7/7/25

1. Introduction to Network Security and Cryptography.

Outline
→ Basic Concept of Computer & Nw. Security
→ Security Goals.
→ Security Threats & vulnerabilities.
→ Access Control & Attacks.
→ OSI Security & Architecture.
→ Security Services, Security mechanisms.
→ classical encryption technique.

Substitution
a) Mono-alphabetic
b) poly-alphabetic

Transposition
a) keyed (columnar Er
b) keyless (Rail fence zig z

Vignere cipher — Playfair cipher — Hill cipher

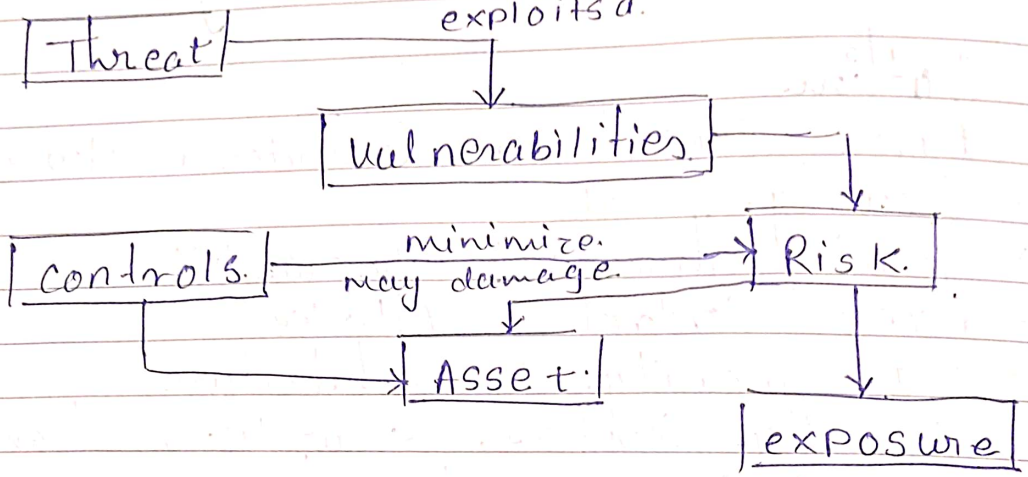
→ Introduction to Steganography.

Complete Security: generic name for collection of tools design to protect data and ~~tools~~ to ~~thwart~~ ~~hacker~~ thwart hackers.

Network Security: Measures to protect a data during transmission.

Internet Security: Measures to protect data during their transmission over a collection of inter-connected networks.

Terminologies in CNS.



① Assert - are Something that has value & is worth protecting.

② Controls. (or. Countermeasures) - Any. Countermeasures or actions that you take to safeguard an. assert are called controls.

③ Threat: A threat is a person or any. entity that can exploit an asset by. pairing your. controls.

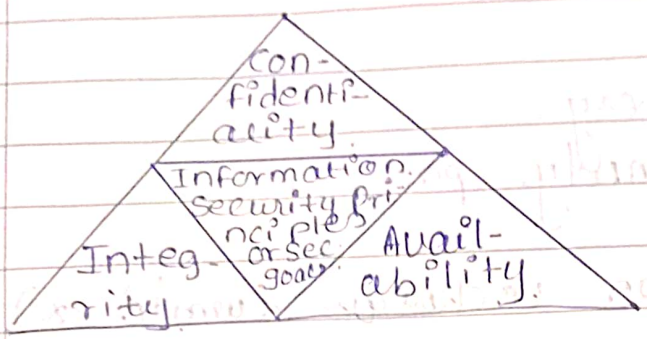
④ Vulnerabilities:- is the. weakness or lack of. Controls around assets.

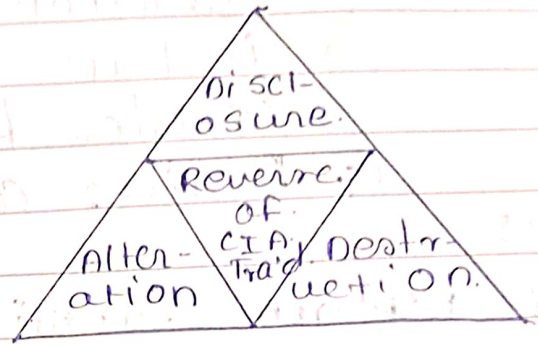
⑤ Risk: The. likelihood of a harm occurring to an. assert

⑥ Exposure ÷ It is an instance of being harmed.

3 pillars of Security. (goals of Security)

CIA [confidentiality, Integrity, Availability]
CIA traid





① Confidentiality.
⇒ an act of protecting information from unauthorized destruction to an entity.

