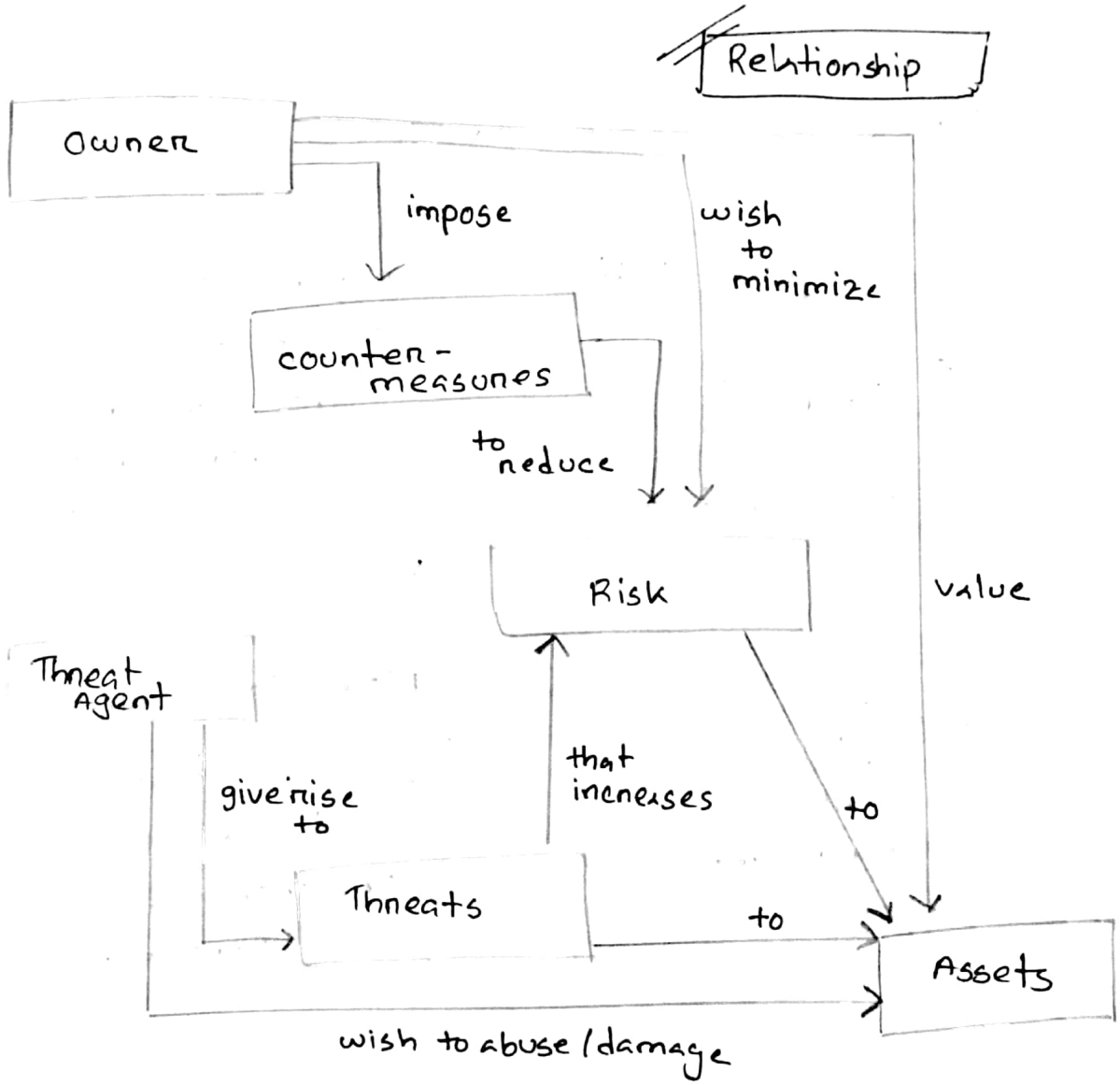
## What is common criteria (CC)?

→ CC is a set of guidelines that provides a framework for evaluting and certifying the security features and capabilities of IT product and service.



Q. with respect to the C.I.A and A.A.A concept what risks are posed by Trojan (TH) Horse?

Final-17

① confidentiality:-

TH allows unauthorize access to sensitive info. disquised as legitimate software. can steal or copy confidential data without user knowledge

Intregity:- data and system are compromised due to TH. modify, delete data, alter system configuration

Availability : impact the availability of system/networks by consuming system resource or disrupting network operation

make system unavailable to user.

## what is security?

→ ~~refers to within~~ systems, application, protocols relies on specific properties intend to prevent unauthorized access, alteration, destruction, disruption.

