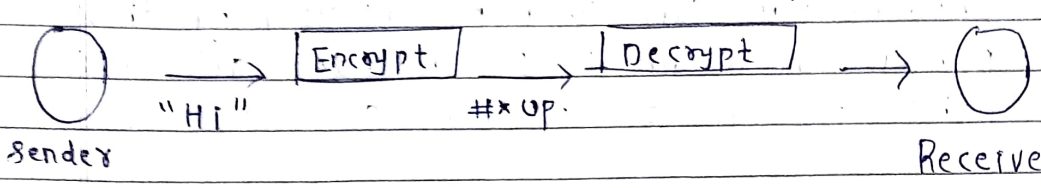
Cryptography

Cryptography



Cryptography : The act or art of writing in secret characters.

Cryptoanalysis : The analysis and de-ciphering of secret writings.

Cryptology : Scientific study of Cryptography and Cryptoanalysis.

- **Cryptography**
- It is a technique of securing information and communications through use of codes so that only those person for whom the information is intended can understand it and process it.

- Crypt = hidden
  graphy = writing

Applications

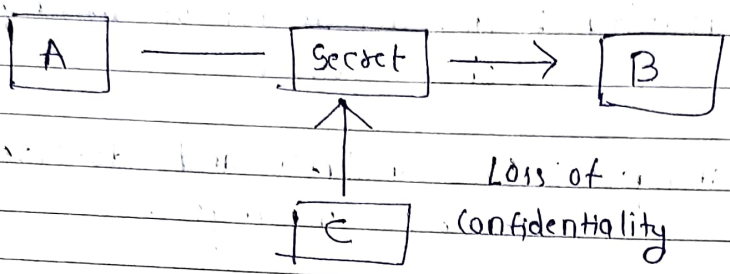
- Secure communication
- File and database security
- Electronic funds transfer
- Digital cash
- Electronic mail
- Electronic voting
- Secure web browsing
- Digital currencies
- Secure protocols

Page No.
Date

Security Services / Principles of Security / Features

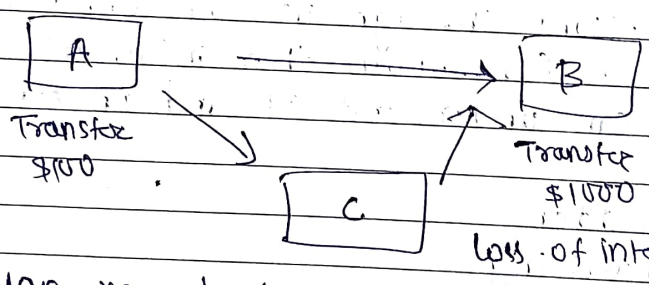
(1) Confidentiality :-

- Information can only be accessed by the person for whom it is intended and no other person except him can access it.
- Only intended receiver understands the message.



(2) Integrity :-

~~Info~~ Ensure that their communication has not been altered, either maliciously or by accident during transmission.

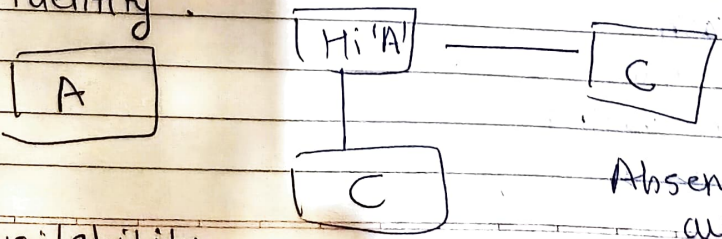


(3) Non-repudiation :-

Sender should not be able to falsely deny that a message was sent

(4) Authentication :

Sender & receiver need to confirm each others identity.