* Information Should be.
1] protected at Rest: when Stored on disk
2] Protected in Motion: when transmitted over Network
3] Protected during use: when processing.
   a] Encryption
   b] Access Control
   c] Data classification.

② Integrity:
⇒ an act of protecting information from unauthorized modification by an entity.
mechanisms used are ~~of~~ Security.
① Hashing.
② Access Control.
③ Data classification.
④ Input & Output Sanitization.

③ Availability:
=> an act of protecting information from unauthorized destruction by an entity.
① Access control.
② Isolation.
③ Backup
④ Disaster Recovery.
⑤ Busines continuity processes.

8/07/25
10M. Q Explain Substitution technique (write ex).

I Substitution techniques.

① Caesar Cipher
→ Letters are replaced by other letters or Symbols.
→ It is the simplest method used by Julius Caesar
→ Replacing each letter of the alphabet with letter standing 3 places further down the alphabet.

0	1	2	3	4	5	6	7	8	9	10	11	12
A	B	C	D	E	F	G	H	I	J	K	L	M

13	14	15	16	17	18	19	20	21	22	23	24	I
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

CT = Ee (P, 3) (+). PT = W X Y Z
PT = D (C, 3) (-) CT = Z A B C.
= (PT+3) mod 26
22+3 25 mod

plaintext.	ciphertext.
I like security.	LBLN.H. VHFXULWB
Apple	DSSOH.
23456	56789.

② Mono alphabetic cipher.

→ There will be not uniform key.
→ A single cipher alphabet (mapping from plain alphabet to cipher alphabet) is used per message.
→ English language - Nature of plaintext is known
→ Better security than caesar cipher.
→ They are easy to break because they reflect the frequency data of the original alphabet.
→ prone to guessing attack using the english letter frequency of occurrence of letters.

PT	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
CT	F	I	G	L	P	A	K	M	Q	S	B	H	V	U	Y

P	Q	R	S	T	U	V	W	X	Y	Z
T	Z	X	W	E	J	H	D	R	O	C

Eg. PT = INFORMATION.
QUAYXVFEQYU.

Monoalphabetic cipher frequency Analysis method

Frequency analysis is a technique used to break mono alphabetic cipher by studying the frequency of letter or grp of letter in cipher text it exploits the fact that in any given language appear more frequently then others typical frequency of letter in english.

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

Steps:

1) Count the frequency of each letter in the CT
2) Compare with standard english letter frequency
3) Make educate guesses for substitutions.
4) Use known word patterns. (e.g. The AND, IS) to refine guesses
5) Count- continue iterating until the messg is deciphered.

Example

ciphertext: ZPV IBWFBTF DVSF MFTTBHF.

Frequency analysis may suggest
Z → Y P → O V → U etc.

Guessing, ZPV → YOU
IBWF → HAVE

YOU HAVE A SECURE MESSAGE

9/07/25

Vignere cipher

→ It is a multi letter encryption technique
→ It consists of the 26 caesar cipher with shifts of 0 through 25

Method 2: Encryption process

$$C_i = (P_i + K_i \bmod m) \bmod 26$$

Decryption

$$P_i = (C_i - K_i \bmod m) \bmod 26$$

Method 1 - Vignere Table

→ Uses vignere table where alphabets are arranged in rows and column. Just write A-Z skipping one alphabet from left at a time in a row.

PT = I AM FINE OK
KEY = DONE

PT	I	A	M	F	I	N	E	O	K	
key	D	O	N	E	D	O	N	E	D	
	L	O	Z	J	L	B	R	S	N	

plain text: APPLE
Security key: SNOW
Algorithm - Vignere cipher.

PT	A	P	P	L	E
K	S	N	O	W	S
CT	S	C	D	H	W

zainab

Method 2:

PT	A	P	P	L	E	
P'value	0	15	15	11	4.	
key	S	N	O	W	S	
k'value	18	13	14	22	18	
CT.	18	28	43	7	22.	

Q Solve using Vignere cipher algorithm

1] PT = ATTACK AT DAWN.
Key = LEMON. ~~LEMON. LE~~

2] PT. = GIVE MONEY
key = LOCK. ~~LOCKL~~.

3] PT = SHE IS LISTENING.
Key. = GOOD.

~~Poly alphabetic cipher~~

→. PT A T T A CK A T D A W N.
Key L E M O NL E M O N L E
CT. 11 23 16.14.15 21 4 5 17 13 7 17.
L X Q O P V E F R N H R

PT G I V E M.O N E Y.
Key L O C K L O C K L.
CT

PT S H E I S L I S T ENFI N G.
Key G O O D G O O D G O O D G O
CT

PT. = EASTORWEST.
key REGIONREGI.
CT = ?

Encryption Technique.