## what are the security goals?

1. Confidentiality → refers to keeping info. secret from all but those who are authorised can access it

CSE

**what is confidentiality**

2. Intregity

**what is Intregity**

CSE Final

refers to ensuring information hasnot been altered by unauthorized or unknown means

3. Availability

Data/ information is available when needed

**what is availability**

# Confidentiality

Two dimmension

**what is Secrecy?**

Secrecy is about keeping sensitive information hidden from people who shouldn't have access to it

(protection from unauthorize)

**what is privacy?**

privacy is about having control over your personal information and deciding who gets to know what about you

(protecting personal info)

**what are Tools of confidentiality?**

CSE final

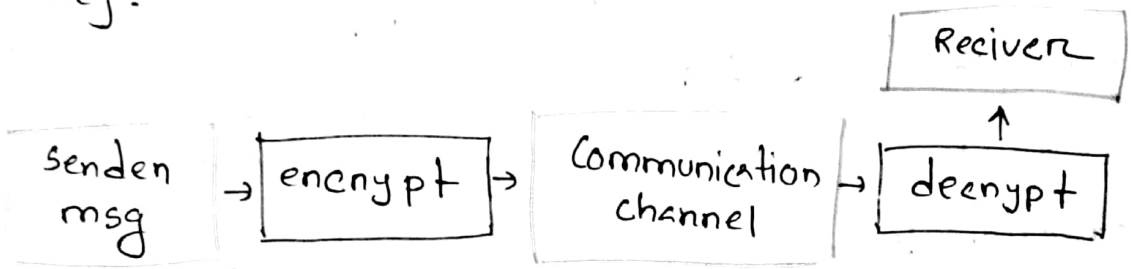
what are the steps to make data confidential?

5 tools

1. Encryption
2. Access control → limiting access using Rules and policies
3. Authentication
4. Authorization
5. physical security

## what is encryption?

→ is the process of transformation of information using a secret key called encryption key and the transformed information can only be read using another secret called decryption key.




umarks CSE-Final

— , —

## Authentication vs Authorization

| | |
|---|---|
| ① who are you? | ① what are you allowed to do? |
| ② is the process of verifying the identity of a user or entity. | ② is the process of determing what actions or resource a user is allowed to access or perform after they have been authenticated. |

# Intregity

two dimmension

## what is data Intregity?

→ means keeping info. and program. safe from any changes unless theyre allowed and approved

## what is System Intregity?

→ is like making sure a computer/system does its job properly without any unwanted interference

## what are tools of Intregity?

1. Backups
2. checksums →
3. Data connecting codes

### what is checksum?

a checksum is a simple way to check if a file has been changed or corrupted.

<a checksum function depends on the entire content, a small change to the file will result in a different output value>

## What are the security properties? 6 prop-

1. Confidentiality
   - Encryption
   - Access controll
   - Authentication
   - Authorization
   - physical security

2. Integrity
   - Backups
   - checksum
   - Data connecting codes

3. Availability
   - physical protection
   - compotional Redundanices

4. Authenticity → The property of an entity or source of data being genuine and being able to verified & trusted

5. Accountability

6. Anonymity → :- refers to the condition where certain records/actions /transection cannot be directly linked to any specific Individual.

(*) Difference between passive and active security attack?

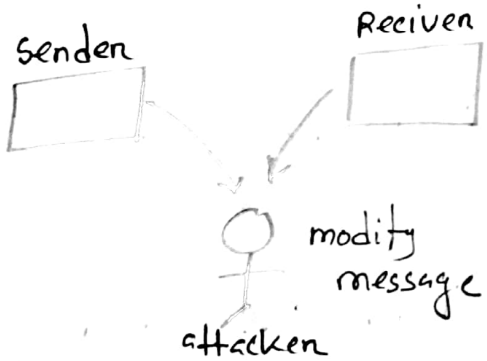
| Active attack | passive attack |
| --- | --- |
| (1) Active attack is dangen to Intregity & Availability | (1) dangerl to confidentiality |
| (2) modification information takeplace | (2) No modification |
| (3) attention is on prevention | (3) is on detection |
| (4) due to this attack, execution is always damaged system | (4) no hanm to system |
| (5) system resounces also canbechanged | (5) no change in system resounce |
| (6) can easily detected | (7) very difficult to detect |
| (7) punspose is to hanm the ecosystem | (7) punpose is to learn about the ecosystem |

(8) duration :- short

(9) Complexity :- High

(10) def :- what is active attack?

Active attack is an attack where the attackers attempts to modify /alter the content of message on the system itself




(11) Type

(1) Dos

(2) Modification

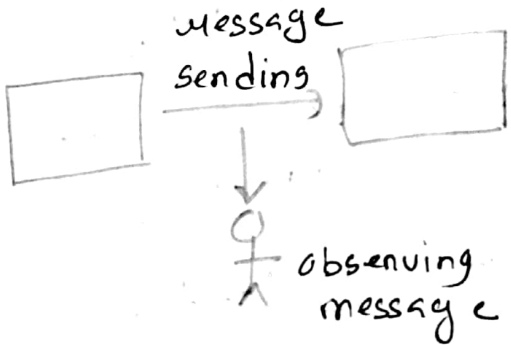
(3) Masquerade

(8) duration :- long

(9) complexity :- low

(10) def :- what is passive attack?

passive attack is an attack that involve the attacker observing /monitoring the system without making any changes to it




