19-03-24 Information Security

→ Infor. Security services:

1. Confidentiality (to valid user)
2. Data Integrity (data secure)
3. Authentication (from valid source)

→ Types of authentications:

1. Msg Encryption
2. Msg authentication code (MAC)

C(M,K) = mac code
{fixed size}

3. Hash function

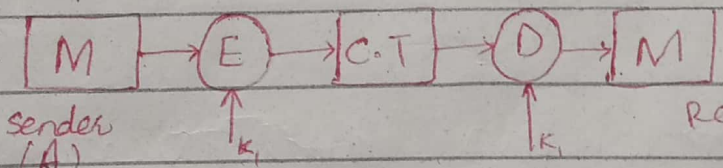
h = H(M)

H(x) ≠ H(y) unless x = y

Through Encryption:

achieve confidentiality

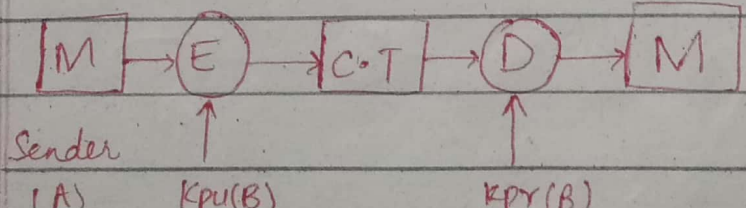
1.



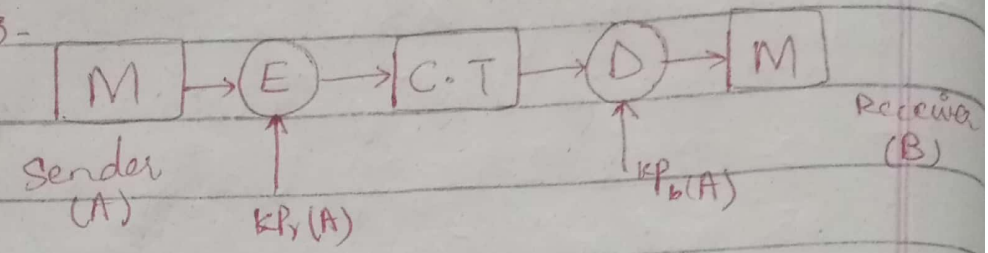
2. Asymmetric:

→ achieve confidentiality

→ not achieve authentication



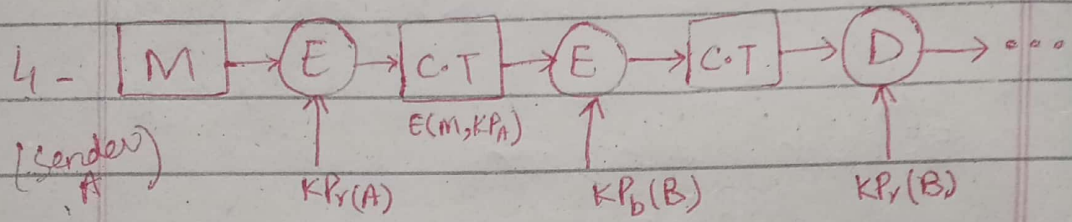
3-

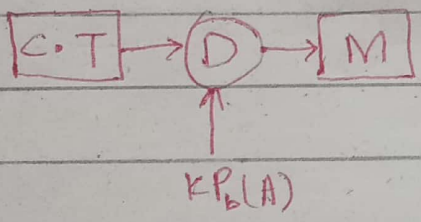


→ No Confidentiality

→ Achieve Authentication

4-





(Receiver B)

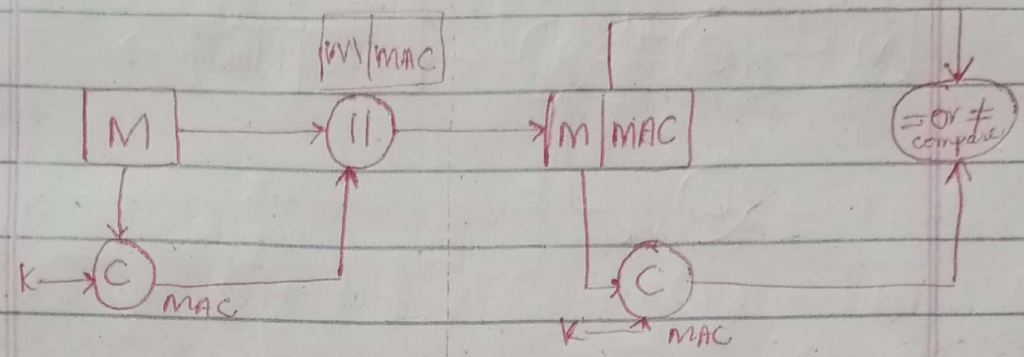
→ Achieve authentication and confidentiality.