PT.	E	A	S	T	O	R	W	E	S	T.
P'value	4	0	18	19	14	17	22	4	18	19.
key	R	E	G	I	O	N	R	E	G	I.
K'value.	17	4	6	8	14	13	17	4	6	8
C'value.	21.	4	24	1	2	4	13	8	24	1.
CT.	V	E	Y	B	C	E	N	I	Y	B.

Decryption (C-K) mod 26.

CT.	V	E	Y	B	C	E	N	I	Y	B
C'value	21	4	24	1.	2	4	13	8	24	1.
~~K'value~~ key	R	E	G	I	O	N	R	E	G	I.
K'value	17	4	6	8	14	13	17	4	6	8
P'value	4	0	18	19	4	17	22	4	18	19.
PT.	E	A	S	T	O	R	W	E	S	T.

Hill Cipher

→ It is poly-alphabetic substitution cipher based on linear algebra algorithm.

1] Arrange the key and the plaintext in a matrix format.
2] Carry out multiplication of the key and plaintext
3] Perform mod 26 operation on the resultant multiplication.
4] Use the table again to convert numbers back to alphabet.

5] There alphabet represent Ciphertext

Example: Encrypt the message "EXAM" using Hill cipher with the key. $\begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}$ $\begin{pmatrix} J & E \\ F & H \end{pmatrix}$

Soln: PT = EXAM → Convert into matrix

$\begin{bmatrix} 4 & 0 \\ 23 & 12 \end{bmatrix}$ $\begin{pmatrix} E & A \\ X & M \end{pmatrix}$

Multiply the key & PT matrices

$$\begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} * \begin{bmatrix} 4 & 0 \\ 23 & 12 \end{bmatrix} = \begin{bmatrix} 128 & 48 \\ 181 & 84 \end{bmatrix}$$

Perform mod 26 operation

$$\begin{bmatrix} 128 & 48 \\ 181 & 84 \end{bmatrix} \bmod 26 = \begin{bmatrix} 24 & 22 \\ 25 & 6 \end{bmatrix} \begin{bmatrix} Y & W \\ Z & G \end{bmatrix}$$

CT = Y W G

Hill Cipher

Encrypt the message DEE using Key $\begin{bmatrix} 2 & 4 & 5 \\ 9 & 2 & 1 \\ 3 & 8 & 7 \end{bmatrix}$

DEE - $\begin{bmatrix} 3 \\ 4 \\ 5 \end{bmatrix}$

Multiple Key & plaintext

$$\begin{bmatrix} 2 & 4 & 5 \\ 9 & 2 & 1 \\ 3 & 8 & 7 \end{bmatrix} \times \begin{bmatrix} 3 \\ 4 \\ 5 \end{bmatrix} = \begin{bmatrix} 47 \\ 40 \\ 96 \end{bmatrix} \bmod 26 \begin{bmatrix} 21 \\ 14 \\ 24 \end{bmatrix}$$

CT = V O Y

* playfair algorithm
  5 × 5 = 25 alphabets 26

~~I/p~~
I/p PT & key Guest
use key

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

Solve using playfair cipher

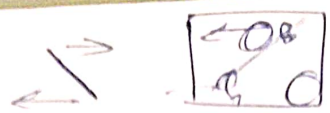
① key = MONARCHY
PT = ATTACK.

② Given key = MONARCHY
Draw 5×5 matrix of the above key

~~M~~ O N A R
C H Y B D
~~E~~ ~~F~~ G ~~H~~ ~~I/J~~
I J K

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

② Pair the plaintext
PT = ATTACK
= RSSRDE



use playfair cipher to encrypt the word GREET using key-word moon mission

KEY = MOONMISSION
PT = GREET

① Given key = MOONMISSION.
Draw 5×5 matrix of the above key

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

② pair the plain text
PT = GREET
= GR EX ET
= HQ CZ DU

Key = GUJAR
= SURGICAL STRIKE

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

PT = SU RG IC AL ST RI KE
PA GU UQ IM TO GA MC

EGE

Q. Encrypt the using playfair cipher + steps 10M

Diff between monoalphabetic & poly-alphabetic

Monoalphabetic	polyalphabetic
① Not more secure can be easily broken	① It is more secure and hard cannot be easily broken.
② One fixed alphabet is used.	② More than one alphabe
③ Same Substitution rule is used for each ST.	③ The substitution rule changes continuously by letter to letter according to the elements of encryption key
④ In MA for particular only one substitution can be used.	In polyalphabet for particular diff Substitution can be done using Vignere

* Cryptography

Transposition technique:

In this technique, position of characters jumbled up (mixed up) like a letters arranging game. The two techniques are

a) keyed and b) keyless.

In keyed transposition a random key is used to describe the transposition sequence & carry out the transposition over algorithm ① Arrange the plaintext in a column under the given key

② Rearrage the PT columnwise in keys alphabetic order. [The key can be a number ranging between 0 to 9].