(11) Type :-

(1) ~~eye~~ Eaves dropping

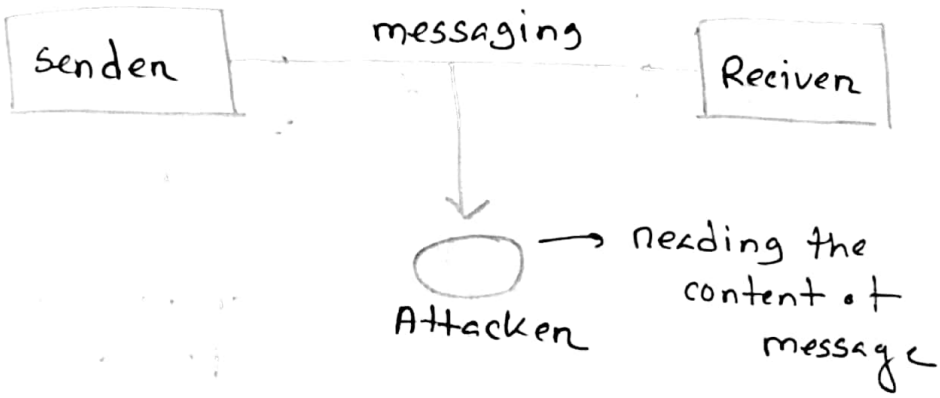
(2) Traffice analysis

(3) Replay

## (*) what is Eaves dropping Attack?

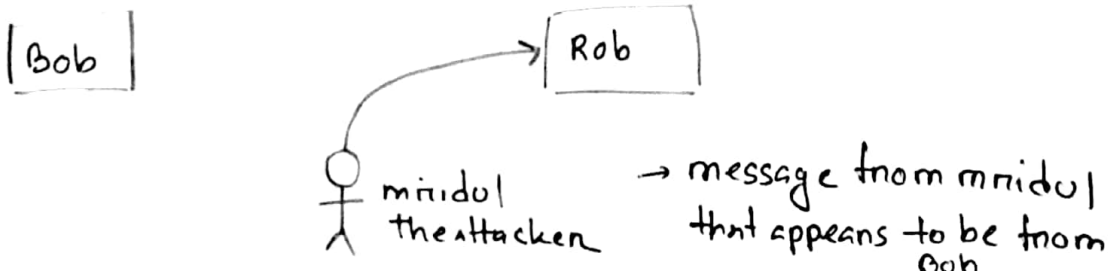
CSE final

→ It is passive attack where attackers intercepts and reads data that is transmitted between two device without the knowledge or consent of the parties involved.



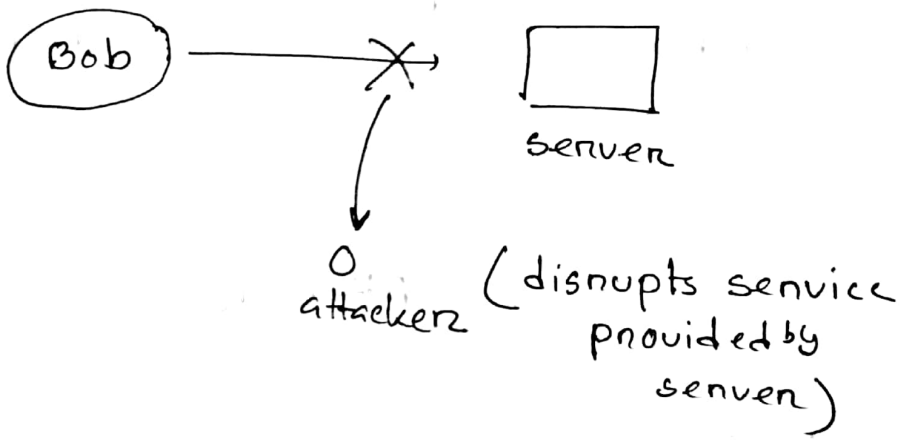

## (*) what is masquerading Attack?

→ it is a type of active attack where attackers pretends to be someone else (a legitimate user/system) to gain unauthorized access to system / data.



## what is Dos attack?

→ Denial of service is a type of active attack where attackers aim to render a computer/device unavailable to its intended users by intrepting the device's normal functionality.



# chapter-4

## Encryption :- dissoused previous

plaintext (M) $\xrightarrow[\text{Encryption (E)}]{}$ ciphen text (C)

decryption (D)

① $C = E(M)$ ← senden sends msg and encrypted)

② $M = D(C)$ ← decrypted and recived y.

## what is cryptosystem? swf final

a cryptosystem is consistof seven component

1. a set of plain text
2. ciphen texts
3. encryption keys
4. decryption keys
5. conespondence between encryption & decryption keys
6. Encryption Algo
7. decryption Algo

## what is caesar cipher?

→ is a simple and ancient method of encryption that involves shifting the letters of the alphabets by a fixed number of positions.

letter ← $S(c, k)$ → key

**if $k > 0$** encryption key
forward passing

$S(A, 3) = D$ $(A+3 = D)$

encryption key

$S(B, 3) = E$ $(B+3 = E$

AB ⟶ DE (after encryption)

**if $k < 0$** decryption key
Backward passing

$S(D, -3) = A$ $(D-3 = A)$

decryption key

$S(E, -3) = B$ $(E-3 = B)$

DE ⟶ AB (after decryption)

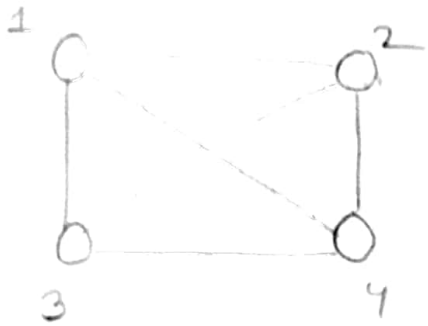
symmetric key crypto

**what is symmetric key distribution?**

→ fast and efficient

→ Too many keys

→ Sender – Reciver has same shared encryption-decryption key




if n parties

$$\text{keys} = \frac{n(n-1)}{2}$$

$$= 4(4-1)/2$$

$$= 6 \text{ keys}$$

asymmetric key crypto

**what is public key cryptography?**

→ provides best security

→ slower

keysize is larger

if n parties, key = 2n

To send to B: A needs public key of B to encrypt the message ($P_B$)

A ——→ B

send encrypted msg using $P_B$

$$C = E_{P_B}(M)$$

B need two keys

$P_B$, $S_B$

To decrypt the msg. B will use own private key. ($S_B$)

B ——→ B

decrypt msg using $S_B$

$$M = D_{S_B}(C)$$

ensure message are authentic and unchanged during transmission

## what is digital signature?

→ To ensure that the text has come from specific sender.

