- Main goals of N.S. —
  1. Confidentiality
  2. Integrity
  3. Availability

* Cryptographic algorithms should not delay the availability (adversary) of services to people.

Cryptographic algorithms protect data, not channel or n/w. (could be public)

→ enable users to communicate in a secure environment.

Encryption to protect data.

- Cryptography — to secure
- Cryptanalysis — to figure out weaknesses (vulnerabilities) of the system
  (more difficult) — Analysis of syst / algos.

→ Cryptology

Both work together & are compulsory

for key { DES — Data Encryption Standard (64 bit key)
AES (128 bit key)

We try to find whether algo. can be broken using brute force. If we reach anywhere near, we decide its not safe.
For AES, e.g. we check whether we can generate 2^{127} keys. ($L 2^{128}$)

① Encryption / Encipherment

↓ covering the data while sending from one end to other (confidentiality)

helpful in passive attacks.

② Authentication – Verifying whether sender & receiver are legit user.

③ Notarization – Using trusted third party for securing communication betw. sender & receiver.

④ Hashing – Append an extra msg. to actual msg. to verify the data received.

Security Mechanisms – Providing security to data. Procedure used to protect info.

↳ Firewalls to protect

Security from threats, authentication, encryption, Authentication

⑤ Traffic Padding – In order to divert the adversary, some bogus info/ data is sent over the network & actual data is sent from another channel. Prevent attacker from doing traffic analysis.

⑥ Routing (Control) – Multiple routes are used to send data betw. sender & receiver (instead of single route) so that adversary is not able to find the actual route.

⑦ Access Control – Securing your system using some Password or OTP etc. (whether we have the right to access the data).

⑧ Digital Signature – Used to verify whether sender & receiver is legit or not & integrity of data is maintained or not. D.S. uses 2 keys. Sender signs it using its private key & if someone changes the data, he won't be able to sign it again.

D.S. & encryption together

Assymitric key – Sender encrypts using public key of receiver. (No integrity)

echnography

Trusted 3rd party → setup to comm. b/w sender & receiver,
- To avoid repudition
- Digital signature
- Authorized can only

Services provided by these mechanisms –

1. Confidentiality
   Integrity
2. Authentication
3. Non - Repudition
4. Access Control

Challenges to Security Mechanisms –

Developer should know

1. All possible attacks on that n/w.
2. Key management — Trusted 3rd party – 3rd party should be trusted.
3. Where to apply what security mechanism
4. Which Appropriate algo. to be used.
5. Key Updation after some time.
6. While designing or developing a ~~system~~ software, security is incorporated during development of software (design phase) or it is done after the development of software.
7. Attacker has an advantage over ~~at~~ developer. – Developer has to cover all possible loopholes (& he has a limited vision of n/w & most of system) while ~~developer~~ attacker has to find any one loophole / weakness & he can corrupt the entire system.
   Cryptanalysis is important.

If complexity of finding the key is less than system

(8) Ensuring availability - Algo. used shouldn't take lot of time finding security mechanism compatible with your system.

Threat - possible danger or vulnerability in system which could be attacked

Cryptanalytic Attack - Using / Exploiting mathematical weakness of system or algo.

Non-cryptanalytic Attack - Simply trying to interpret the msg. (without using brain)

Eg. - Spoofing, Masquerading, Traffic Analysis, DOS Attack,
↳ Passive ↳ not knowing the msg. ↳ Passive

replay → attacker sends same msg. again after some time. (it stored it).
→ Eg. - msg to send money.

Kerchoff's Principle -

A system is secure enough, when everything except key is known to an attacker but the system is secure.
(Algo., language, set of possible keys → all known)

→ What a cryptosystem comprises of -

P ; C ; K, E, D

P → set of PT
K → set of keys
E → set of Encryption functions

Let $x \in P$, $k \in K$

$e_k \in E$

$d_k \in D$

$e_k(x) = y \in C$

$d_k(y) = x$

Property –

$$d_k(e_k(x)) = x$$

encryption & decryption func. → one to one

One ≠ P.T. should give only one C.T. & vice-versa.

$x_1, x_2 \in P$ $\quad x_1 \neq x_2$

$y = e_k(x_1) = e_k(x_2)$

Ambiguity

- **Shift Cipher :**

$P = \{A, B, \ldots Z\}$

$C = \{A, B, \ldots Z\}$

$\{0, 1, \ldots 25\}$

$P = C = K = \{0, 1, \ldots 25\} = Z_{26}$

↓ set of integers & residue modulo 26

Eg – Alice to Bob $\quad k = 3$

message = C R Y P T O

2 17 24 15 19 14

+3

5 20 27/26 18 22 17

=1

C = F U B S W R

For decryption, subtract

5	20	1	18	22	17
- 3					
2	17	-2	15	19	14
		+26			
		24			

P = C R Y P T O

$e_k = (x + k) \bmod 26$

$d_k = (y - k) \bmod 26.$

No. of keys possible = 26 $\{0, 1, \ldots 25\}$

Exhaustive key search possible. (key space very small)

$k = 50 \Rightarrow k = 50 \% 26 = 24$

Z → set of integers

Z^+ → set of +ve integers

Z_m → modulo m $\{0, 1, \ldots (m-1)\}$

Properties -

~~x t~~

$x | y \quad (y = qx)$

$\Rightarrow$ x is completely divides y

$\gcd(x, y) | x$

$\gcd(y | x) | x$

$x = 24 \qquad y = 10$

$$24 = 10 * 2 + 4$$
$$10 = 4 * 2 + 2$$
$$4 = 2 \times (2) + 0$$

There exist 2 numbers r, s s.t. — when x & y are 2 integers.

$$rx + sy = \gcd(x, y)$$
$$= 2$$

$$24r + 10s = 2$$

~~$r = 5$~~ $\quad r = 3 \qquad s = -7$

$$24 \times 3 + 10 \times -7$$
$$= 72 - 70$$
$$= 2$$

$$24 = 10 \times 2 + 4 \qquad \text{——— (1)}$$

$$10 = 4 \times 2 + \boxed{2}$$

→ gcd

$$10 - 4 \times 2 = 2$$

Put 4 from (1)

~~$10 - (10 \times 2$~~

$$10 - (24 - 10 \times 2) \times 2 = 2$$

~~-3×10~~

$$-2 \times 24 + 5 \times 10 = 2$$

$r = -2 \qquad s = 5$

$Z_m = \{0, 1, \ldots (m-1)\}$

$y = q\,x + r$

$r = y \bmod x$

$x +_m y = (x+y) \bmod m$

$x \times_m y = (x \times y) \bmod m$

$Z_{10} = \{0, 1, 2, \ldots 9\}$

$x = 5 \qquad y = 9$

$x +_{10} y = 4$

$x \times_{10} y = 5$

~~Proofs~~

Properties of Addition modulo m -

$x, y, z \in Z_m$

1) Commutative :

$$x +_m y = y +_m x$$

2) Associative :

$$(x +_m y) +_m z = x +_m (y +_m z)$$

3) Closure :

$$x, y \in Z_m \Rightarrow x +_m y \in Z_m$$

4) Identity:

$$x +_m 0 = x$$

5) Inverse :

$$x +_m y = 0 \Rightarrow y = -x \text{ or } m-x$$

$$x +_m (m-x) = 0$$

m is any integer.

Z_{10} : $x = 8$ Inverse = 2

Z_5 : $x = 5$ Inverse = 5

Z_3 : $x = 1$ Inverse = 2

Properties of Multiplication modulo m -

1) Commutative -

$$x \times_m y = y \times_m x$$

2) Associative -

$$(x \times_m y) \times_m z = x *_m (y *_m z)$$

3) Closure -

$$x, y \in Z_m \Rightarrow x *_m y \in Z_m$$

4) Identity -

$$x \times_m 1 = x$$

5) Inverse -

$$x *_m y = 1$$

Inverse of all nos. are not possible.