Eg. 563214 [NO no. are repeated.

use the key, 'ENCRYPT' to "Save the king from attack."

E	N	C	R	Y	P	T
2	3	1	5	7	4	6
S	A	V	E	T	H	E
K	I	N	G	F	R	O
M	A	T	T	A	C	K

CT = 1 2 3 4 5 6 7

= VNT SKM AIA EGT EOK TFA HRC.

Q. Solve using columnar transposition technique.
key = SORROW
PT = Demonetization tonight

S	O	R	R	O	W
5	1	3	4	2	6
D	E	M	O	N	E
T	I	Z	A	T	I
O	N	T	O	N	I
G	H	T			

CT = 1 2 3 4 5 6
EINHNTNMZTIOAODTOGEII

In this technique a transposition is described without a random key. It is also known as rail fence reference cipher. Since it uses the rail size a key and does not use a random

Algorithm:
① Based on rail fence arrange the PT.
② Rearrange the PT row wise to get the CT.

Q. Encrypt the plaintext "save the king from attack" using railfence cipher. assume suitable railsize.

Q railsize = 3 (rows)
depth

rs1	S				T				I				R				T									k
rs2		A		E		H		k		N		F		O		A		T		C					
rs3			V				E	.			G.				M				A							

CT = STIRTKAEHKNFOATCVEGMA

Q. PT = DEMONETIZATION TO NIGHT
railsize = 4

rs1	D						E				T						I		O						G	
rs2		E				E		T		I				T		I		N				I		G		
rs3			M		N				Z			T			T		N									
rs4				O							A					O										

CT = DTOGEEIINIHMNZTTNTOAO

GN ⇒ Steganography.

It is practice of concealing a msg within another msg common image or file the info is only hidden & not encrypted. The hidden is so non-obvious that it is difficult to discover it by anyone who is unaware of the presence of the hidden info. only who knows what to look for and where can lookout for the hidden info.

They are many diff methods of performing Steganography. The most famous of all the one that modifies only the images,

audio or videos. It is difficult to make out any difference betn the file with modified LSB's and files where LSB's are not modified. hence the info can be transfered hidden. where generally there files are not considered harmful or are thoughly inspected for finding info transfer.

uses of steganography

1. Leak corporate busifiers or personal datas without being caught by firewall, IDS or other detection mechanism.
2. sending info special grp without knowledge of other
3. Attacking users with hidden malicious code in the downloaded media files.

* Diff.

Cryptography	Steganography
Info is transferred. (PT → CT)	Info is hidden.
Transfered info is visible.	Hidden info is not vissible.
Provides confidentiality, Integrity, Non-repudiation.	Only confidentiality
Various recognized & approved algorithm are used.	No such specific algo. used.

18/07/25

OSI Security Architecture

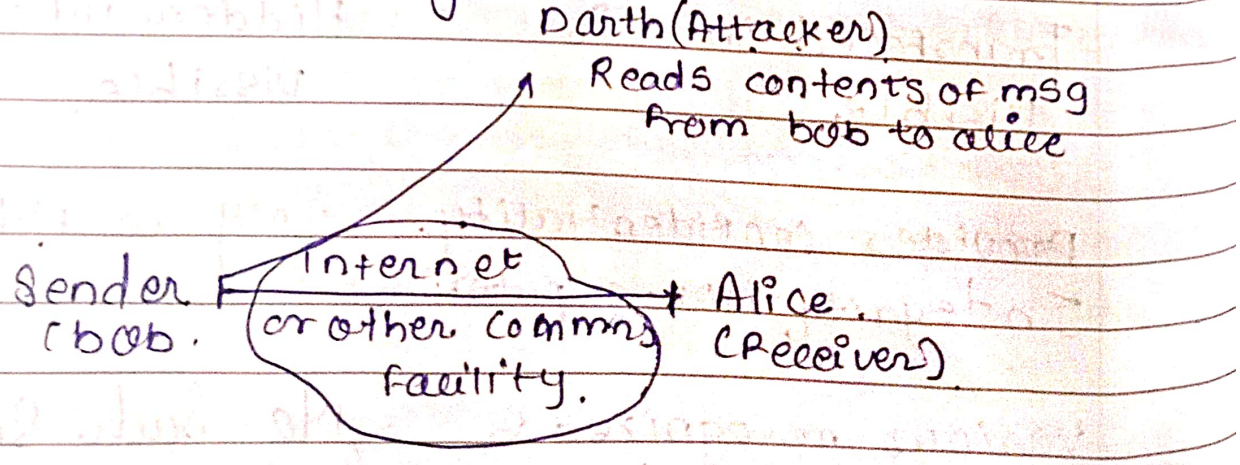
Security attacks.
Security Mechanism
Security Services.