- Reliable,
- secure,
- easy validation

$$m' = E_{P_B}(D_{S_B}(m))$$

∴ if $m = m'$ ; signature is valid

Here, A sign's contract using private key

B verify contract using A's public key

CSE Final

## what is Man In the middle (MITM) attack?

→ It occurs when an unauthorized third party intermupts communication between two parties.

- view, change
- add, delete
- traffic

$\boxed{m \neq m'}$ not match

BOB send = (m, s) : (e, s)

← 3rd party change the msg = (e', s')

Just change can't decrypt

Alice think it is from BOB = (e', s') : (m', s')

(*) what are the two attacks in crypto system?

(1) Man in the middle

(2) Brute force

what is brutefoce attack?

SWP final

Describe How brutefoce attack?

refers to trying different probable/possible keys over a ciphertext to decrypt into a meaningful text.

what is unicity distance?

esf

Find unicity distance of cipher where the number of keys = 25 and the language is english

it is a point at which the cyphertext is long enough for an attacker to successfull decrypt it, recover the original message without knowing the key.

$$\text{Unicity distance}, n = \frac{k}{1-\alpha}$$

$k \rightarrow$ key Length

$\alpha \rightarrow$ constant

$$= \frac{25}{1-1.25}$$

(*)

In English text,

1 character = 8 bit

a msg with t charachten has

$n = 8t$ bit $\quad t = \frac{n}{8}$

$\therefore$ Total No. of possible array $= 2^n = \boxed{2^{8t}}$

we know,

1 character $\longrightarrow$ 1.25 bit info

t " $\longrightarrow$ 1.25t " "

$\therefore$ no of t byte array $= \boxed{2^{1.25t}}$

$= 2^{1.25 \times n/8}$

$= 2^{0.16n}$

$\therefore$ valid text $= 2^{\alpha n}$

$$\boxed{\therefore \text{probability of getting valid text} = \frac{2^{\alpha n}}{2^n} = \frac{1}{2^{(1-\alpha)n}}}$$

$$\boxed{\text{Probability of getting plain text} = \frac{2^k}{2^{(1-\alpha)n}}}$$

$k$ = length of decryption key

$\alpha$ = constant

$n = 8t$

$t$ = no of character

Final 17

Q. Suppose we are using ASCII encoding. Now each english alaphabet is estimated to carry $\underset{\alpha}{\underline{1.25 \text{ bits}}}$. calculate the probability that a randomly selected sequence of $\underset{n}{\underline{32 \text{ bits}}}$ is a meaningful text msg.

$$\text{probability valid test} = \frac{1}{2^{(1-\alpha)n}} = \frac{1}{2^{(1-1.25)32}}$$

$$= 256$$

$$\therefore \text{probability among all} = \frac{256}{2^{32}} = 5.96 \times 10^{-8}$$

Final

(*) The english language has an info of about 1.25 per character. Thus when using the standard 8 bit ascii encoding about 6.75 bits character are redundant. compute the probability that a random array of t bytes corresponding to English text.

$$\text{probability} = \frac{\text{total valid msg}}{\text{no of total } t \text{ byte msg}}$$

$$= \frac{2^{1.25t}}{2^{8t}}$$

$$= \frac{1}{2^{6.75t}}$$

$$= 2^{-6.75t}$$

The probability that a random array of t bytes corresponds to english text $= 2^{-6.75t}$

SWE final

Brute force decryption is likely succed for message in natural language that are not too short

— True

what is non-repudiation? (Accountability) SWE

→ principle states that ensuring a user cannot deny having performed a specific action ; provides a way to prove that a user indeed performed an action (sending message) and protects them falsely accusing of having performed that action

what is security by obscurity? CSE final

Security through obscurity is a principle states that relies on secrecy of system design and implementation (hiding) information for preventing unauthorize access?

# chapter-3

**

## what are the 10 security principle?

1. Economy of mechanism
2. Fail-safe defaults
3. complete mediation
4. open design
5. SEparation of privilege
6. Least privilege → CSE Final advocates granting user/system only the minimum level access on permission to perform their task
7. Least common mechanism
8. Psychological acceptability
9. compromise Recording
10. work factor

## what is economy of mechanism?

→ keeping design and implementation of security measures simple.

## what is Fail-safe defaults?

CSE Final

→ priciple states that the default configuration of a system should have a conservative protection schema.

(access to an object/resource in starting should be denied by default unless explictly granted

Example :- consumer grade router violates the principle. Default well know password/ easy to guess

Final - 17

## what is complete mediation? with example

the principle states that every permission access to a resource must be checked when requested on compliance for an authority.

