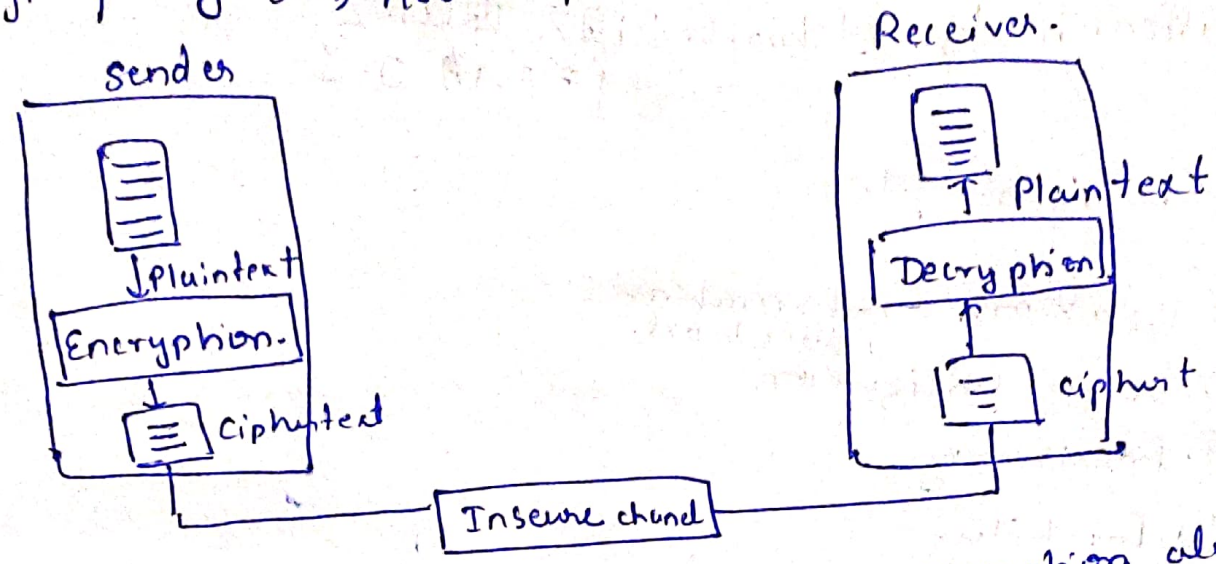
Introduction to CSF

* Cryptography. ⇝ what is Cryptography
⇝ How to prevent attacks on insecure channel.



Cryptography → Art of hiding data using encryption along algorithm. convert for converting plaintext → ciphertext.

Goals & Security.

CIA Triads

① Confidentiality: Prevention of unauthorized access of information assets.
protect data when information assets are in Rest, motion or during use.
#Encryption, access control.

② Integrity: Prevention of unauthorized modification of information assets.
~~when it we accessing data it should be~~
when we are sending data over internet; it doesn't not allow ~~accessible~~ modification in b/w to authorized person.

③ Availability: Ensuring authorized access of information assets when required.
#Backup, # Disaster Recovery
act of prevention of data from distruction of. unauthorized accessed users.

Security Services

Security Services enhances the security of different layers in OSI model.

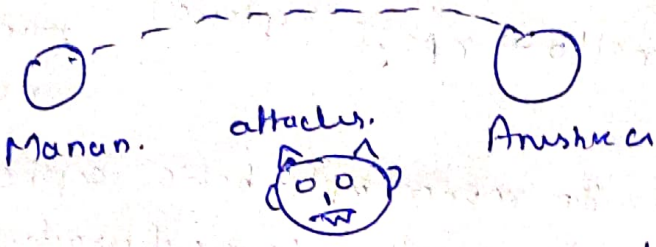
① Authentication ② access control ③ data integrity.

④ Data confidentiality

↳ Find the identity of authorized user.
or proof authorized users.

Types of Attacks.

① Passive attack. ⇒ Attacker will only monitor the data.