TYPES OF ATTACKS.

- Passive
  - Release of Msg content
  - Traffic Analysis
- Active
  - Masquerade
  - Replay attack
  - Modification of msg
  - Denial of Services

- Passive attack makes attempt to collect info from the System but doesn't modify. alter the System data all the resources. is an e.g of passive attack Eaves dropping. or just monitoring of info. The goal of opponent there to gain the info that is being transmitted.

i) Release of Menage contents



ii). Traffic Analysis

The opponent is able to capture the contents of the msg. but not attack the extract the info from the msg.

The opponent (attackers) might observe the pattern of msgs to get the location or any clue regarding in origin of msg passive attacks are difficult to detect bcz they do not involve modification of info.

Attackers aim is such type of attack active is to corrupt or destroy the data. as well as.

① Masquerade takes place when an attack pretends to be an authentic user.

It is generally done gain accen to a system or steal imp data from system. Such login id or pass or authentic user to gain accen to your Network

② Replay attack

A Replay attack is also known as playback attack attacker repeatedly keep transmitting data to make the network jam. or delay the transition of data. transmission of data R.A involves passive capturing of data and retransmission of subsequent info in order to create unauthorize effect.

Modification of Messages.
In modification the original data that has been sent by authentic user is been disrupt or modified by attacker to make it non meaning-full for the receiver usually the content sequence is been change.

Denial of Service.
Denial of Service Means making the net unavailable for a user those who want to communicate. ~~Securly~~ Securely.

Q Diff bet^n passive & Active

Active	Passive
① Attacker needs to have physical control of the media or network	Attackers merely needs to observe communication in the network or media.
② It can be easily detected	It cannot be easily detected.
It affect the System.	It does not affect the System.
It involves in modification of data.	It involves in monitering of data.
It does not check for loopholes or vulnerabilities.	

It is difficult to prevent network active attack.

07/25.

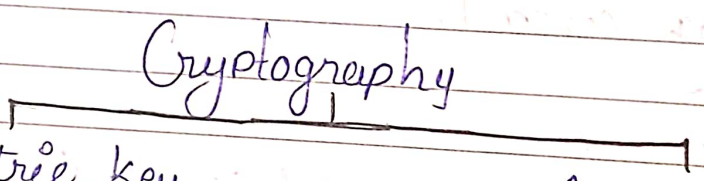
Security Mechanism

1. Encipherement.
2. Digital signature.
3. Acces control.
4. Data integrity.
5. Authentication exchange.
6. Traffic padding
7. Routing control.

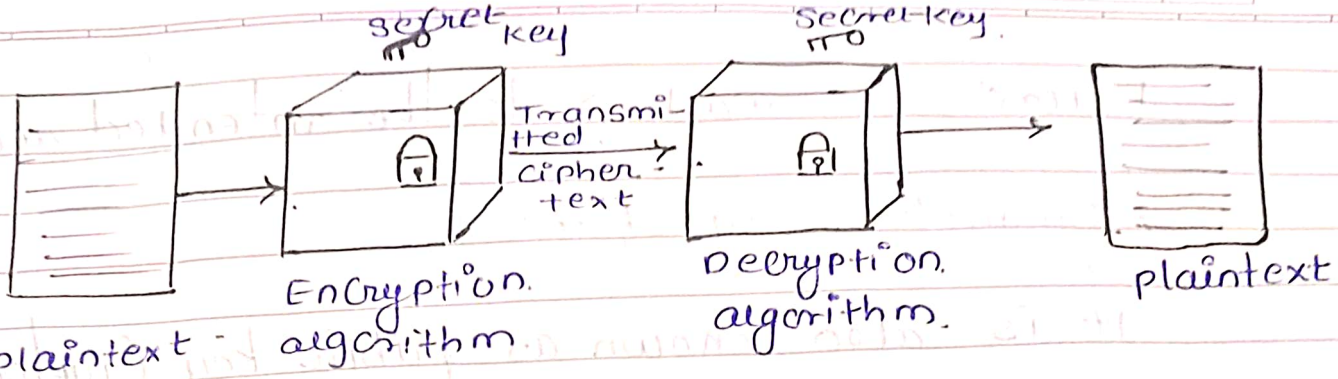
Chp. Cryptography. key. management, distribution & User authentication.

Outline

- Block cipher modes of operations
- DES
- AES
- RC5 Algorithm.
- Hashing techniques - SHA256, SHA-512
- HMAC & CMAC
- Digital Signature Schemes - RSA, DSS, Remote user authentication protocols. kerberos.
- Digital Certificate - X.509, PKI.