✓ Inverse is possible if $\gcd(x, m) = 1$

In Z_6, inverse of 2, 3, 4 are not possible.
as $\gcd(x, 6) \neq 1$

In Z_5, inverse of all 0 - 4 is possible

Proof:

$$\gcd(x, m) = 1$$

$$x \in Z_m$$

$$rx + sm = 1$$

$rx + sm = 1$

$rx = 1 - sm$

$\left(r = q \bmod m + r' \right)$

$r' = r \bmod m$

$(q \bmod m + r \bmod m)\, x = 1 - sm$

$(r \bmod m)\, x = 1 - sm - qmx$

$(r \bmod m)\, x = 1 + m(-s - qx)$

$(r \bmod m)\, x = m(-s - qx) + 1$

$(\Rightarrow \text{Rem}^n = 1$ when divided by $m)$

$(r \bmod m)\, x \equiv 1 \pmod m$

$r \bmod m$ becomes inverse of x in modulo

$y \bmod x = r$

$r \equiv y \pmod x \Rightarrow r \bmod x = y \bmod x$

x divide both r & y and give same remainder

$(r \bmod m)\, x \equiv 1 \pmod m$

$r \bmod m *_m x = 1$

$(r \bmod m \times_m x = 1)$

$\rightarrow$ inverse

$y = r \bmod m$

∴ If x & y are co-prime, there exists some y for each x s.t. ~~$y = x^{-1}$~~. $xy \bmod m = 1$

Q. Find inverse of x

$x = 7 \quad m = 15$

~~$xy_m = 1$~~ Repeated division method

$15 = 7 \times 2 + 1$

~~$7 =$~~ $15 - 7 \times 2 = 1$

$7(-2) + 15 = 1$

$7(13) \cancel{+15} = 1 - 15$

$y = 13$

Let $\gcd(x, m) \neq 1$

Prove that ~~an~~ M.I. doesn't exist.

Let $\gcd(x, m) = d$ & let's assume M.I. ~~exists~~ is y.

$$\frac{x}{d} \times m = \frac{m}{d} \times x$$

$$x \times \left(\frac{m}{d}\right) \equiv 0 \pmod{m}$$

Multiplying y both sides -

$$y \times_m \left(x \times_m \frac{m}{d}\right) = 0$$

$$\left(y \times_m x\right) \times_m \frac{m}{d} = 0$$

$$1 \times_m \frac{m}{d} = 0$$

$$\frac{m}{d} = 0$$

This is not possible.

Hence $\gcd(x, m) \neq 1$ is not possible.

- Affine Cipher -

To increase key space,
we take 2 set of keys s.t.

$(a, b) \in Z_{26} \times Z_{26}$; $\gcd(a, 26) = 1$

$P = C = Z_{26}$

$C_{(a,b)}(x) = (ax + b) \bmod 26$

$y = (ax + b) \bmod 26$

$x = a^{-1}(y - b) \bmod 26$

$d_{(a,b)}\ y = a^{-1}(y + (26 - b)) \bmod 26$

Eg -

$k = (23, 18)$ ← coprime with 26

P = STRIKE AT THREE

18 19 8 10 4

$C_1 = 23 \times 18 + 18$
$= 432 \bmod 26$
$= 16 = Q$

$C_2 = 19 \times 23 + 18$
$= 360 \bmod 26$
$= 13 = N$

$C_3 = 14 \times 23 + 18$
$= 324 \bmod 26$
$= 19 = T$

$C_4 = 8 \times 18 + 18$

$C_4 = 8 \times 23 + 18$

$= 20$

$= U$

$C_5 = 10 \times 23 + 18$

$= 14$

$= O$

$C_6 = 4 \times 23 + 18$

$= 6$

$= G$

$C = $ U N T U O G

$P = a^{-1} = 23^{-1} \bmod 26$

$26 = 23 \times 1 + 3$

$26 - 23 \times 1 = 3$

$26 - 23 - 2 = 1$

$26 = 2 \times 13$

$2 = \frac{26}{13}$

$26 = 23 \times 1 + 3$

$23 = 3 \times 7 + 2$

$3 = 2 \times 1 + 1$

Rem Rem

$3 - 2 \times 1 = 1$

$(26 - 23) - (23 - 3 \times 7) = 1$

Replace from their respective equations one by one

$3 - (23 - 3 \times 7) = 1$

$3 \times 8 - 23 = 1$

$(26 - 23) \times 8 - 23 = 1$

$26 \times 8 - 23 \times 9 = 1$

Inverse $= -9 = 26 - 9 = 17$

$(23)^{-1} = 17$

$x = a^{-1}(y + 26 - b) \bmod 26$

$P_1 = 17(16 + 26 - 18) \bmod 26$

$= 17 \times 24 \bmod 26$

$= 408 \bmod 26$

$= 18 = S$

$P_2 = 17(13 + 8) \bmod 26$

$= 357 \bmod 26$

$= 19 = T$

same

Eg - M.I. of 15 modulo 26

$26 = 15 \times 1 + 11$

$15 = 11 \times 1 + 4$

$11 = 4 \times 2 + 3$

$4 = 3 \times 1 + 1$

$4 - 3 = 1$

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

$-11 + 4 \times 3 = 1$

$-11 + (15 - 11) \times 3 = 1$

$3 \times 15 - 4 \times 11 = 1$

$3 \times 15 - 4(26 - 15) = 1$

$3 \times 15 - 4 \times 26 + 4 \times 15 = 1$

$7 \times 15 - 4 \times 26 = 1$

Inverse = 7

Drawback -

1) Key space is small $(Z_{26} \times Z_{26})$
2) If a character gets repeated 5 times, then the corresponding cipher text character will also be repeated 5 times. Hence, frequency analysis is possible.

- Vignesr Cipher -

Key space → $(Z_{26})^m$

$Z_{26} \times Z_{26} \times$ ---------- m times

$x_1, x_2, \ldots x_m, x_{m+1}, \ldots x_{2m} \ldots$
$k_1, k_2 \ldots k_m, k_1, k_2 \ldots k_m \ldots$

$y_1 = (x_1 + k_1) \bmod 26$
$y_2 = (x_2 + k_2) \bmod 26$

Decryption -

$x_i = (y_i - k_i) \bmod 26$
$= (y_i + (26 - k_i))$

Eg. - P = CRYPTOGRAPHY (2 17 24 15 19 14 6 17 0 15 7 24)

deceptive (3 4 2 4 15 19 8 19 → 21 → 4)

CRYPTOGRAPHY
deceptivedec

= ~~5~~ 20 R
= 5 21 0 19 8 7 14 (R 12) 4 18 11 0
= F V A T I H O M E S ML A

Freq. analysis is not possible.
We can find out the key in finite no. of computation.

How to know whether a cipher is secure or not?

1) If we can find key in less computationally than ~~its~~ not secure.
2) If factorisation is not possible, its secure.
3) Even if factorisation is possible & still key couldn't be determined by computations. (Unconditionally secure)
   → Doesn't exist still now.

Shannon gave the concept of Perfect Secrecy.