(a) Traffic analysis: The volume of data send over network.
The time for which data send on network.

(b) Eavesdropping: Tapping of user system

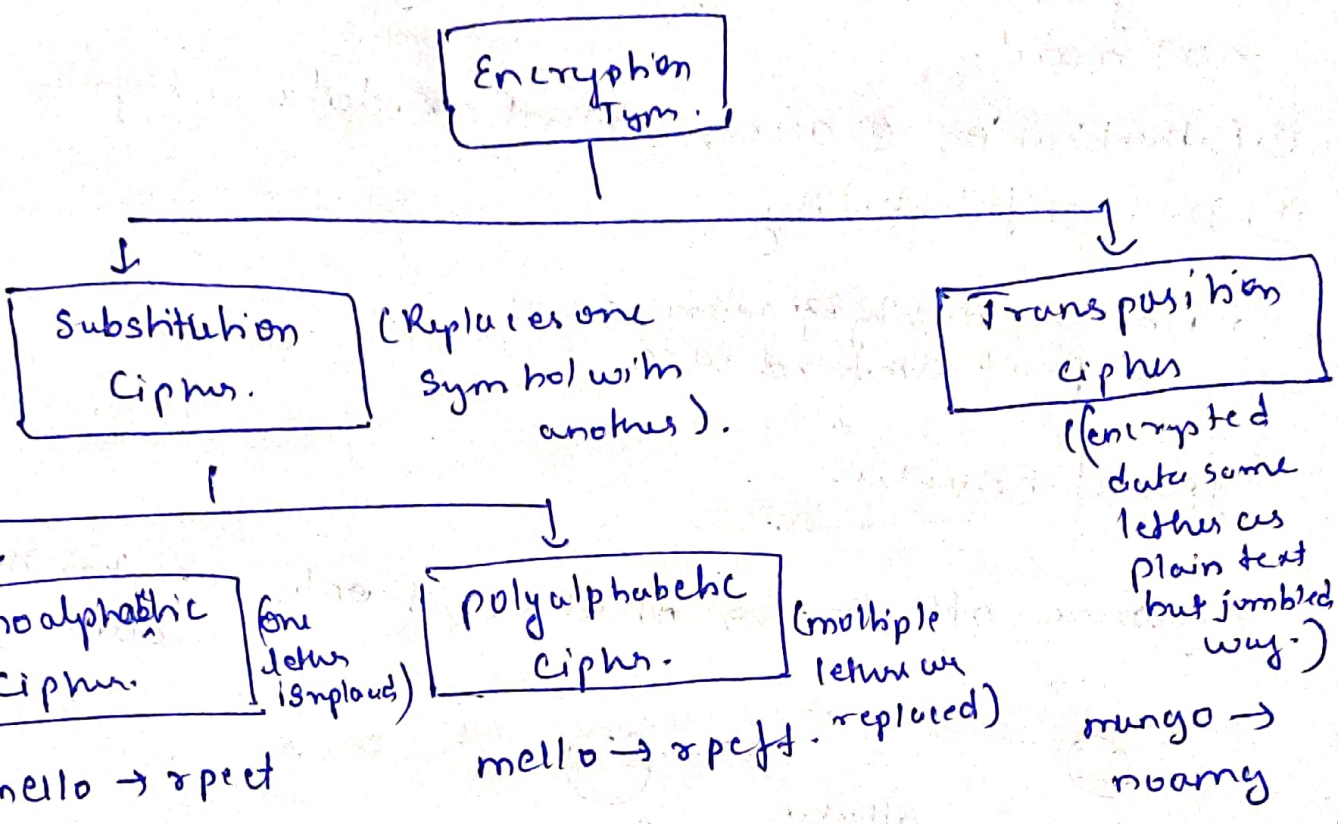
② Active attack ⇒ 1) Attacker can change the data of user.
2) Attacker can also put false data in place of user data.

(a) Replay Attack: steal communication / password packets of user during login and resend that packets in future for ~~Communication~~ performing any type attacks on system.
Eg Facebook login.