1) Symmetric key.
- Also called as "Secret key. Cryp"
- A Single key is used for encryption & Decryption
- As shown in diagram Sender encrypt. plaintext using. shared key. & resultant ciphertext is transmitted through communication medium such as te internet., at the receiver side the ciphertext is decrypted. using. same. Secret key. to obtained original. plaintext.
- Example. DES & Data Encryption Standard), Blowfish AES. Stream and block cipher.



- Mathematically represented as blowfish AES Stream & block cipher.

$P = D(K, E(P))$

where P = P.T, E(P) = encryption of P.T

~~D(K, E(P))~~ D(K, E(P)) = Decryption.

Advantages:

- It is faster than asymmetric
- Because of simple key. data cannot decrypt easily at receiver side even if intercepted by attacker
- Receiver should have same key to decrypt.
- Symmetric key achieve the authentication principle before it checks receivers identity
- System resources are less utilised.

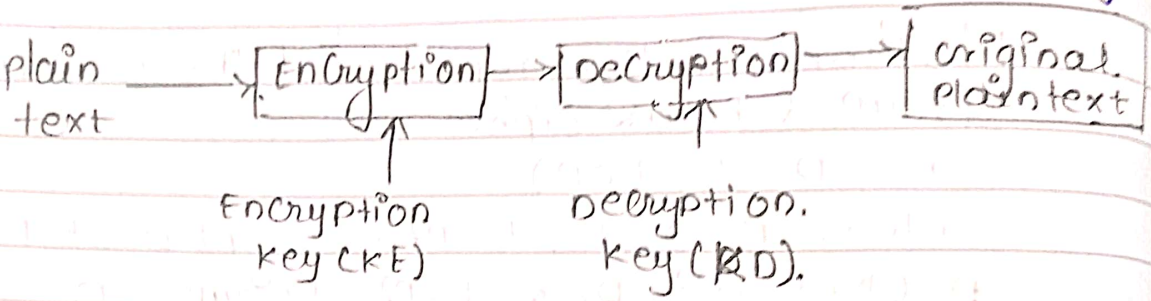
Disadvantages:

- Once the key is stolen while transmitting data between sender & receiver it is very easy to the decrypt the msg, as same key is used for encryption & Decryption
- key is transmitted first & then msg is transmitted to the receiver if the attacker intercept the communication between sender & receiver then he decrypt the msg.

before it reaches to the intended receiver.

2) Asymmetric Key [Public]

- It is also known as public key Cryptography



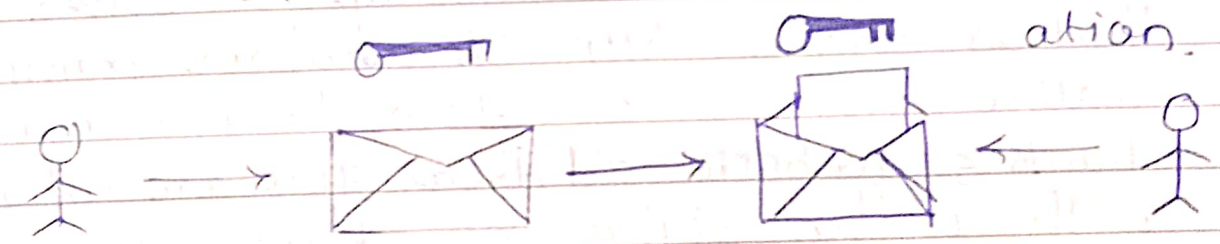
- Two keys are used as shown in above diagram once for encryption & another for decryption.
- It is represented as P = D(kd, E(ke, P))
  ke = encrypt key kd = decrypt key
- for example : RSA & Diffie Hellman key exchange algorithm.

Advantage.

- key can't be distributed among the sender & receiver as both of them have own keys, so there is no problem of key distribution while transmitting a data over secure channel.
- Main advantage is that two seperate key are used for encry and decrypt even if encryption key is stolen by attacker he/she can't decrypt the msg as decryption key is available with receiver only.
- Easy to use for user and scalable as much administrative work is not require

Disadvantage:
- More transmission time is required
- more resources required

key used.	corresponding key required	Security service provider
Encryption public key.	decryption : private key	confidentiality
private key.	public key.	Authentication & non repudiation.



Encrypted msg with user B public key

Msg. Decrypted with user B's private key.

