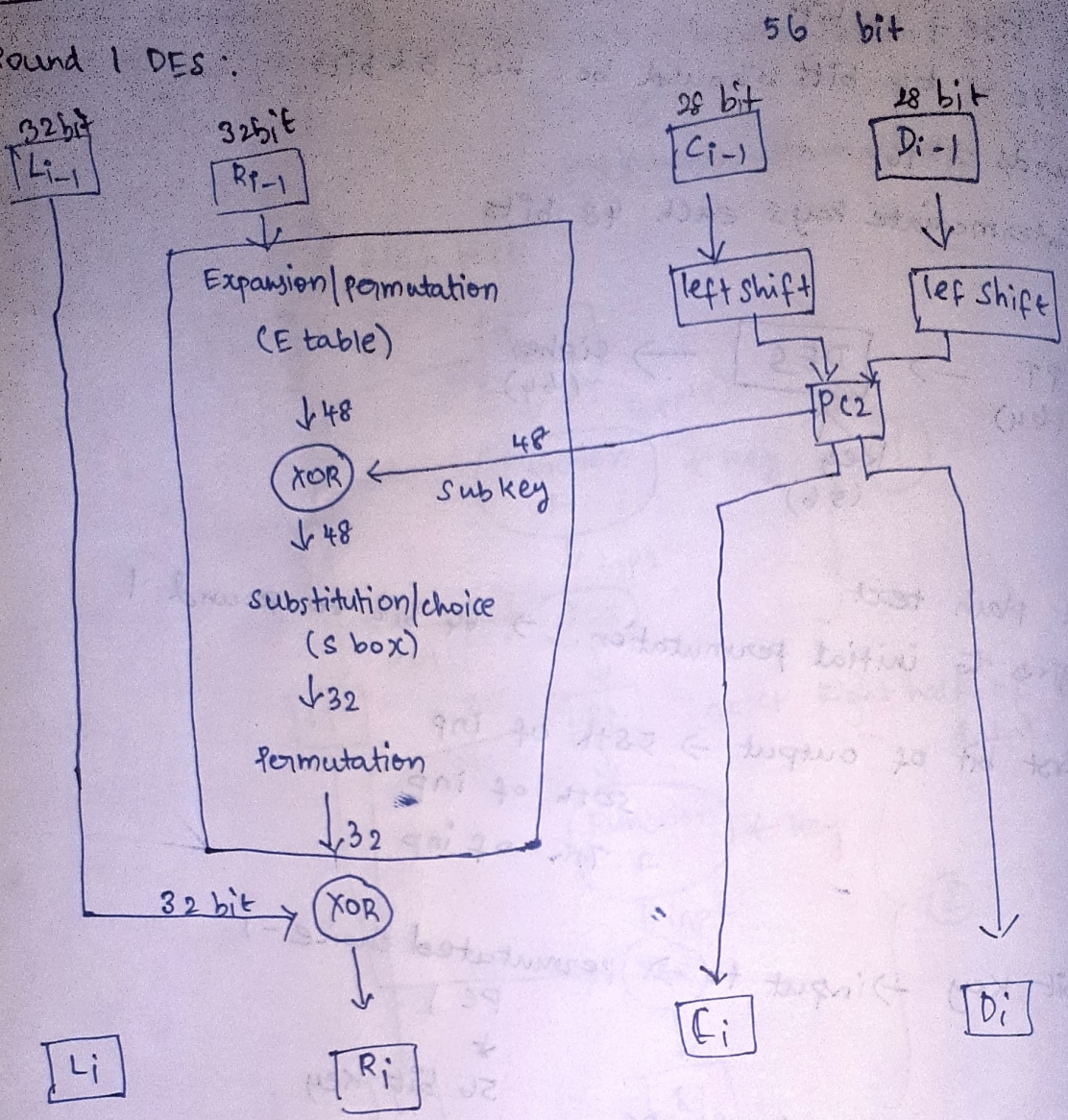


input to ↓

Inverse intial permutation → 64 bit cipher text.

3rd Feb :

Round 1 DES :



In SBox, divide 48 bits.

→ First 6 bit in S1 Box

→ 2nd 6 bits in S2 Box

⇒ So totally 8 SBoxes (8 × 6 = 48 bits)

6 bits → Box → 4 bits output

(So totally 32 bits as output)

6 bit → $b_1 b_2 b_3 b_4 b_5 b_6$

$b_1 b_6$ → row of matrix (2bits → 00, 01, 10, 11) → so 4 rows

$b_2 b_3 b_4 b_5$ → column of matrix (4 bits → 0, ... 15) → so 16 col.

matrix → 4 × 16

Example:

B = 101111

$b_1 b_6$ = 11 ⇒ row = 3

$b_2 b_3 b_4 b_5$ ⇒ 0111 ⇒ column = 7

7 + 3 ⇒ 10 ⟹ 1010 is output (4 bit value)