(b) Masquerade attack: steal communication packets getting user access to user account. like whatsapp scam emergency money transfer from friend.

(c) DOS attack: Denial of Service
generate extra workload on ~~service~~ server. till server goes off. Attacker doesn't get any benefits in these type of attacks, only these attacks to used to take Revenge.

✱ Data Encryption Techniques.



✱ **monoalphabetic ciphers:-** In monoalphabetic ciphers a ~~characters~~ of plaintext is replace by another same characters in ciphertext. regardless of their position.

✱ **polyalphabetic ciphers:-** Occurance of the plain text is replaced by different letters / substitute in cipher text.

or

each same characters ⟶ different ~~substitute~~ ~~Subsistute~~ Substitute.

① ~~Affine Ciphers~~

Cryptography

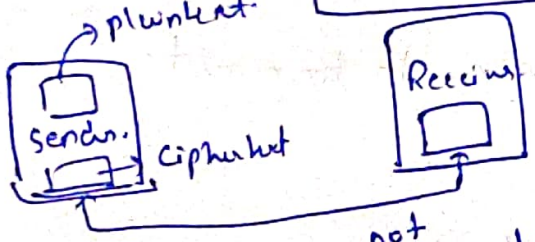
Eg RSA

Symmetric

Same key is used for encryption & description

Disadvantage: ① More No of key's is required for Cryptography.

Secured channel is required for key exchange



② Key is not secured in ~~write~~ transition. as unsecured channel is used during

③ Same key is used to ~~decrypt~~ decrypt the message.

① for N computer (system) it requires $\frac{N(N-1)}{2}$ keys. (each user unique key for communication)

Advantages.

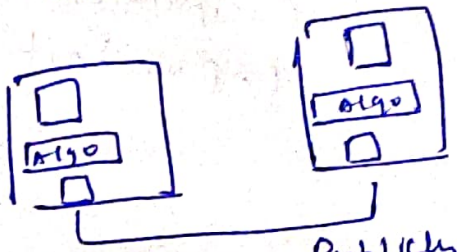
① Encryption is faster.

② Security increase if encryption key is of long size.

Eg DES (Data encryption Standard)
AES (Advanced encryption standard)

Asymmetric

different key is used for encryption & description.



Math

Publicly - available publicly

Public private key - only available to individual either sender/ Receiver.

Public key → encryption
private key → description

publicly → email Id
private key → password.

Eg sender email → Recv.

Advantages

~~Disadvantages~~

① less No. key's are used to manage communication

Disadvantages

② Slower

③ Since both the keys are mathematically connected High Computional powered is required.

★ RSA Algorithm

Rivest Shamir Adleman Algorithm.

ⓐ Perform encryption & Decryption using RSA.

abbreviations

C = ciphertext
P = plaintext

Formulas:

Ciphertext → plaintext

$$C = P^e \bmod n$$

Plaintext → ciphertext

$$P = C^d \bmod n.$$

Variables Required to solve RSA question

(P), (Q), n, (e), ϕ, d, (M) → message to transmit.

- (P), (Q) → given in question
- e → may be given in question
- M → must be given.

Type 1:

e Value given in question.

Qu. $p=7, q=11, M=8, C=17$

Formula 1: $n = p \times q \Rightarrow 7 \times 11 \Rightarrow 77$ ——— (A)

Formula 2: $\phi = (p-1) \times (q-1) \Rightarrow 60$ ——— (B)

Formula 3: ~~To calculate~~ d

$d \cdot e \bmod \phi = 1$ } This rule must be satisfied.