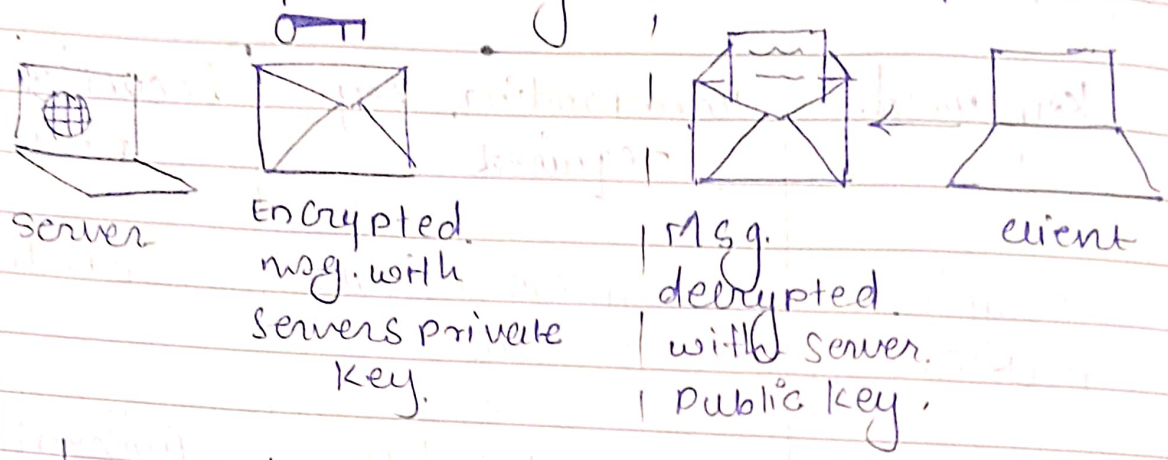
Consider the two use cases of asymmetric keys

1] Use Case 1 : user A wants to send a secret message to user B.

user A knows : user A's public & private key
user B's public key.

user B knows : User A's public key, user B's public & private key.

2] use case 2: It provide authority & authentication keys for providing authentication



This is highly used today. For server Validation that is using https:// another example is online transaction How do you ensure Bank's website address you are interacting with is the right one. This is what precisly asymmetric helps you to solve client want to authenticate the server. before it begins the transaction. It sends a server a PT msg and ask it to encrypt with its private key. If server encrypts the msg. that which client sends with its. private key and sends it back to the client. client uses the world known public key of the server and decrypt the msg. it receives from the server if the msg. get sucessfully decrypted and it matches with what the client send. earlier to the server encrypt the client has validated. it is indeed interacting with the authentic server no one else would. have known the server's private key

The client is satisfied and it becaure: becomes Secure
So we conclude that assymmetric keys can be used for authentication and non repudiation.

Comparison Attributes.	Symmetric keys	Asymmetric key
Speed	High	Low
complexity	low	high
Number of keys	high	low
key distribution	problematic	Easier.
Security services	Confidentiality	Confidentiality Authentication Non-repudiatio

cipher

Block.
Grp of bits
→ Block / byte

Stream cipher
bits by bits.

① Confusion – Substitution.
② Diffusion – Transposition or permutation
③ Feistal Structure (Round).

① Confusion - Substitution
② Diffusion - Transposition or permutation
③ ~~Feistal Structure, fiestal. Structures~~
formula: $L_i = R_{i-1}$ $R_i = L_{i-1} \times OR\ F(R_{i-1}, K_i)$

Simple Example (2-Round feistal cipher)

Assume:

plaintext = [L0, R0] = [1010, 1100]

key 1 = 0110, key 2 = 0011

let F [R, K] = R XOR K.

Round 1:

L1 = R0 = 1100

R1 = L0 XOR F[R0, key1] = 1010 XOR [1100 XOR 0110] = 1010

1010 XOR 1010 = 0000

Round 2:

L2 = R1 = 0000

R2 = L1 XOR F(R1, key2] = 1100 XOR [0000 XOR 0011

= 1100 XOR [0011] = 1111

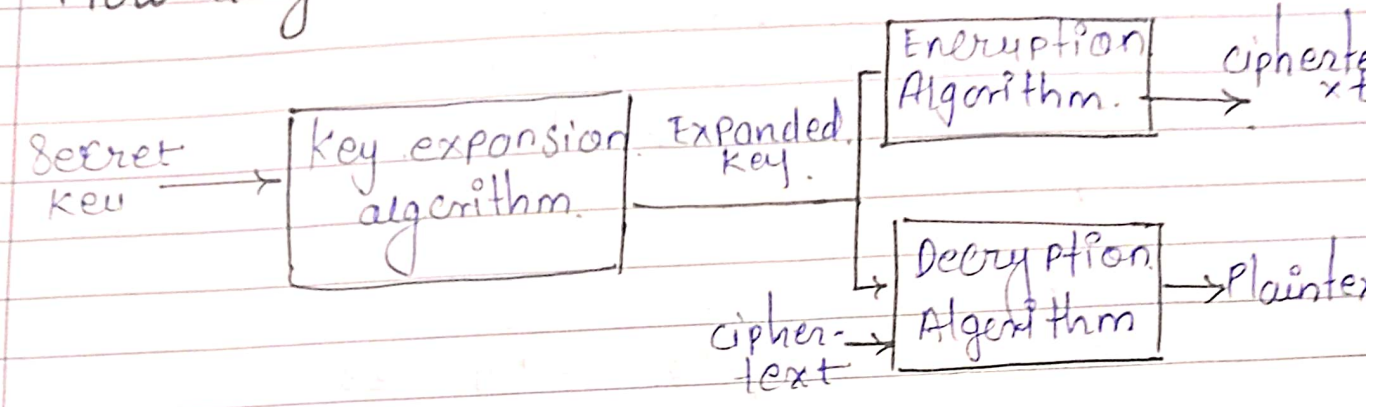
ciphertext = [L2, R2] = [0000, 1111]