P, C, K, E, D

$x \in P$

$P_r(X = x)$

$P_r(K = k) \quad k \in K$ } Independent (randomly chosen)

$P_r(Y = y)$

$$P_r[Y = y] = P_r[(K = k) \wedge (x = x = d_k(y))] \quad (y = e_k(x))$$

There can be many keys that give us the same CT with diff. PT.

et

$$P(A|B) = \frac{P(\frac{B}{A}) \cdot P(A)}{P(B)}$$

$$C(k) = \{ e_k(x) : x \in P \}$$

$$P_r[Y=y] = \sum_{\{k: y \in C(k)\}} P_r[(K=k)]\, P_r[X=x]$$

$$P_r[Y=y \mid X=x] = \sum_{\{k: x = d_k(y)\}} P_r[K=k]$$

$$P_r[X=x \mid Y=y] = \frac{P_r[X=x] \cdot P_r[Y=y \mid X=x]}{P_r[Y=y]}$$

$P_r(M)$

Acc. to Perfect secrecy, $P_r(M)$ should be dependent only on $P_r[X=x]$ (not key as well)

Eg.-

$P = \{a, b\}$

$K = \{k_1, k_2, k_3\}$

$P_r[a] = \frac{1}{4}$ → Prob. of a string used as PT

$P_r(b) = \frac{3}{4}$

$P_r[K=k_1] = \frac{1}{2}$ → Prob. of k_1 selected as key.

$P_r[K_2] = \frac{1}{4}$ $\quad P_r[K_3] = \frac{1}{4}$

$e_{k_1}(a) = 1$ $\quad e_{k_1}(b) = 2$ $\quad e_{k_3}(a) = 3$

$e_{k_2}(a) = 2$ $\quad e_{k_3}(b) = 4$ $\quad e_{k_2}(b) = 3$

~~$e_{k_2}(a) = 2$~~

~~$e_{k_3}(a) = 3$~~

P(a/1)

$e_{K_1}(b) = 1$

$e_{K_2}(b) = 2$

$e_{K_3}(b) = 4$

Find out the value of ~~output~~ probability of 1. using the C.T.

$P(Y=y) = \sum P(K=K_i) \cdot P(X=x)$

$P(Y=1) = \sum P(K=K_1) \cdot P(X=a)$

$= \frac{1}{2} \cdot \frac{1}{4} = \frac{1}{8}$

CT=2 in a

$P(Y=2) = \sum P(K=K_2) \cdot P(X=a) + P(K=K_1) \cdot P(X=$

$= \frac{1}{8} + \frac{1}{4} \cdot \frac{1}{4} = \frac{1}{4} \times \frac{1}{4} + \frac{1}{2} \times \frac{3}{4}$

$= \frac{1}{8} + \frac{1}{16} = \frac{4}{16} = \frac{1+6}{16} = \frac{7}{16}$

$P(Y=3) = \sum P(K=K_3) P(X=a) + P(K=K_2) P(X=b)$

$= \frac{1}{4} \times \frac{1}{4} + \frac{1}{4} \times \frac{3}{4}$

$= \frac{4}{16}$

$= \frac{1}{4}$

$P(Y=4) = P(K=K_3) P(X=b)$

$= \frac{1}{4} \times \frac{3}{4}$

$= \frac{3}{16}$

$P(a/1) = \frac{P_r(a) P_r(1/a)}{P_r(1)}$ $P_r(a/1) = 1$ $= \frac{1}{7}$

$P(b/2) = 6/8$ $P(b/3) = 3/4$ $P(b/4) = 1$

$P(a/1) = \frac{P_r(a) \cdot P_r(1/a)}{P_r(1)}$ $P(r=r_1)$

$= \frac{\frac{1}{4} \times \frac{1}{2}}{\frac{1}{8}}$

$= 1$

$P(a/2) = \frac{P_r(a) \cdot P_r(2/a)}{P_r(2)}$

$= \frac{\frac{1}{4} \times \frac{1}{4}}{\frac{7}{16}}$

$= \frac{1}{7}$

$P(b/2) = \frac{P_r(b) \cdot P_r(2/b)}{P_r(2)}$

$= \frac{\frac{3}{4} \times \frac{1}{2}}{\frac{7}{16}}$

$= \frac{6}{7}$

$P(b/3) = \frac{P_r(b) \cdot P_r(3/b)}{P_r(3)}$

$= \frac{\frac{3}{4} \times \frac{1}{4}}{\frac{1}{4}}$

$= \frac{3}{4}$

→ since 4 can be derived with only one key, $P_r = 1$

$$P(b/4) = \frac{P_r(b) \cdot P_r(4/b)}{P_r(4)}$$

$$= \frac{\frac{3}{4} \times \frac{1}{4}}{\frac{3}{16}}$$

$$= 1$$

$$P_r[X = x \mid Y = y] = \frac{P_r(X = x) \cdot P_r[Y = y \mid X = x]}{P_r(Y = y)}$$

Acc. to perfect secrecy

→ $P_r(X = x \mid Y = y) = \frac{P_r(X = x) \cdot P_r[Y = y \mid X = x]}{P_r(Y = y)} = P_r[X = x]$

→ Shift cipher is following Perfect secrecy only in the case of equiprobable $\frac{1}{|K|}$ keys.

$$P = C = K = Z_{26}$$

$$y = (x + k) \bmod 26$$

$$P_r(K = k) = \frac{1}{26}$$

$$P_r(Y = y) = \sum_{k, y \in C(k)} P_r[K = k] \, P_r[X = x = d_k(y)]$$

$$= \sum_{k \in Z_{26}} \frac{1}{26} P_r[X = x = (y - k) \bmod 26]$$

$$= \frac{1}{26} \sum_{k \in Z_{26}} P_r(X = x)$$

$$= \frac{1}{26} \times 1$$

$$= \frac{1}{26}$$

$$P_r(Y = y \mid X = x) = \sum_{k x = d_k(y)} P_r(K = k)$$

↳ Only one key with 'X' will give a particular 'Y' a particular

$$= \frac{1}{26}$$

$$P_r(X = x \mid Y = y) = \frac{P_r(X = x) \cdot P_r(Y = y \mid X = x)}{P_r(Y = y)}$$

$$= \frac{P_r(X = x) \; 1/26}{\frac{1}{26}}$$

$$= P_r(X = x)$$

Perfect Secrecy -
Even if we know the cipher text, we cannot guess anything about plain text.
(For every P.T., we have a new key).

One Time Pad

Whether a particular system is following Perfect secrecy or not?

→ Latin square - In every row & every column, the no is not repeated.

1	2	3
3	1	2
2	3	1

$P = C = K = \{1, 2, 3\}$

$e_i(j) = L(i, j)$ (key → PT; i^{th} row, j^{th} col.)

$Pr(K=1) = Pr(K=2) = Pr(K=3) = \frac{1}{3}$

Does this system follow P.S.?

$$Pr(y=y) = \sum_{k \in \{1,2,3\}} Pr(K=k) \cdot Pr(x = x \mid d_k(y))$$

$$= \frac{1}{3} \sum_{k \in \{1,2,3\}} Pr(x=x)$$

$$Pr(y=y \mid x=x) = \sum_{k \in} Pr(K=k)$$

$\neq$

$$Pr(y=y) = Pr(y=y, K=1) + Pr(y=y, K=2) + Pr(y=y, K=3)$$
$$= Pr(K=1) \cdot Pr(y=y \mid K=1) + Pr(K=2) Pr(y=y \mid K=2) + Pr(K=3) Pr(y=y \mid K=3)$$

$$= \frac{1}{3}\left(3 \times \frac{1}{3}\right)$$

$$= \frac{1}{3}$$

$P_r(Y=1 \mid K=1) = P_r(X=1) = \frac{1}{3}$

$P_r(Y=P \mid K=2) = P_r(X=2) = \frac{1}{3}$

$P_r(Y=1 \mid K=3) = \frac{1}{3}$

Similarly for all Y

$$P_r(Y=y \mid X=x) = \sum_k P_r(K=k)$$

$$= \frac{1}{3}$$

$P_r(Y=1 \mid X=1) = P_r(K=1) = \frac{1}{3}$

↳ in 3 rows ↳ only in when $K=1$

$$P_r(X=x \mid Y=y) = \frac{P_r(X=x) \cdot P_r(Y=y \mid X=x)}{P_r(Y=y)}$$

$$= \frac{P_r(X=x) \cdot \frac{1}{3}}{\frac{1}{3}}$$

$$= P_r(X=x)$$

Q. $P(K=1) = P(K=2) = \frac{1}{4}$ $\quad P(K=3) = \frac{1}{2}$

~~Same ques.~~

$P(X=1) = P(X=2) = \frac{1}{8}$ $\quad P(X=3) = \frac{3}{4}$

Same ques.