$d \cdot 17 \bmod \phi = 1$

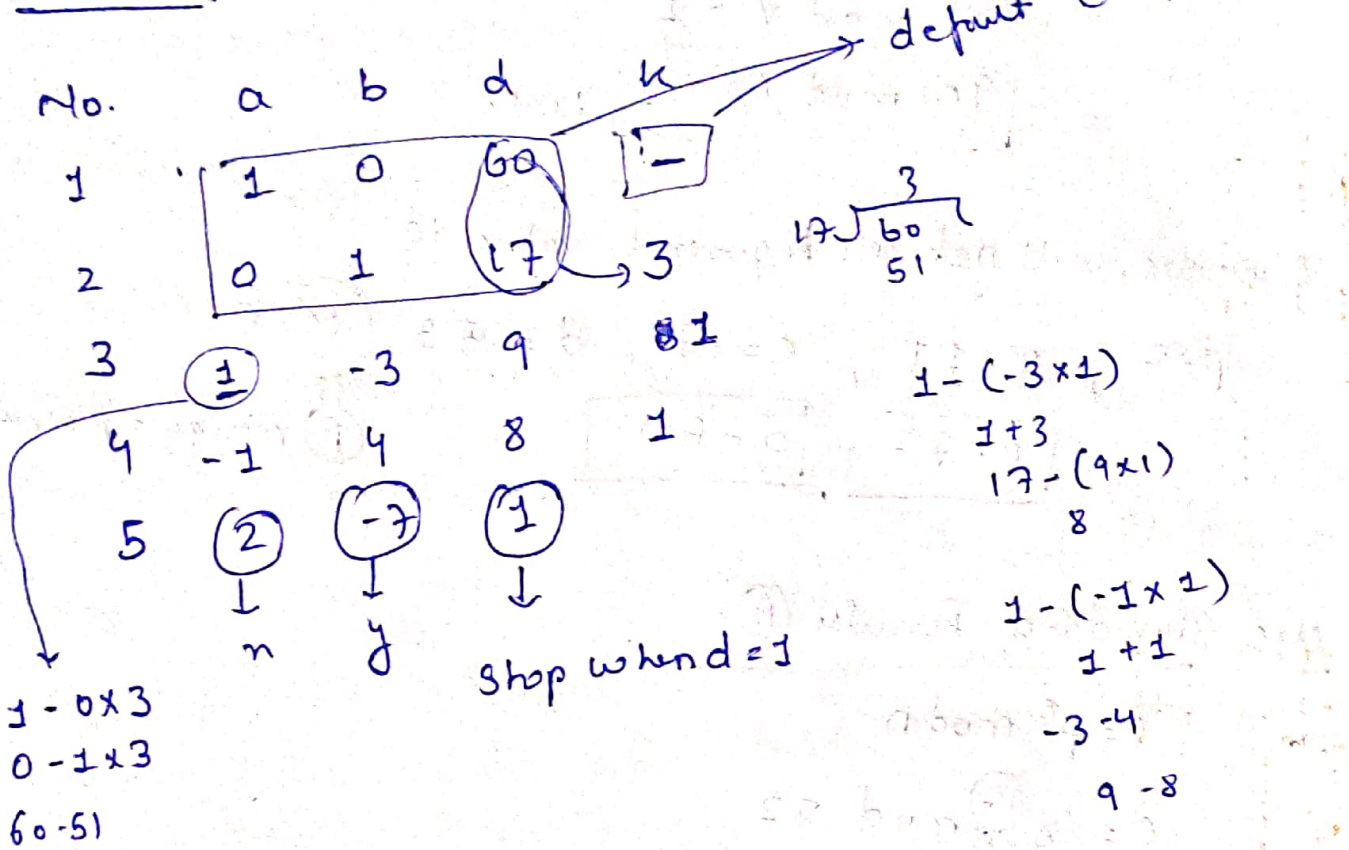
Formula 4: To calculate d

$ax + by = \gcd(a, b)$ where $a = \phi, b = e$

$\phi n + ey = \gcd(\phi, e)$

$60n + 17y = \gcd(60, 17)$ } where to get d in this formula i.e, y=d.

Table



Substitute x and y in above formula.