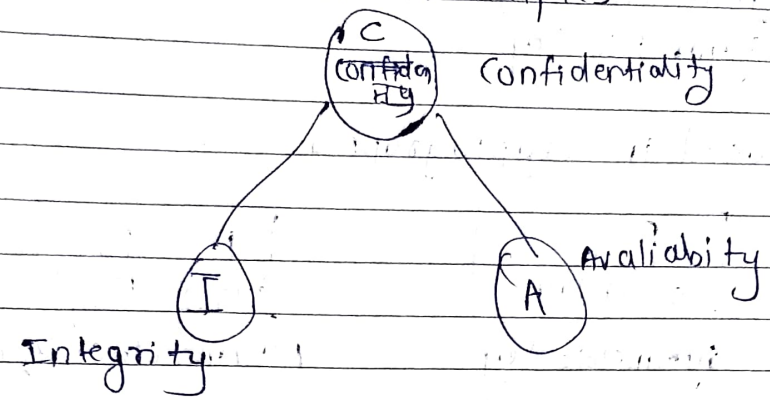


(5) Availability

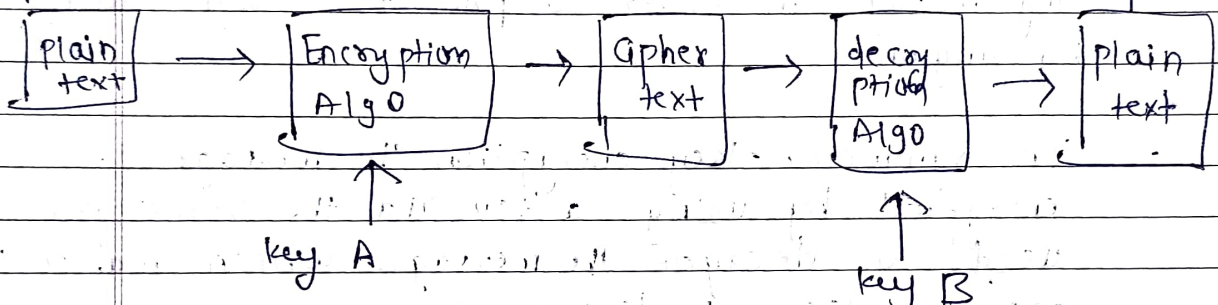
Page No.
Date

The CIA traid in Cryptography

Three fundamental Principles



Cryptography components



- Cipher is the method for encrypting messages.

The key which is an input to the Algo is secret.

- key is a string of numbers or characters

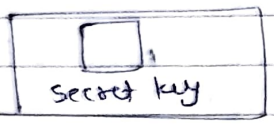
- If same key is used for encryption & decryption the algorithm is called symmetric

- If different keys are used for encryption & decryption the algorithm is called Asymmetric.

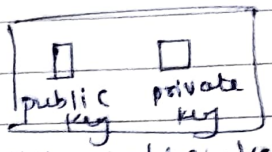
Categories of Cryptography

(1) Symmetric-key
(2) Asymmetric key

Key used in cryptography



Symmetric-key



Asymmetric-key

(1) Symmetric key

- Encryption is a process to change the form of any message, in order to protect it from reading by anyone.
- In Symmetric-key encryption the message is encrypted by using a key and the same key is used to decrypt the message, which makes it easy to use but less secure.
- It also requires a safe method to transfer the key from one party to another.

(2) Asymmetric key

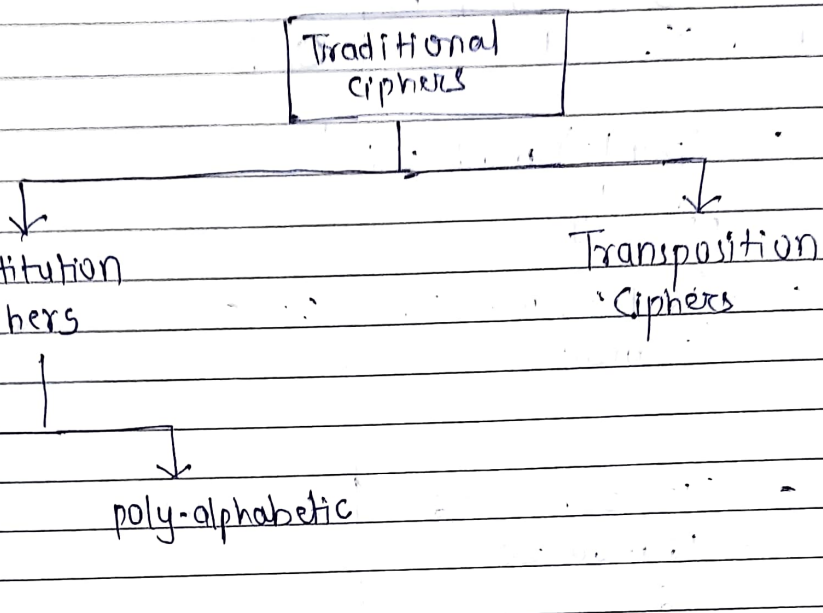
Asymmetric key Encryption is based on public and private key encryption techniques.

It uses two different key to encrypt and decrypt the message.

It is more secure than the Symmetric key encryption technique but is much slower.

Symmetric-key Cryptography

- Traditional ciphers
- Simple Modern ciphers
- Modern Round Ciphers
- Mode of Operation



- A substitution cipher replaces one symbol with another.