Example :- electronic door access control

bkash payment need pin everytime → to prevent unauthorized

17 Final

Q describe a process through which a system can fullfill the complete medition security principle?

① when an open access to object they send a nequest to the system

② check authonization

③ Verify penmission

④ nepeat for every attempt

CSF final

what is kenckhoff's principle?

⇒ " a cryptosystem should be secure even if everything about the system except the key is public knowledge "

CBE final what is open design principle?

security design + anchitecture → public

cyptonaginaphic key → private

## what is separation of privilege?

→ principle states that multiple condition should be fullfilled to achive access to restricted resource
(double/2way verification)

## what is least common mechanism?

→ priciple states that when system has multiple user allowing resources to be shared by more than one user should be minimised.

## what is work factor?

→ principle states the cost of breaking a security mechanism should be compared with the resource of an attacker when designing a security schemal

a university database vs military grade secrets
(student) attackers (pro attackers)

## what is compromising Recording?

→ suggest rather focusing on preventing intrusions. it also important to detect and record them for analysis & investigation purpose.

---

## what are the 4 mechanism of access control?

1. Access control Matrices
2. Access control list
3. capabilities
4. Role-based Access Control (RBAC)

ACM

# Access Controll Matrices

vs

difference between Access control Matrice vs Access control list

refers to a table that sets Rules for who can do what with certain things.

(a table that defines permissions)

→ file/folder/etc we want to define access

| | /etc/pass | /usr/bin |
|---|---|---|
| root | read, write | read, write, execution |
| mike | read | read, execution |

↓ user, group system

→ access rights

↓ empty cell means no access

**Pros:-**

→ easy format

→ easily see a cell and tell which user can do what with a file

**cons**

- huge size
- complex
- hard to manage
- time consuming

# ACL — Access control list

Each object/file has a list of users who can access it and their rights.

| /etc/password |
| --- |
| root: r, w, x<br>mike: r |

| /usr/bin |
| --- |
| root: r, w, x<br>mike :- r, x |

**Props**

→ small size than ACM

→ change/remove entry easily

**cons**

→ poor efficiency

→ Finding out all access right for a user is too slow

# Capabilities

For each user, it seperatly lists the objects/file with what the can access and what they can do with each object.

| | | |
|---|---|---|
| root | → | /etc/pass :- r,w,x<br>/usr/bin :- r,w,x |
| mike | → | /etc/pass :- r<br>/usr/bin : r,w |

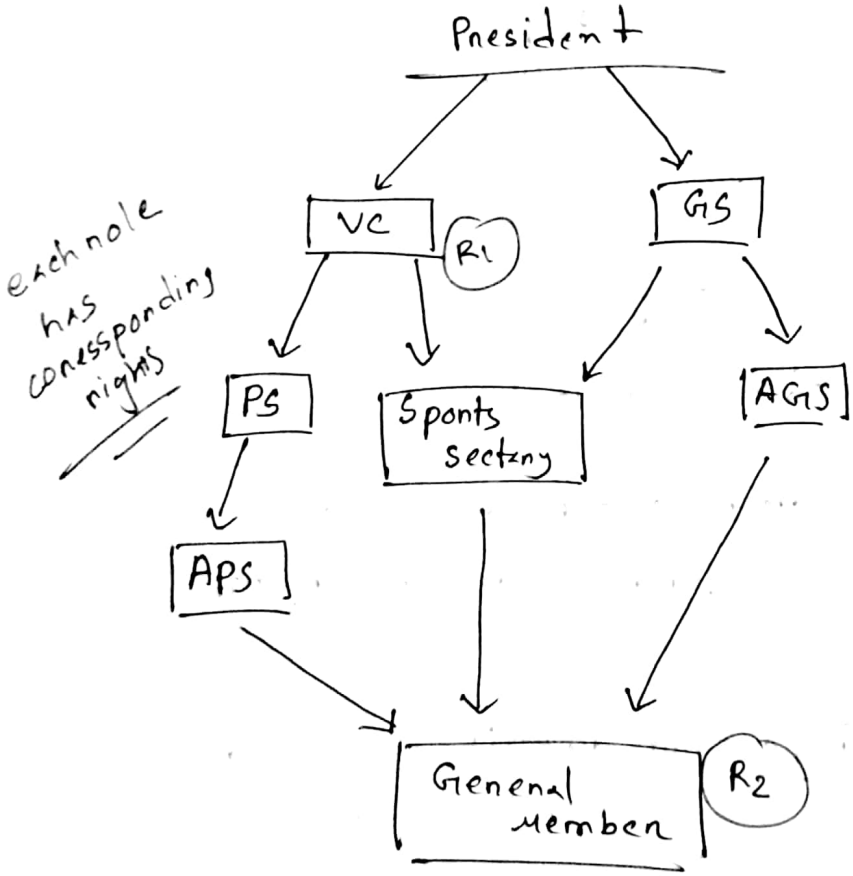
pros :-
- → easy to find
- → reduce workload
- → admins only needs to access for pain with actual rights.

Cons :- They are not directly associated with objects

# RBAC

## Role based Action control

→ define roles and then specify access control rights for those roles rather than for subjects directly.



if roles $R_1$ is above $R_2$ in the hierarchy,
then $R_1$ inherits the access rights of $R_2$

AAA CSE Final SWE Final TI

(*) what is digital signature? and its step?

digital signature is a cryptographic technique used to validate the authenticity and integrity of a digital message, document.

$$m' = E_{P_A}(D_{S_A}(m))$$

if $m' = m$ ; valid signature

(1) A attach signature with message encryption with its private key

(2) B decrypt and verify contract using A' public key.