$60x + 17y = \gcd(60, 17)$

$60(2) + 17(-7) = \gcd(60, 17)$

$120 - 119 = \gcd(60, 17)$

$1 = \gcd(60, 17)$

∴, since $\gcd(60, 17) = 1$

∴ $\boxed{y = -7}$ is correct ✓ but.

$d > \phi$ ← $y = d$ → d = Negative.

$d = d \bmod \phi$

$d = d + \phi$

$\boxed{d = -7 + 60 = 53}$

Now, use formula 3. ie. to verify d value.
if my answer be 1.

$d.e \bmod \phi = 1$

$d.17 \bmod \phi = 1$

$53.17 \bmod \phi = 1$

$901 \bmod \phi = 1$

$\boxed{901 \bmod 60 = 1}$ True.

Now we, will get all Required value ie.

$p=7$, $q=11$, $e=17$, $d=53$, (M) $= 8$

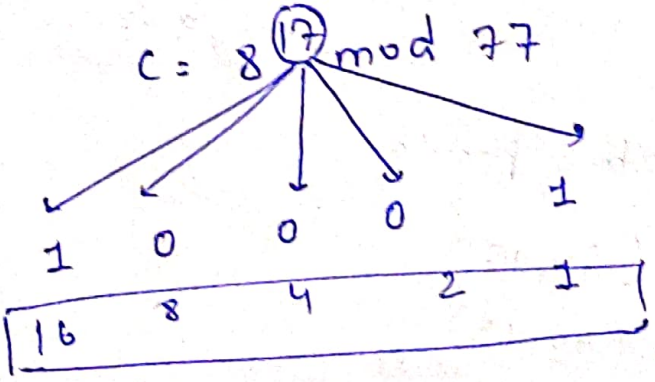
$\boxed{n=77}$, $\boxed{d=60}$

(P) messag = plaintext.

Use Standard Formula (A).

$C = p^e \bmod n$

$C = 8^{17} \bmod 77$



(a) $8^1 \bmod 77 = 8$

(b) $8^{16} \bmod 77 = (8^8)^2 = (71)^2 \bmod 77$

$8^8 \bmod 77 \Rightarrow$
$16777216 \bmod 77 = 71$

$\Rightarrow 5041 \bmod 77 \Rightarrow 36$

$C = (8^{17}) \bmod 77$

8×36

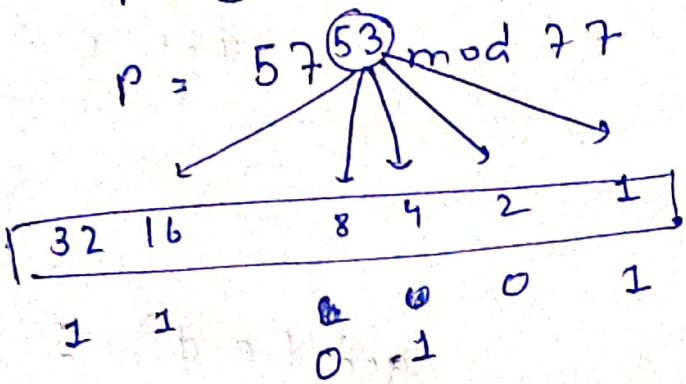
$C = 288 \bmod 77$

$\boxed{C = 57}$

Use standard Formula (B)

$P = C^d \bmod n$

$P = 57^{53} \bmod 77$



(a) $(57)^1 \bmod 77 = 57$

(b) $(57)^2 \bmod 77 = 3249 \bmod 77 = 15$

(c) $(57)^4 \bmod 77 = 10556001 \bmod 77 = 71$

(d) $(57)^8 \bmod 77 = (57^4)^2 \bmod 77 \Rightarrow (71)^2 \bmod 77 = 36$

(e) $(57)^{16} \bmod 77 = (57^8)^2 \bmod 77 \Rightarrow (36)^2 \bmod 77 = 64$

(f) $(57)^{32} \bmod 77 = (57^{16})^2 \bmod 77 \Rightarrow (64)^2 \bmod 77 = 15$

$P = C^d \bmod n$

$P = 57^{53} \bmod 77$

$P = 3885120 \bmod 77$

$P = 8$

Type 2: If e value is not given in question itself

$p = 7, q = 11, M = 8, \phi = 60$

$p = 7, q = 11$
$e = ?\ d = ?$
$\phi = 60, n = 77$

(3) Rules.