Caesar ciphers

- Letters are replaced by other letters or symbols.
- Casar cipher is a method in which each letter in the alphabet is rotated by three letters as shown.

Algo
For each plaintext letter 'p', substitute the cipher text letter 'c'

$$C = E(p, k) \bmod 26 = (p + k) \bmod 26$$
$$p = D(C, k) \bmod 26 = (C - k) \bmod 26$$

Page No.
Date

Caesar Cipher - Example

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
A	B	C	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s

t	u	v	w	x	y	z
19	20	21	22	23	24	25

k	u	N	A	L
N	X	q	D	O

$c = (p + k) \bmod 26$

p: plain, k: key

$c = (10 + 3) \bmod 26$
$= 13 \bmod 26$

$c = 20 + 3 \% 26$
$= 23 \% 26$
$= 23$

$c = (13 + 3) \bmod 26$
$= 16 \bmod 26$
$= 16$

$c = (0 + 3) \% 26$
$= 3$

$11 + 3 \bmod 26$
$= 14 \% 26$
$= 14$

plain text = kaunel
cipher text = NXqDO

Page No.
Date

Monoalphabetic cipher

- The "cipher" line can be any permutation of the 26 alphabetic characters.
- There are 26! pairing of letters
- Statistical Analysis would make it feasible to crack the key.

Polyalphabetic cipher (Vigenère cipher)

- Improve on the simple monoalphabetic technique
- 26 caesar ciphers with shifts 0 through 25

Encry. process

$$C_i = (P_i + K_{i \bmod m}) \bmod 26$$

Decry

$$P_i = (C_i - K_{i \bmod m}) \bmod 26$$

- Use table & key word to encipher a message
  - repeat keyword over text e.g FACE

```
F A C E F A C E F A C E F
M Y C A T H A S F L E A S
```

Using a key to shift alphabet

- obtain a key for this algo and then shift the alphabets.

(2) Transposition Cipher

Columnar Transposition

- This involves rearragment of characters on the plain text into columns

plain text Cipher text

Ciphers :- Shannon's characteristics of "Good" ciphers

(1) The amount of secrecy needed should determine the amount of labor appropriate for the encryption & decryption

(2) The set of keys and enciphering algorithm should be free from complexity.

(3) The implementation of the process should be as simple as possible

(4) Errors in ciphering should not propagate and cause corruption of further information in the message.

(5) The size of the enciphered text should be no larger than the text of the original message.

Encryption Systems :- properities of Trustworthy Systems

- It is based on sound Maths.
- It has been analyzed by compentent experts & found to be sound.
- It has stood the "test of time"

Page No.
Date

Cryptanalysis

Techniques

- Cryptanalysis is the process of breaking an encryption code.
- Several techniques can be used to reduce the algorithm :-

(1) Attempt to recognize patterns in encrypted messages, to be able to break subsequent ones by applying a straightforward decryption algo.

(2) Attempt to reduce the key, in order to break subsequent messages easily.

(3) Attempt to find weakness in the implementation or env. of use of encryption.

(4) Attempt to find general weaknesses in an encryption algorithm, without necessarily having intercepted any messages

Basic Terminology

(1) plain text - The original message

(2) Ciphertext - the coded message.

(3) Cipher - algo. for transforming plaintext to Cipher text

(4) key : info used in cipher known only to Sender/receiver

(5) encipher (encrypt)
converting plaintext to ciphertext

(6) decipher (decrypt)
converting ciphertext to plaintext

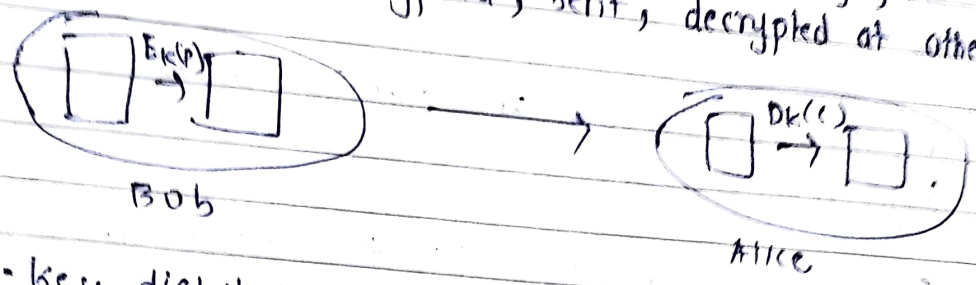
(7) Cryptography
study of encryption principles / methods

(8) Cryptoanalysis :
The study of principles / methods of deciphering ciphertext without knowing key.