$P_r(Y=y) = \sum P_r(K=k) \cdot P_r(X=x)$

$= P_r(Y=y, K=1) + P_r(Y=y, K=2) + P_r(Y=y, K=3)$

$= P_r(K=1) \cdot P_r(Y=y \mid K=1) + P_r(K=2) P_r(Y=y \mid K=2) + P_r(K=3) P_r(Y=y \mid K=3)$

$= P_r(K=1) \cdot P_r(Y=1 \mid K=1) + P_r(K=2) \cdot P_r(Y=1 \mid K=2) + P_r(K=3) P_r$

$= \frac{1}{4} \times \frac{1}{8} + \frac{1}{4} \times \frac{1}{8} + \frac{1}{2} \times \frac{3}{4}$

$= \frac{1}{16} + \frac{3}{8} = \frac{7}{16}$

$P_r(Y=1 \mid K=1) = P_r(X=1) = \frac{1}{8}$

$P_r(Y=2 \mid K=1) = P_r(X=2) = \frac{1}{8}$

$P_r(Y=3 \mid K=1) = P_r(X=3) = \frac{3}{4}$

$P_r(Y=1 \mid K=2) = P_r(X=2) = \frac{1}{8}$

$P_r(Y=2 \mid K=2) = P_r(X=3) = \frac{3}{4}$

$P_r(X=3 \mid K=3) = P_r(X=1) = \frac{1}{8}$

$P_r(Y=1 \mid K=3) = P_r(X=3) = \frac{3}{4}$

$P_r(Y=1 \mid K=1) = \frac{1}{8}$

$(K=2) = \frac{1}{8}$

$K=3 = \frac{3}{4}$

$Y=2 \mid K=1 = \frac{1}{8}$

$K=2 = \frac{3}{4}$

$K=3 = \frac{1}{8}$

$$Pr(y = y \mid x = x) = \sum_k Pr(k = K) = \frac{1}{4} Pr[k = K]$$

$k = k_1, k_2, k_3, k_4$

$$Pr[Y = 1 \mid X = 1] = Pr[k = 1] = \frac{1}{4}$$

$$[Y = 1 \mid X = 2) = \frac{1}{4}$$

$$P[X = x \mid Y = y]$$

$$[X = 1 \mid Y = 1) = \frac{Pr[X = 1] Pr[Y = 1 \mid X = 1]}{Pr[Y = 1]}$$

$$= \frac{Pr(X = 1) \frac{1}{4}}{\frac{7}{16}}$$

Monoalphabetic cipher – One character in P.T. gets mapped to one unique character in C.T.

Eg. – Shift Cipher, Caesar Cipher

Polyalphabetic –

Hill Cipher, ~~Vigenere~~ Vigenere

Transposition – Rearrangement of characters

- **Vigenere Cipher -**

$K = (Z_{26})^m$ $\quad P = C = (Z_{26})^m$

key = CIPHER → m = 6
2 8 15 7 4 17

Each s will be mapped to diff characters

P = Security is compromised
CIPHERCI PH ER

= 20 12 17 27 21 25 21 32 28 25 6 5 14 ...
$27 \bmod 26 = 1$, $32 \bmod 26 = 6$
U M R B V Z V G X Z G F O

23 6 21 16 25 20 12 18
X G V Q Z U M S

key space = $26^m = 26^6$

- **Hill Cipher :**
Can be broken by Known PT attack.

$P = C = (Z_{26})^m$ → taking linear combination of m characters at a time

$K = m \times m$ matrix

$$e_K(P) = (x_1 \; x_2) \begin{pmatrix} k_1 & k_2 \\ k_3 & k_4 \end{pmatrix} = (y_1 \; y_2)$$

$$PK = C$$
$$P = CK^{-1}$$

Matrix should be invertible ~~on Z_{26}~~ → ~~gcd = 1~~
↳ $|A| \neq 0$

Inverse of $|A|$ exists in Z_{26} ↳ $\gcd(|A|, 26) = 1$

$7 \times x = 1 \mod 26$

$x = 15$

Eg.-

$$K = \begin{bmatrix} 11 & 8 \\ 3 & 7 \end{bmatrix}$$

$|K| = 77 - 24$

$= 53 \mod 26$

$= 1$

Inverse of 1 should exist in Z_{26}

$$K^{-1} = \begin{bmatrix} 7 & -8 \\ -3 & 11 \end{bmatrix} \rightarrow 26 - 8$$

$$= \begin{bmatrix} 7 & 18 \\ 23 & 11 \end{bmatrix}$$

$P = CR$

$x_1 = 2 \quad x_2 = 17$

$$(y_1 \quad y_2) = (x_1 \quad x_2) \begin{pmatrix} k_1 & k_2 \\ k_3 & k_4 \end{pmatrix}$$

$y_1 = x_1 k_1 + x_2 k_3$

$= 2 \times 11 + 17 \times 3$

$= 22 + 51$

$= 73 \mod 26$

$= 21$

$y_2 = x_1 k_2 + x_2 k_4$

$= 2 \times 18 + 17 \times 7$

$= 36 + 119 = 155$

$= 5$

Ques.

$$K = \begin{bmatrix} 10 & 5 & 12 \\ 3 & 14 & 21 \\ 8 & 7 & 1 \end{bmatrix}$$

$$|A| = 10(14 - 21 \times 7) - 5(3 - 21 \times 8) + 12(21 - 14 \times 8)$$

$$= -1330 + 825 - 1092$$

$$= -1597 \mod 26$$

$$= 15$$

↳ Inverse exists as its co-prime with 26

$$\text{Co-factor} = \begin{bmatrix} -133 & 165 & -11 \\ +79 & -96 & 91 \\ -63 & -174 & 125 \end{bmatrix}$$

$$= \begin{bmatrix} 23 & 9 & 15 \\ 1 & 8 & 13 \\ 15 & 8 & 21 \end{bmatrix}$$

$$\text{adj}(A) = \begin{bmatrix} 23 & 1 & 15 \\ 9 & 8 & 8 \\ 15 & 13 & 21 \end{bmatrix}$$

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

$$= 7 \times \text{adj}(A)$$

$$= \begin{bmatrix} 161 & 7 & 105 \\ 63 & 56 & 56 \\ 105 & 91 & 147 \end{bmatrix}$$

$$= \begin{bmatrix} 5 & 7 & 1 \\ 11 & 4 & 4 \\ 1 & 13 & 17 \end{bmatrix}$$

Substitution Cipher -

$P = C = Z_{26}$

A	B	C	D	E	F	G	H	I	J	...	S	...
E	G	A	I	H	B	D	J	C	F	...	Z	...

$\{0, 1, \ldots 25\} \rightarrow \{0, 1, \ldots 25\}$

$\phi : A' \rightarrow A'$

$\phi : Z_{26} \rightarrow Z_{26}$

P = SECURITY IS COMPROMISED

= Z H A

26! permutations possible $= 10^{26}$

Brute Force attack not possible.

Freq. analysis possible.

Transposition Cipher -

Rearrangement of letters

P = security ~~is~~ ~~compromised~~.

s	c	r	t
e	u	i	y

Read row wise C = scrteuiy

We can increase no. of rows.