- message digest
- private key encryption
- attach signature
- verification

Briefly explain A.A.A concepts in modern computer security

CSE Final

A A A → Accounting (tracking and recording user activites)

↓ Authentication

↘ Authorization

CSE Final

(3) Suppose bob want to send message $m = 13$ to Alice

Both Alice public and private key are (33.3) and (33.7). Now calculate the cipher text C and decrypt it to retrive the message, m

$m = 13$

private $= (33.3)$

$\therefore$ cipher Text, $c = (m^e \bmod n)$

$= (13^3 \bmod 33 = 19$

To decrypt

$m = (13^7 \bmod 33) = 19$

Que

A computer can test a password in every nanosecond. How much time it will take for an attacker to crack the password length of 8 (password may consist any 128 ascii)

ans:-

length = 8

character = 128

time $= 10^9 s$

possible combination $= 128^8$

Total time needed

$= 128^8 / 10^9 \ s$

$= 72.05 \times 10^6 \ s$

suppose we have a network of 2300 users.

## Symentric key cryptosystem

$$\text{Keys} = \frac{n(n-1)}{2} = \frac{2300(2300-1)}{2}$$

$$= 2643850$$

## Asymentic

$$\text{keys} = 2n = 4600$$

Find the unicity distance of casear cipher where the number of keys=25 and the language is english

unifon distance

$$U() = \frac{H(k)}{D}$$

$$\therefore H(k) = \log_2 2^k$$

$\therefore$ if key (25)

$$\therefore H(k) = \log_2 2^{25}$$

$$= 25$$

noof characten in english

$$\therefore D = \log_2(26) - 1.25$$

amout of info cunnied per characten in english

$$= 3.45$$

$$\therefore u = \frac{H(k)}{D}$$

$$= \frac{25}{3.45} = 7.24 \simeq 8$$

TTSWE

Q. suppose you are given the following text $\boxed{\text{dog}}$ and a random matrix K. Now find the cipher text using Hill cipher

$$K = \begin{bmatrix} 1 & 2 & 5 \\ 3 & 3 & 4 \\ 2 & 1 & 3 \end{bmatrix}$$

watch promi answer

① Turn the text into matrix dog

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

| x | y | z |
|---|---|---|
| 23 | 24 | 25 |

$$X = \begin{bmatrix} 3 & 14 & 6 \end{bmatrix}$$

key(K) . plaintext(X)

ciphen Text = $(\cancel{\text{Plaintext}(X)} \cdot \cancel{\text{key}(K)}) \bmod 26$

$$= \begin{bmatrix} 3 & 14 & 6 \end{bmatrix} \cdot \begin{bmatrix} 1 & 2 & 5 \\ 3 & 3 & 4 \\ 2 & 1 & 3 \end{bmatrix} \bmod 26$$

wonnt careful!

$c_{11} = (3\times1) + (14\times3) + (6\times2) = 57 \bmod 26$
$= 5$

$c_{12} = (3\times2) + (14\times3) + 6\times1 = 54 \bmod 26$
$= 2$

$c_{13} = (3\times5) + (14\times4) + (6\times3) = 89 \bmod 26$
$= 11$

ciphen text $= [\ 5 \quad 2 \quad 11\ ]$

$= fcL$

$\boxed{dog \rightarrow fcL}$

— · —

## what is hill ciphen?

→ Hill ciphen is a polygnaphic substitution ciphen that is based on concept of linean algebna.

→ polygnaphic subsititution is a ciphen where uniform subsitution is penfonmed on letten blocks

$\boxed{\vec{C} = K \cdot \vec{X}}$ → ciphen encnyption

$\boxed{\vec{X} = K^{-1} \cdot \vec{C}}$ → decnyption

TTSWE

## ⊛ why ECB mode bad with images?

Electronic codebook mode (ECB) → fails to hide pattern and details

→ simple

$C_i = E_k(B_i)$ → encryption

$B_i = D_k(C_i)$ → Decryption

Reason :-

① Lack of Diffusion :- ecb mode encrypts each block of plaintext independently. so identical plaintext are encrypted into indentical cipher

② Pattern preservation :- since identical block to indentical cipher, this lead visible pattern in encrypt message Image which reveal the original Image.

Lack of Randomness :-

③ Easy to anaylze and predict the content in ecb mode

SWE - 18
Final

## (*) what is one time Pads (OTP)?

→ OTP is a type of encryption that is theoritically unbreakable whenused connectly.

It includes using a random key that is as long as the message being encrypted.

key is same lenght as message generated

SWE Final - 18

(*) Suppose the number of keys for substitution cipher 26! if we partion the plaintext into bignam. what will be the number of key in keyspace.

possible biagrams = $26^2$
= 676

No logic just memonize

The key sin bignam substitution cipher
= 676!

SWE-18

What is substitution cipher? write the main disadvantages of it?

→ A substitution cipher is a method of encryption where each letter in plaintext is replaced by another letter. The key substitution cipher is a fixed permutation of alphabet.

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

$$D_k(x) = (x-k) \bmod 26$$

$k$ = any random value

Disadvantage

① Frequency analysis can reveals patterns in substitution cipher based on most common letters and letter combinations that appears frequently

② Securely sharing keys between parties are challenging

③ modern cryptographic technique can easily bereaks it.