Rule 1: $1 < e < \phi$

Rule 2: $\phi = 60$
30×2
$15 \times 2 \times 2$
$5 \times 3 \times 2 \times 2$.

Rule 3: e should not in table of 60.

$\gcd(e, \phi) = 1$

Eg ① ① $1 < (17) < \phi$

② 17 is not in table 60 it's composite

③ 17 is not in table of 60.

$\gcd(17, 60) = 1$

Eg ② we can also select $e = 13$

① $1 < (13) < \phi$

② $\gcd(e, \phi) \Rightarrow \gcd(13, 60) = 1$

RSA Example-1

p=3, q=5, e=3

p=3 q=5
e=3 d=3
ϕ=8 n=15

① $n = pq = 15$

② $\phi(n) = (p-1) \times (q-1) = 8$

③ $d \cdot e \bmod \phi = 1$

$an + by = \gcd(a, b)$

$\phi x + ey = \gcd(\phi, e)$

$8x + 3y = \gcd(\phi, e)$

S.No.	a	b	d	k
1.	1	0	8	
2.	0	1	3	2
3.	1	-5	0	0
4.	0	1	3	0
5.	1	-5	0	0
6.	0	1	3	0
7.	1			

SNO.	a	b	d	k
1.	1	0	8	-
2.	0	1	3	2
3.	1	-2	2	1
4.	-1	3	1	2
	x	y		

1 - (-2×1)
1 - (-2) = 3
3 - (2×1)

$8x + 3y = \gcd(8,3)$

$8(-1) + 3(3) = \gcd(8,3)$

$-8 + 9 = \gcd(8,3)$

$1 = \gcd(8,3)$ condition satisfied.

$y = d = 3$

$d > \phi$

$d = d \bmod \phi$

$d = -ve.$

$d = d + \phi$

None of condition are true $\therefore$ $d = 3$

Now

$p = 3$, $q = 5$

$d = 3$, $d = 3$

$\phi = 8$, $n = 15$

$M = 2$ Given.

Now Formula (A) $C = P^e \bmod n$

$C = 2^3 \bmod 15$

$C = 8$

Formula (B) $P = C^d \bmod n$

$P = 8^3 \bmod 15$

$P = 2$ = M given in question.

RSA Example-2

Qy $p = 11$, $q = 7$

$e = 37$ $d = ?$ (13)

$\phi = 60$ $n = 77$.

Formula 3 $d.e \bmod \phi = 1$

$d.37 \bmod \phi = 1$

$an + by = \gcd(a, b)$

$\phi n + ey = \gcd(\phi, e)$

$60n + 37y = \gcd(60, 37)$

S.No.	n	y	d	k
1.	1	0	60	-
2.	0	1	37	1
3.	1	-1	23	1
4.	-1	2	14	1
5.	2	-3	9	1
6.	-3	5	5	1
7.	5	-8	4	1
8.	(-8)	(13)	(1).	

$2 - (-3) =$

$23 - 14 \times 1$

$-1 - (2 \times 1)$

$-1 - 2$

$1 - (-1)$

$1 - (-1 \times 1)$

$1 - (-1)$

~~$-1 * ($~~

$-1 - 2$

$2 - (-3) = 5$

$-3 - 5 = -8$

~~$-3 * 5$~~ $-3 - 5$

$5 - (-3)$

$5 - 4 =$

$60n + 37y = \gcd(60, 37)$

$60 \times (-8) + 37(13) = \gcd(60, 37)$

$-480 + 481 = \gcd(60, 37)$

$1 = \gcd(60, 37)$ Proved.

$\therefore y = d = 13$