Read spirally

Polyalphabetic cipher

$m = 6$

π:

1	2	3	4	5	6
5	4	1	6	3	2

$\pi : \{1,2,3,4,5,6\} \rightarrow \{1,2,3,4,5,6\}$

$x_1 \; x_2 \; x_3 \; x_4 \; x_5 \; x_6$

$x_{\pi(1)} \; x_{\pi(2)} \; x_{\pi(3)} \; x_{\pi(4)} \; x_{\pi(5)} \; x_{\pi(6)}$

$x_5 \; \tau \; x_4$

security is compromised

r u s i c e

π^{-1}:

1	2	3	4	5	6
3	6	5	2	1	4

Easily Breakable (PT is not changed, small m)

- **Playfair Cipher –**

5 * 5 matrix as 26 elements can be arranged (keep any 1 of them in I)

Key size is not fixed (can be very high)

But since we have 26 letters, we take

balloon

Eg.- F

K = SECURITY

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

If K = balloon
↳ don't repeat

B	A	L	O	N
C	D	E	F	

OP = PL
WC = CY
↓ same colm
↓ down letter in same colm

P → PA RT YA TT EN → in same grp.
TX XT
→ bogus

→ Take in a group of 2 (a[i]c[j])

→ row of P × colm of A
→ row of A × colm of P
→ in same row (so next letter in row)

P = PA RT YA TX TE NX
C = OB EB AB AV FT OW

Decryption :-

P = PA RT YA

Eg.-

P = Meet me at park

= VT TF VT BY OB BP

e is mapped to T everytime.
Not good

K = 25!

B.F. not possible
Freq. analysis possible

- **CRYPTANALYSIS :**
  ↳ trying to find the key ✓

1) Cipher Text Only Attack.

2) Known PT Attack –
   Attacker by chance got some pairs of PT-CT.

3) Chosen PT Attack –
   Himself chosen PT & gets its encrypted.

4) Chosen CT Attack –
   By chance he knows the decryption algo. & key is already embedded in that.
   He can get chosen CT decrypted.
   ↳ Strongest

While designing the algo., we focus on Chosen CT Attack.
From attacker's POV, CT only attack is the easiest.
↙ No need to know anything else.

In Vigenere Cipher, we can get to know the length of the key.

This is C class . This
↓
K=code

Product cipher -

Given by Shannon

Here, we are combining 2 cryptosystems together.
→ ciphers

$S_1 \rightarrow \{P, C, K_1, E_1, D_1\}$

$S_2 \rightarrow \{P, C, K_2, E_2, D_2\}$

$$P = C = P$$

$e_{K_1}(x) = y \qquad d_{K_1}(y) = x$

$e_{K_2}(x) = y \qquad d_{K_2}(y) = x$

$$S_1 \times S_2$$

$$\{P, C, K_1 \times K_2, e_s, D\}$$

$$e_{(K_1, K_2)}(x) = y = e_{K_2}(e_{K_1}(x))$$

$$d_{(K_1, K_2)}(y) = x = d_{K_1}(d_{K_2}(y))$$

$$d_{K_1}(d_{K_2}(e_{K_2}(e_{K_1}(x)))) =$$

$$d_{K_1}(e_{K_1}(x)) = x$$

Eg-

Shift cipher: $K = Z_{26} \qquad e_b(x) = x + b \mod 26 \qquad d_x(y) = y - b \bmod 26$

Multiplicative cipher → $K = Z_{26} = \{a \in Z_{26}, \gcd(a, 26) = 1\}$ $\quad e_a(x) = ax \bmod 26$

$d_a(y) =$

$x = a^{-1} y \bmod 26$

Affine cipher: $M \times S$

$$e_{(K_1, K_2)}(x) = e_{K_2}(e_{K_1}(x))$$
$$= e^s_b(e^m_a(x))$$

$= e_b(ax \bmod 26)$

$= *(ax+b) \bmod 26$

$d_a(d_b(y)) = d_a(ax+b-b)$

$= d_a(ax)$

$= (a^{-1}ax)$

$= x$

S x M :

$= e_a(e_b(x))$

$= e_a(x+b)$

$= a(x+b) \bmod 26$

Not same

Eg. -

$P = 7 \qquad K = (3, 5)$

$M \times S \ \& \ e = (ax+b) \bmod 26$

$= (3x+5) \bmod 26$

$= 26 \bmod 26$

$= 0$

d :

$S \times M \ \& \ e = a(x+b) \bmod 26$

$= 3(7+5) \bmod 26$

$= 3 \times 12 \bmod 26$

$= 36 \bmod 26$

$= 10$

$d_{(3,5)} = d_b(d_a(x))$

$= d_b(a^{-1}(ax+b))$

$= d_b(a^{-1}ax + a^{-1}b)$

$= d_k(x + b)$

$= (x + b - b)$

$= (7 + 5 - 5)$

$= 7 + 0 \mod 26$

$= 7$

~~$d = a^{-1}(x - b)$~~ $d = a^{-1}y - b$

$= 9 \times 10 - 5$

$= 85 \mod 26$

$= 7$

On decryption both $S_1 \times S_2$ & $S_2 \times S_1$ should give same P.T.

- **Block Cipher** -

Derived from Product Cipher

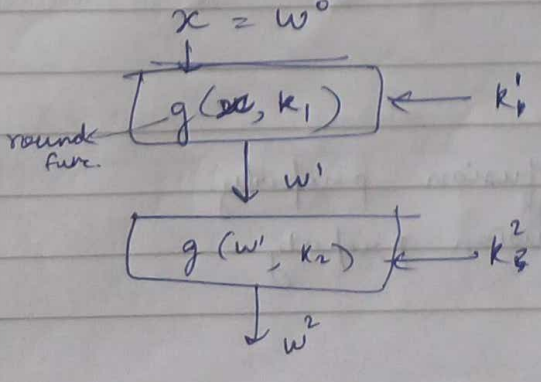
Taking a block of bits together.

We'll do iterations of encryptions

K → main key

small subkeys derived from it which will be used in subsequent iterations.

$K \rightarrow k_1^1, k_2^2, \ldots k_b^n$



$$w^0 = w_1^0, w_2^0 \dots w_{\phi}^0$$

$$k'_{\phi} = k'_1, k'_2 \dots k'_0$$

(should be irreducible)

$$g \Rightarrow (w_1^0 \oplus k'_1), (w_2^0 \oplus k'_2)$$

$\oplus$: XOR, addition mod 2

$$w^r = g(w^{r-1}, k^{*r})$$

$$g^{-1}(w^r, k^{*r}) = w^{r-1}$$

- **Substitution Permutation Network –**

  lm bits

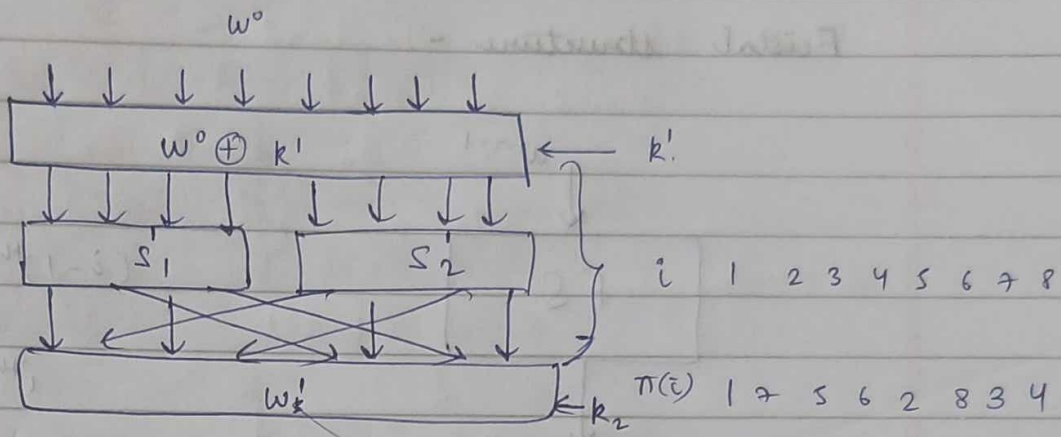
  $l = 4 \quad m = 2 \rightarrow$ 4 bits grouped together