DES [Data Encryption Standard]

C0 (First 28 bits): 00-010010 01101001 01011011 1100

C1: 00100100 01010010 10110111 1000.

Flow diagram of Rivest Cipher 5 (RC5).



RSA Algorithm. Rivest Shamir Adleman

1) Consider 2 large prime nos p & q.
2) Calculate the product say $N = p * q$
   calculate $\phi(n) = (p-1) * (q-1)$
3) Assume e such that $gcd(e, \phi(n)) = 1$
4) Assume d such that $d = e^{-1} \bmod (n)$. $d = 1 \bmod \phi($
   $[d \times e = 1 \bmod \phi(n)$
   $d \times e \bmod \phi(n) = 1 \bmod \phi(n)$
   $[d \times e \bmod \phi(n) = 1]]$
5) Publickey = {e, n} Private key = {d, n} n=40 m=16 m=10
6) Encryption m - message ($m < n$). m = ----
   $c = m^e \bmod$
7) Decryption. $m = C^d \bmod \phi(n)$

Example $p = 3$ $q = 5$

1) $n = p \times q = 3 \times 5 = 15$.
2) $\phi(n) = (3-1) \times (5-1)$
   $= 2 \times 4 = 8$.
   $e = 3, 5, 7$.
3) $e = 3$ $gcd(3, 8) = 1$.
4) Compute d.
   $d \times e \bmod \phi(n) = 1$.
   $d \times 3 \bmod 8 = 1$.
   $3 \times 3 \bmod 8 \neq 1$.
   $4 \bmod 8 = 1$

5) Public key. = {3, 15}
Private key. = {3, 15}

6) Encryption $m = 4 < 15$

$C = 4^3 \bmod 15$

$C = 4.$

Example $p = 3$ $q = 11$

Compute $n = p * q = 3 * 11 = 33$

Compute $\phi(n) = (p-1) * (q-1) = 2 * 20 = 20$

choose e such that $1 < e < \phi(n)$ and e and $\phi(n)$ are coprime. let $e = 7$.

Compute a value for d such that $(d * e) \text{ MOD } \phi(n) = 1$ one. Solution is $d = 3 (3 * 7) \text{ Mod } 20 = 1$.

public key is $(e, n) => (7, 33)$

private key is (d, n) $(3, 33)$

The encryption of $m = 2$ is $C = 2^7 \text{ mod } 33 = 29$

The decryption of $C = 29$ is $m = 29^3 \text{ MOD } 33 = 2$

Solve, using RSA algorithm

Given $p = 13$ $q = 11$. $m = 13$ (plain text)

Calculate, e, d, encryption & decryption.

① $N = p \times q = 13 \times 11 = 143.$

② $\phi(n) = (13-1) * (11-1) = 12 \times 10 = 120.$

③ Select $e = 13$ gcd $(13, 120) = 1.$

④ Calculate d.

Do the following procedure till you are getting an integer.

$$d = \frac{(\phi(n) * i) + 1}{e}$$

$i = 1$ $d = \frac{120 \times 1 + 1}{13} = \frac{121}{13} = 9.30$

$i = 2$ $d = \frac{241}{13} = 18.5$

$.1 = 8$ bcoz p

$i=3 \quad d = \frac{361}{13} = 27.76$

$i=4 \quad d = \frac{481}{13} = 37$

5) Public key = $\{e, N\} = \{13, 143\}$
private key = $\{d, N\} = \{37, 143\}$

6) Encryption
$M = 13 \quad 13 < 143$ ✓

$C = 13^{13} \mod 143$

$13 \mod 13 = 13.$
$13^2 \mod 143 = 169 \mod 143 = 26.$
$13^4 \mod 143 = 26^2 \mod 143.$
$= 676 - (143 \times 4) = 104.$
$13^6 \mod 143 = 104^2 \mod 143$
$10816 - (143 \times 75) = 91.$

$C = (13^6 \mod 143 + (13^4 \mod 143) + (13 \mod 143)) \mod 143$

$= 91 + 104 + 26 \mod 143$
$221 \mod 143.$
$= 52.$