(9) Cryptology
both Cryptography & Cryptoanalysis.

Symmetric Cryptography

- Both parties must agree on a secret key, K
- message is encrypted, sent, decrypted at other side



- key distribution must be secret
  - Otherwise messages can be decrypted
  - users can be impersonate

Key distribution

Sending this key directly makes it easy for hackers to capture it in transit

⇒ This is where the Diffie Hellman key exchange algorithm can help us in securely exchanging keys,

What is DHKE

- Algo to securely exchange keys
- usp communicated over "insecure" channels

How do one-way function work?

Page No.
Date

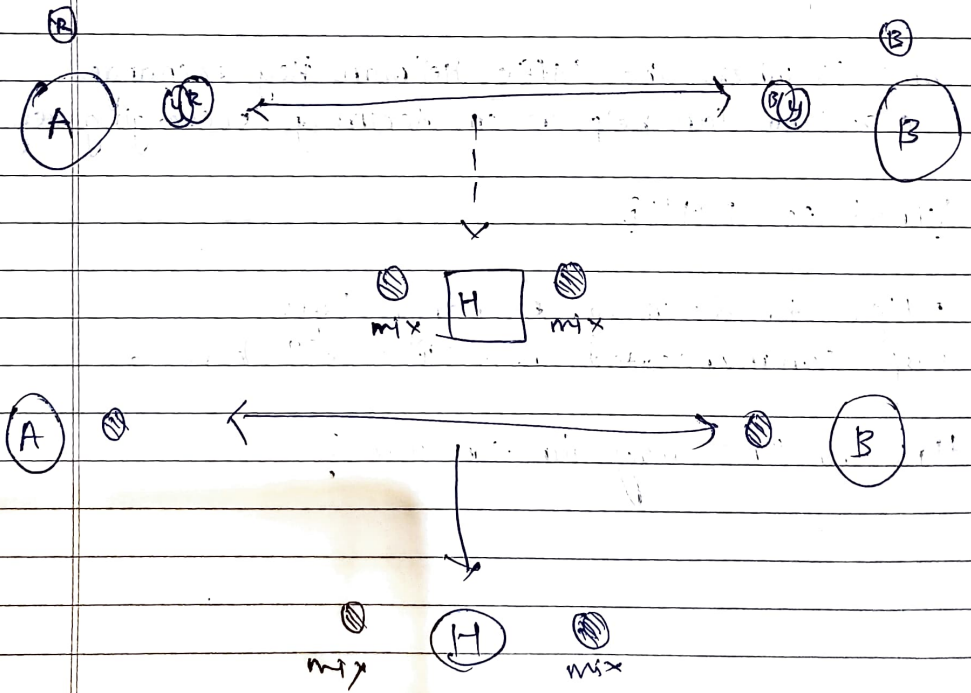
- Both users must have their private colors set, and must decide on a common public color to be used.

- The private colors and public colors are mixed together

- The color mixture is the sent among the users.

- The private colors are now combined with the mixture to find actual secret color.

- Both will get single color



Steps in key Exchange

(1) Choose q & α

a. choose a prime number q
b. Select α as a primitive root of q

To be primitive root,

$\alpha \bmod q$
$\alpha^2 \bmod q$
$\alpha^3 \bmod q$
⋮
$\alpha^{q-1} \bmod q$

$< q$
$(1, 2, 3, \ldots, q-1)$

(2) Deriving the key Pair

Assume private key $= X_a$ where $X_a < q$	Assume private key $= X_b$ where $X_b < q$
public key (Y_a) becomes:	public key (Y_b) becomes:
$Y_a \alpha^{X_a} \bmod q$	$Y_b = \alpha^{X_b} \bmod q$
key pair: $\{X_a, Y_a\}$	key pair: $\{X_b, Y_b\}$

(3) Key Generation

para X_a, Y_b, q	para: X_b, Y_a, q
Secret key	key
$K = (Y_b)^{X_a} \bmod q$	$K = (Y_a)^{X_b} \bmod q$

Page No.
Date

$q = 17$
$\alpha = 3$

X_a
$X_a = 15$

(Y_a)

$Y_a = 3^{15} \bmod 17 = 6$

key pair (15, 6)

$X_b = 13$

(Y_b)
$(Y_b) = 3^{13} \bmod 17 = 12$

key pair (13, 12)

para : X_a, Y_b, q

$k = 12^{15} \bmod 17 = 10$ ← | → $k = 6^{13} \bmod 17 = 10$

Appln

- Public key Infrastructure
- SSL / TSL Handshake
- SSH (Secure Shell Access)