  $l = 4 \quad m = 4$

In every round same steps will be performed-

1) Key mixing → XOR of key & PT
2) Substitution
3) Permutation

S - box → Diffusion property
P - box → Confusion property



Eg. -

4×4 size

S-Box of Present Cipher

x	0	1	2	3	4	5
S(x)	C	5	6	B	9	0

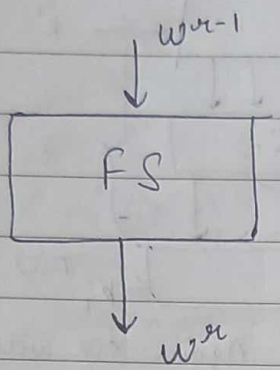
x	6	7	8	9	A	B
S(x)	A	D	3	E	F	8

x	C	D	E	F
S(x)	4	7	1	2

0 → 0000
C → 1100

Our motive is to hide the key, so we want to distribute key in CT in such a manner that no. func. can give me back the key.
S-box makes it non-linear.
Make S-box so secure,
No linear func. can get us make the key.

Feistal structure -

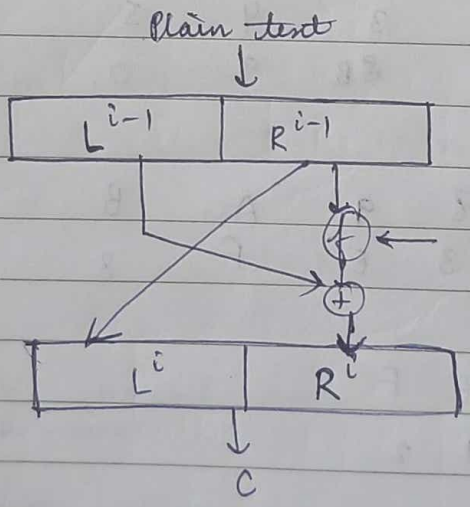


$(i-1)^{th}$ round → i^{th} round

$(i-1)^{th}$ round $\quad L^{i-1} \quad R^{i-1}$

$L^i \neq L^i \quad R^i$

Feistal Structure for i^{th} round -



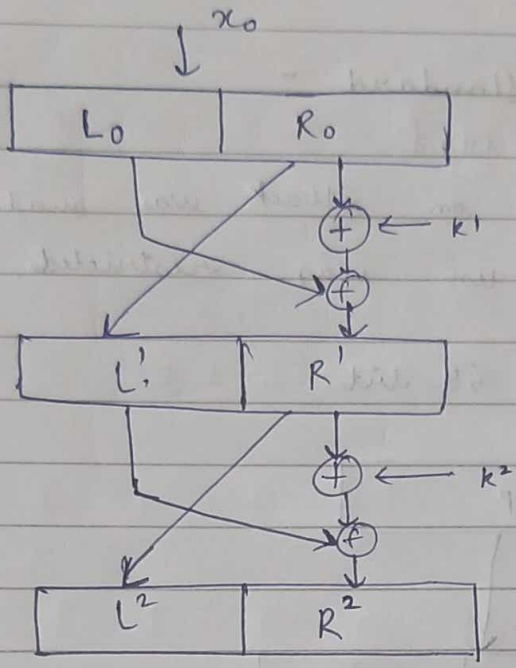
$L^i = R^{i-1}$

$R^i = L^{i-1} \oplus f(R^{i-1}, K^i)$

f function can change, rest n/w remains same.

Not considering inverse of f

Advantage of F.N.



Decryption -

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

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

Take XOR both sides

$\Leftrightarrow f(R^{i-1}, k^i) \oplus R^i = L^{i-1}$

$\rightarrow L^{i-1} = R^i \oplus f(R^{i-1}, k^i)$

f function remains the same in both encryption & decryption.

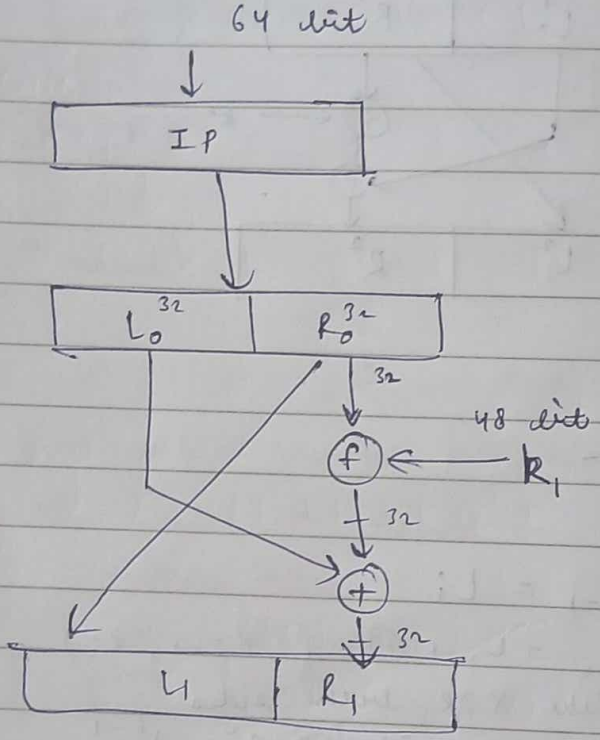
Advantage of F.S. → Not considering inverse of f.

Data Encryption Standard -

started in 1977

in 1998, an attack was made on DES & its use was restricted.

16 rounds

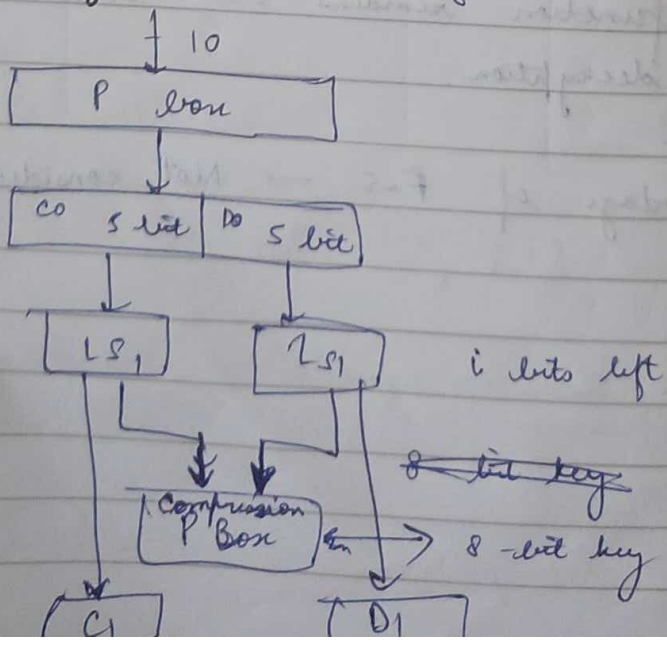


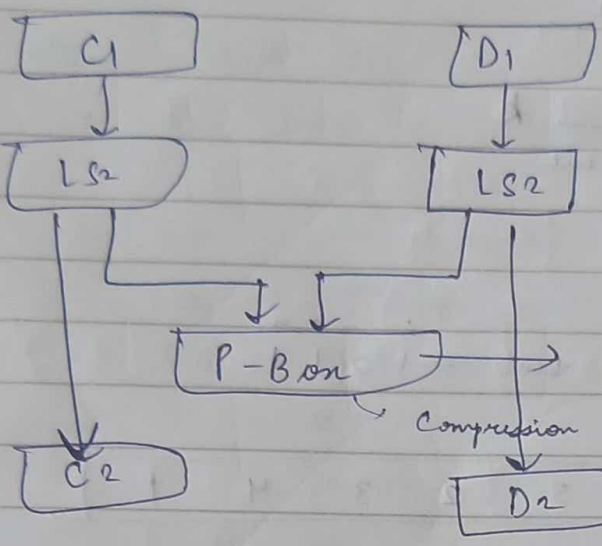
S-DES:

Round key generation ⇒ Key = 10 bit

$K_1 \rightarrow 8$ bit

Key Scheduling Algorithm :- $K_2 \rightarrow 8$





Order -

P Box 1: 3 5 2 7 4 10 1 9 8 6

Key = 1011111110

After P-box:-

3rd

K = 1001 1 01111

LS1 00111 11110

Compression P-box:

Order: 6 3 7 4 8 5 10 9

1 1 1 0 1 1 0 1

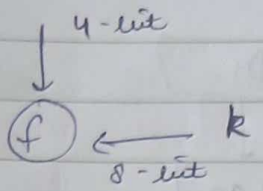
Round 2 -

C1 = 00111 D1 = 11110

LS2: 11100 11011

CP box -

Key for round 2 → 1 1 1 0 0 0 1 1



1) Expansion -

Input = 1 0 1 1

Expansion table -

4	1	2	3	2	3	4	1

1 1 0 1 0 1 1 1 ⊕ k

2) XOR with key

k = 1 1 1 1 1 1 0 1

⊕

1 1 0 1 0 1 1 1

0 0 1 0 1 0 1 0

3) Substitution : 8 i/p → 4 bit o/p

S - box:

	0	1	2	3
0	1	0	3	2
1	3	2	1	0
2	0	2	1	3
3	3	1	2	3

S-Box 1

	0	1	2	3
0	0	1	2	3
1	2	0	1	3
2	3	0	1	0
3	2	1	0	3

S-box 2

0 0 1 0

S Box 1

1 0 1 0

S Box 2

0010

00 → row
01 → col

0th row & 1st col
= 0
= 00

First & last bits → row no.
Middle bits → Col. no.

1 0 1 0

10 → 2nd row

01 → 1st col

= 0

= 00

o/p = 0 0 0 0

In DES.

1 0 11 1 0

First ~~first~~ last bit → row no

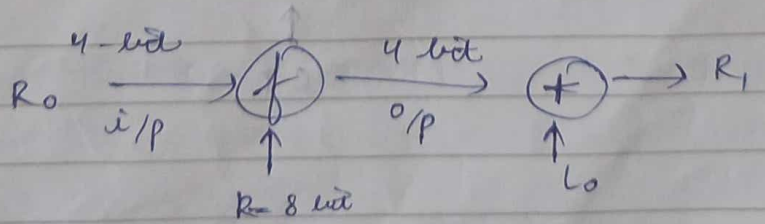
Middle bits → Col no.

↳ upto 15

4) Permutation -

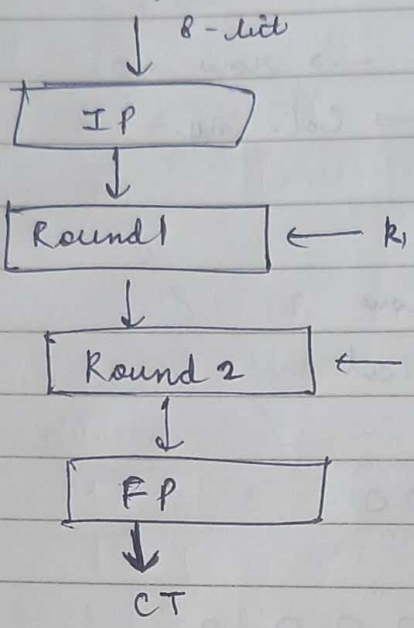
2	4	3	1

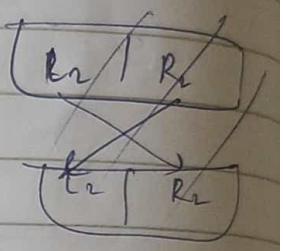
= output



$L_1 = R_0$

Encryption -

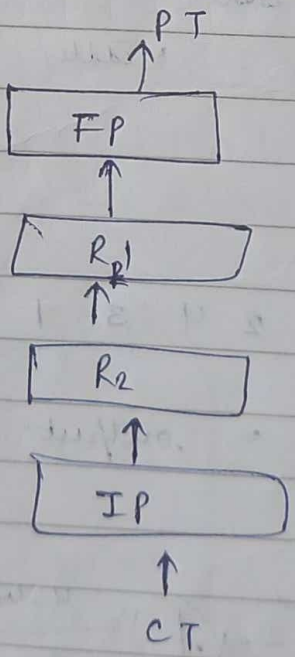




IP : 2 6 3 1 4 8 5 7

FP : 4 1 3 5 7 2 8 6

Decryption -



Example -

PT → 11110010

key → 1011100110

→ Encryption

~~round key~~ -

IP: 2 6 3 1 4 8 5 7

1 0 1 1 1 0 0 1

L_0: 1011 R_0: 1001

L_1 = 1001

k_1: 1 2 3 4 5 6 7 8 9 10

key = 1011100110

~~Expansion~~ :

~~4 1 2 3 2 3 4 1~~

P-Box

3 5 2 7 4 10 1 9 8 6

→ ~~key~~ 1 1 0 0 1 0 1 1 1 0

LS1: 1 2 3 4 5 6 7 8 9 10

1 0 0 1 1 1 1 1 0 0

CP-box: C_1 D_1

6 3 7 4 8 5 10 9

key1 → 0 1 1 1 0 0

~~C_1 = 11001~~ D_1 = 01110

C_1 = 10011 D_1 = 11100

LS2: 1 2 3 4 5 6 7 8 9 10

0 1 1 1 0 1 0 0 1 1

CP-box: 6 3 7 4 8 5 10 9

1 0 1 0 0 1 1

K_2 = 11010011

Round 1 -

$L_0 = 1011$ $R_0 = 100$

$L_1 = 1001$

$R_1 = L_0 \oplus f(R_0, K_1)$

$f(R_0, K_1)$:-

text : $R_0 = 1001$

EP table -

4	1	2	3	2	3	4	1
1	1	0	0	0	0	1	1

XOR :-

$K_1 = 10\ 11\ 11\ 00$

$\oplus$

$11\ 00\ 00\ 11$

$0\ 1\ 1\ 1\ 1\ 1\ 1\ 1$

$01 \rightarrow 1^{st}$ row $\quad 11 \rightarrow 3^{rd}$ row

$11 \rightarrow 3^{rd}$ col $\quad 11 \rightarrow 3^{rd}$ col

$= 0 \quad = 3$

$= 00 \quad = 11$

$o/p = 0011$

P table : 2 4 3 1

0 1 1 0

$R_1 = 1011 \oplus 0110$

$= 1101$

Round 1 o/p = 1001 1101

William Stalling

R_2 : 11011110

$L_2 = R_1 = 1101$

$R_2 = L_1 \oplus f(R_1, K_2)$

$f(R_1, K_2)$:-

$R_1 = 1101$

EP table -

4	1	2	3	2	3	4	1
1	1	1	0	1	0	1	1

XOR :

$K_2 = 11010011$

$\oplus$

11101011

00111000

1st row 1st col = 2 = 10

2nd row 0th col = 3 = 11

o/p = 1011

P - box :