④ English lacks enough entropy and fixed alphabet size

⑤ Any person with enough time can just decode it because people can find meaning in the text.

---

Q SWE 18

suppose you are given the following text 'Tom' and a random matrix. Now find the ciphen text using Hill ciphen

$$K = \begin{bmatrix} 1 & 2 & 5 \\ 3 & 3 & 4 \\ 2 & 1 & 3 \end{bmatrix}$$

Q SWE final 16

what is block cipher? Explain ECB and CFB mode of block cipher!

→ a block cipher is symentric key cipher that encrypts data in fixed-size blocks rather than one bit at a time like a stream cipher

→ The block of plaintext in tranformed into a block of ciphertext of the same size using a cryptographic algorithm and key.

modes of operation in block cipher

1. ECB (Electronic Code book)
2. CBC (cipher block chaining)
3. CFB (cipher Feedback)
4. OFB (output Feedback)

## ECB

1. each plain text block is encrypted independently
2. Deterministic :- same block will always result same ciphenblock
3. multiple block encryption can done parallel
4. patterns can be visible in ciphentext

plain text :- DA BC CD DA

ciphen text :- SBC PQL LOP SBC

6. CFB is slower than ECB

— —

3 — no parallal

4 not visible

## CFB

1. encryption of each plain text segment depends on previous ciphent text segment
2. an error in one segment can affect whole decryption
5. No needs padding

(7)

$C_0$ = intialization vector

$C_i = E_K(C_{i-1}) \oplus B_i$ → encryption

$B_i = E_K(C_{i-1}) \oplus C_i$ → Decryption

16 Final

(*) **What are the problems of CFB block cipher?**

(1) a single bit error in cipher text affects corresponding bit in the decrypted plaintext

(2) Through ECB can work prallel, CFB requires sequential processing because encryption of current block depends on previous cipher block

(3) Improper Intialization vector can compromise security

(4) Due to sequential processing, overall Latency increases

SWE-16

(*) why padding used in encryption?

→ padding used in encryption to ensure that plaintext message is an appropriate length for encryption algorithm particularly in the case of block cipher.

As block cipher operates on fixed size data blocks. padding addresses this requirement by adding extra data to the plaintext to meet necessary length.

SWE 16

Q vigenere cipher uses a key that is as long as the plain text.

Is it true/false?

→ False

SWE-16

(*) In CBC mode we can take advantage of pre computed IV. True/false

False. CBC modes relies on unique and unpredictable IV for each encryption sessions.

SWE-16

(*) what is cryptanalysis?

→ It is the study and pratice of analyzing and breaking cryptographic system which includes various technique to decipher text without having access to key.

(16) (17) swe Final

(*) Between CFB and OFB which one is better?

Ans:- OFB has significant advantage over CFB when it come to error propagation

| CFB | OFB |
|---|---|
| $C_0$ = Intialization vector | $V_0$ = Intialization vector |
| $C_i = E_K(C_{i-1}) \oplus B_i$ | $C_i = V_i \oplus B_i$ |
| $B_i = E_K(C_{i-1}) \oplus C_i$ | $B_i = V_i \oplus C_i$ |
| | $V_i = E_K(V_{i-1})$ |

CFB uses previous ciphertext is the subkey XORed to the plaintext. OFB uses the subkey before it XORed to the plaintext. Since the subkey is not affected by the encryption, errors donot propagate.

(1) OFB is faster > CFB
cause keystream can be pre-computed

SWF 16.77 (1mr)

(a) Encrypt the text "BBC ABC BCA A" using block cipher with padding where $m = 3$ $K = \begin{bmatrix} 1 & 2 & 3 \\ 5 & 6 & 7 \\ 9 & 10 & 11 \end{bmatrix}$

For first block $\vec{x} = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}$ Last block $\vec{x} = \begin{bmatrix} 0 \\ 3 \\ 3 \end{bmatrix}$

Ans:-

Block 1 :- BBC $\rightarrow \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}$

Block 2 : ABC $\rightarrow \begin{bmatrix} 0 \\ 1 \\ 2 \end{bmatrix}$

Block 3 : BCA $\rightarrow \begin{bmatrix} 1 \\ 2 \\ 0 \end{bmatrix}$

Block 4 : A $\underbrace{22}_{\text{Given}}$ $\rightarrow \begin{bmatrix} 0 \\ 3 \\ 3 \end{bmatrix}$

$$\therefore c = (K \cdot \vec{x}) \bmod 26$$

B1 :- $\begin{bmatrix} 1 & 2 & 3 \\ 5 & 6 & 7 \\ 9 & 10 & 11 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 9 \\ 25 \\ 41 \end{bmatrix} \bmod 26 = \begin{matrix} J \\ Y \\ P \end{matrix}$

B2 :- " $\cdot \begin{bmatrix} 0 \\ 1 \\ 2 \end{bmatrix} = \begin{bmatrix} 8 \\ 20 \\ 32 \end{bmatrix} \bmod 26 = \begin{matrix} I \\ U \\ G \end{matrix}$

B3 :- " $\cdot \begin{bmatrix} 1 \\ 2 \\ 0 \end{bmatrix} = \begin{bmatrix} 5 \\ 17 \\ 29 \end{bmatrix} \bmod 26 = \begin{matrix} F \\ R \\ D \end{matrix}$