2	4	3	1
0	1	1	1

$R_2 = 1001 \oplus 0111$

= 1110

Round 2 O/p = 11011110

FP: 4 1 3 5 7 2 8 6

= 1 1 0 1 1 1 0 1

CT = 11011101

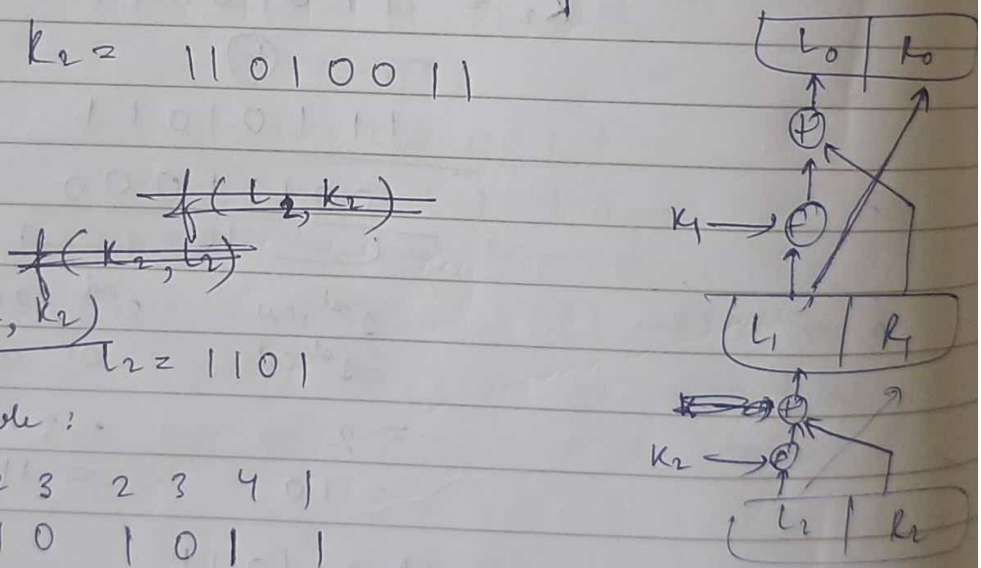
→ Decryption –

IP: 2 6 3 1 4 8 5 7

= 1 1 0 1 1 1 1 0

apply f

K_2 = 11010011



~~f(L2, K2)~~

~~f(K2, L2)~~

f(L2, K2)

L_2 = 1101

EP table:

4 1 2 3 2 3 4 1

1 1 1 0 1 0 1 1

XOR with key –

1 1 1 0 1 0 1 1

1 1 0 1 0 0 1 1

0 0 1 1 1 0 0 0

1st row, 1st col = 2 = 10

2nd row, 0th col = 3 = 11

o/p = 1011

Permutation -

2 4 3 1
0 1 1 1

f = 0 1 1 1
R_2 = 1 1 ⊕ 1 0
L_4 = 1 0 0 1

R_4 = 1 1 0 1

R_0 = L_4
= 1 0 0 1

f (L_4, K_4) :-

L_4 = 1 0 0 1

EP Table :

4 1 2 3 2 3 4 1
1 1 0 0 0 0 1 1

XOR with key -

1 1 0 0 ⊕ 0 0 1 1
K_4 = 1 0 1 1 1 1 0 0
⊕ 0 1 1 1 1 1 1 1

1st row 3rd col = 0 = 00
3rd row 3rd col = 3 = 11

0011

Permutation - 2431

$f = 0110$

$R_1 = 1101$

1011

$L_0 = 1011$

$L_0 = 1011$

$R_0 = 1001$

PT: 4 1 3 5 7 2 8 6

PT = 1 1 1 1 0 0 1 0

Same

DES -

We have 64 bit key

↳ as 8×8 matrix

We want 56-bit key

1 2 3 4 5 6 7 | 8

16

24

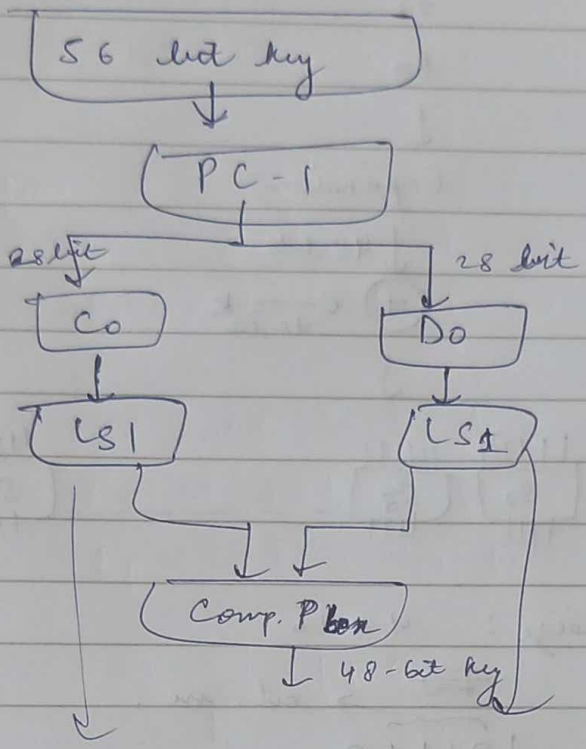
32

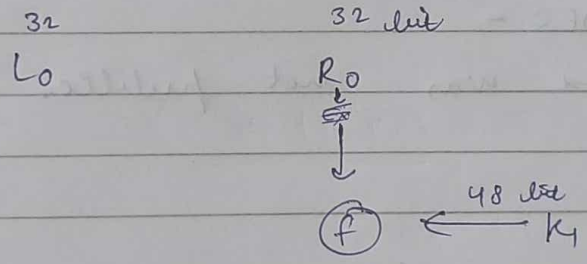
:

:

64

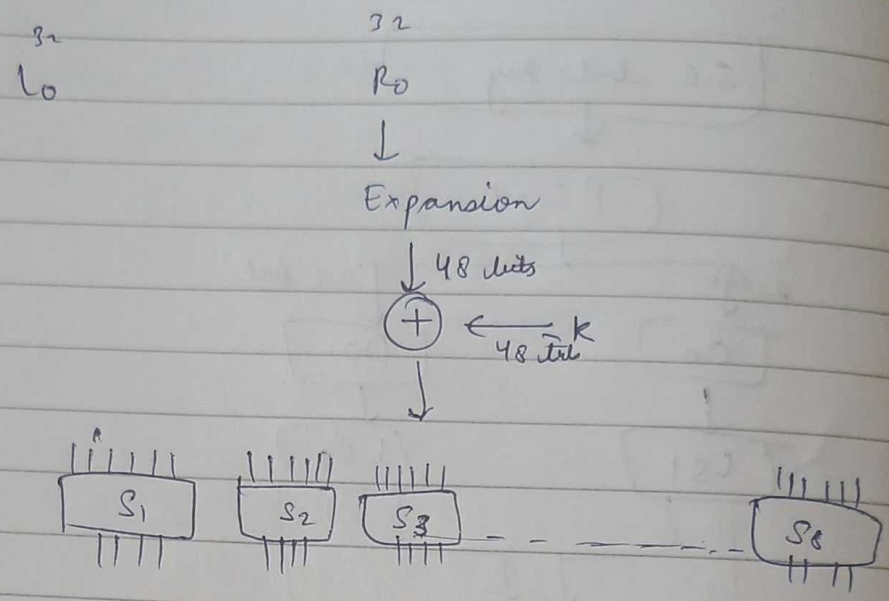
↳ Remove the last col.





R_0 is expanded -

32	1	2	3	4	5
4	5	6	7	8	9
	⋮				



S-box size: 4 × 16

~~10~~ → col. no.

101110

row no.

Problem with DES -

Algo of S-box was not public.