B4 :- " $\cdot \begin{bmatrix} 0 \\ 3 \\ 3 \end{bmatrix} = \begin{bmatrix} 15 \\ 39 \\ 63 \end{bmatrix} \bmod 26 = \begin{matrix} P \\ N \\ L \end{matrix}$

Encrypted Text :- JPY IUG FRD PNL

17 Final

(*) How to detect whether CBC can hide patterns or not? Describ Process

Steps:-

1. Encrypt a plaintext with repeating pattern using CBC mode with a symentric key and random intialization vector.

2. Break the resulting cipher in a block

3. compare the blocks for any repitions

If all cipher blocks are unique, CBC mode successfully hides the pattern. If any blocks are identical, CBC mode fails to hide the pattern.

## ⑤ Problem and Solution of Block cipher

→ leak information about lengths as well as some part of the message

use standard padding method

## ⊛ ECB and CFB mode problem in 3 line

**ECB**

1. leak pattern
2. reveal info in plain text
3. not suitable for sensitive data

**CFB**

1. more complex + slower
2. if error occurs in a block, it will affect next of block decryption
3. not suitable for large scale data

18 Final

(*) Calculate GCD (2260, 812) using eculidean Algo

(1) $a = 2260, \quad b = 812$

$\therefore \text{rem} = a \% b = 636$

(2) $\boxed{a = b}$ $\quad$ $\boxed{b = \text{rem}}$

$a = 812, \quad b = 636$

$\text{rem} = a \% b = 176$

(3) $a = 636$

$b = 176$

$\therefore \text{rem} = 108$

(4) $a = 176, \quad b = 108$

$\text{rem} = 68$

(5) $a = 108, \quad b = 68$

$\text{rem} = 40$

(6) $a = 68 \quad b = 40$

$\text{rem} = 28$

(7) $a = 40 \quad b = 28$

$\text{rem} = 12$

(8) $a = 28 \quad b = 12$

$\text{rem} = 4$

(9) $a = 12, \quad b = 4$

$\text{rem} = 0$ ans

GCD = 4

(4) $\boxed{5^{31} \bmod 13 \text{ using repeated squaring}}$

$31 = 16 + 8 + 4 + 2 + 1$

$5^{31} = (5^{16} \cdot 5^{8} \cdot 5^{4} \cdot 5^{2} \cdot 5^{1}) \bmod 13$

$= (12 \times 8 \times 12 \times 5) \bmod 13$

$= 7680 \bmod 13$

$= 8$

---

$5^1 = 5^1 \bmod 13 = 5$

$5^2 = 5^2 \bmod 13 = 12$

$5^4 = (5^2 \cdot 5^2) \bmod 13$

$= (12 \times 12) \bmod 13$

$= 8$

$5^{16} = (5^8 5^8) \bmod 13$

$= 8$

$5^8 = (5^4 \cdot 5^4) \bmod 13$

$= (8 \times 8) \bmod 13$

$= 12$

(*) what is MAC (Message Authentication code) and How can MAC ensure Data intregity?

Ans:- In ~~cnp~~ cryptography, MAC is a short piece of information that is used for Authenticating and intregating checks a message.

It ensures that message is sent from correct user/sender and has not been changed.

Step-1 :- Message creation

A message :- "Hello! Bro"

Step-2 :- MAC Generation

- A use a secret key shared with B
- a mac algorithm to generate a mac for the message

key = '128 Sp'

∴ Algorithm = HMAC - SHA256

∴ now the mac = "ABC26"

③ message transmission

A sends (message + MAC) → B

④ MAC verification

- Bob receve message + MAC
- now generate a mac using the same key + algo
- if ( recived mac == B' generated mac)

msg is from A

else ~~msg~~ msg has been changed

^

* what is common criteria? draw a diagram to explain Relationship (6)

* what is security and what are the goals of security? (3)

* what is confidentiality? what are tools of confidentiality and types of it? (2) (5)

* what is secrecy? (2)

* what is privacy? (2)

* with the respect of CIA and AAA concept, what risk are posed by Trojan Horse? (3)

* what is encryption? Draw a diagram and write the encryption formula! (2)

* what is intregity? Types of Intregity and what are the tools of it? (3) (2)

* what is checksum? How works?

* Difference between Authentication and Authorization? (2)

* what data and system intregity?

* what are the security properties explain? (1)
* Difference between Active and passive attack? (12)
* what is eaves-dropping attack? draw diagram
* what is masquerading attack? draw diagram
* what is dos attack? draw diagram

— · —

* what is cryptosystem? (7)
* what is caesar cipher? explain with formula's and example (2)
* what is symentric key distribution?
* Explain public key cryptography with formula and example? (2)
* what is digital signatures? explain with example and formula
* what is man in the middle attack? explain with example

(*) what is brutefonce attack?

(*) what is unicity distance?

(*) check all fonmula and 17 question?

— . —

(*) what are the 10 security principle?

(*) what is economoy of mechanism?

(*) what is Fail-safe defaults with example?

(*) what is complete mediation? with example

(*) Describe a process through which a system can fullfill the complete medition security principle?

(*) what is kerckhoff's principle?

(*) what is separation of privilege? example

(*) what is workfactor? example

(*) what is least common mechanism?

* what is compromise recording ?

* what are the mechanism of access control ?