20-03-24 IS

Message Authentication Code (MAC)

$MAC_K = C(K, M)$

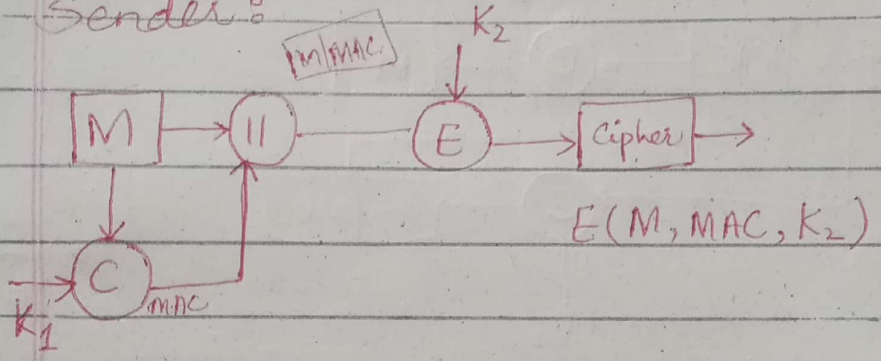
* Authentic if (=)
* Not Confident



Sender Receiver

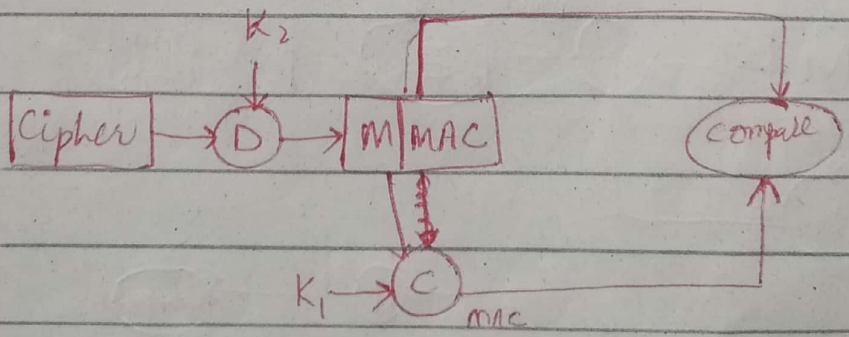
→ Authentication tied to plaintext

(2) Sender:



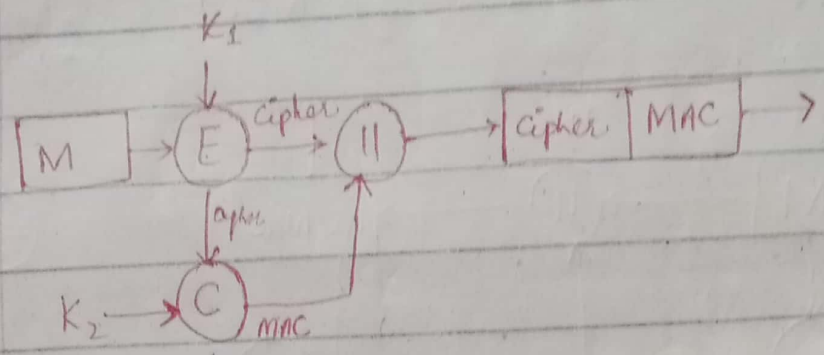
$E(M, MAC, K_2)$

Receiver:

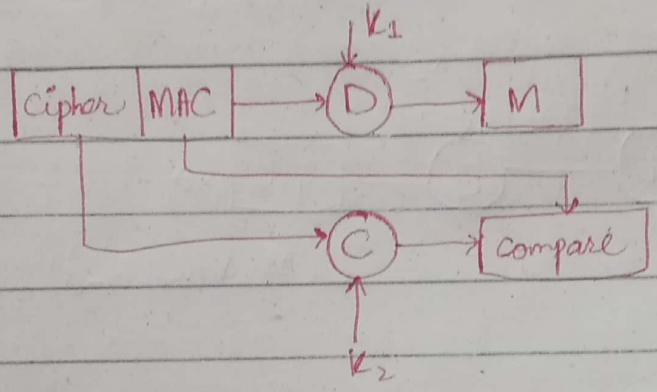


Authentication tied to plain text

(3) Sender:



Receiver:

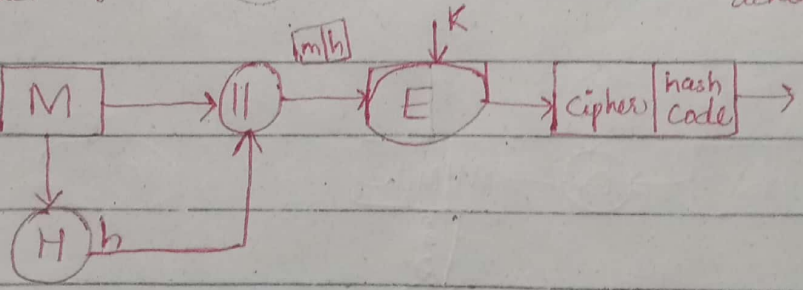


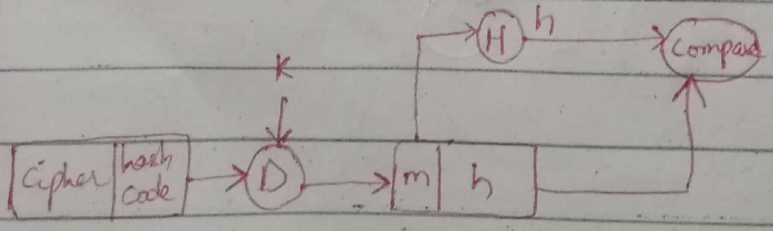
Hash Function:-

hash value / message digest ← h = H(M)

Both are achieve

(1)

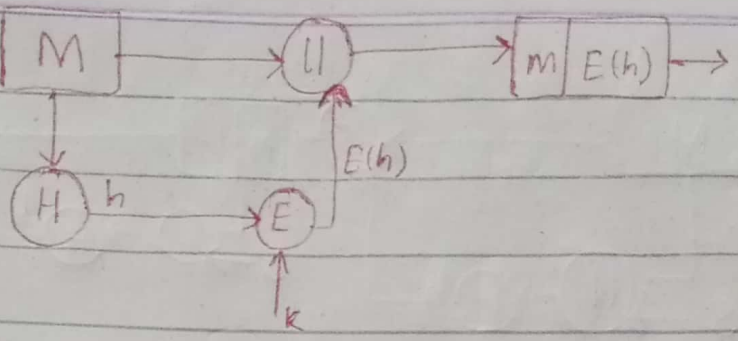




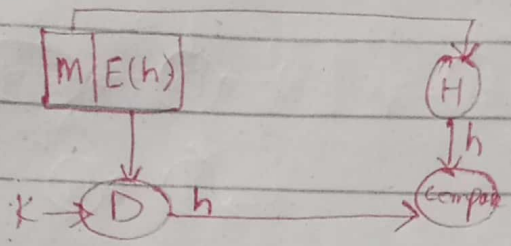
→ Authentication
→ No Confidentiality

Sender :

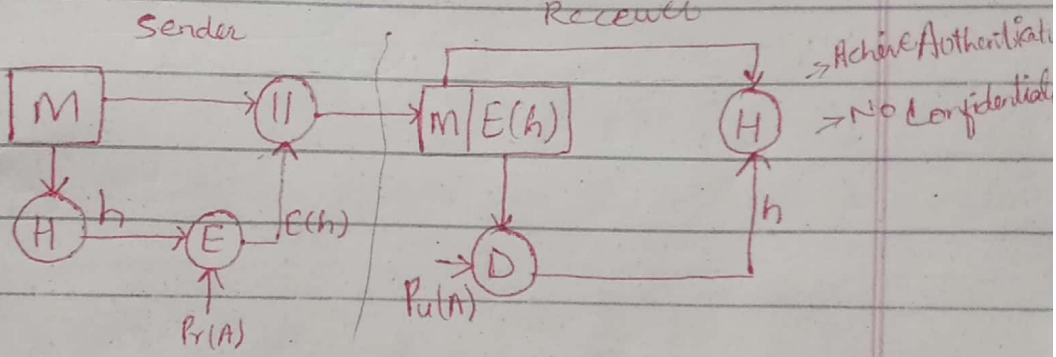
(2)



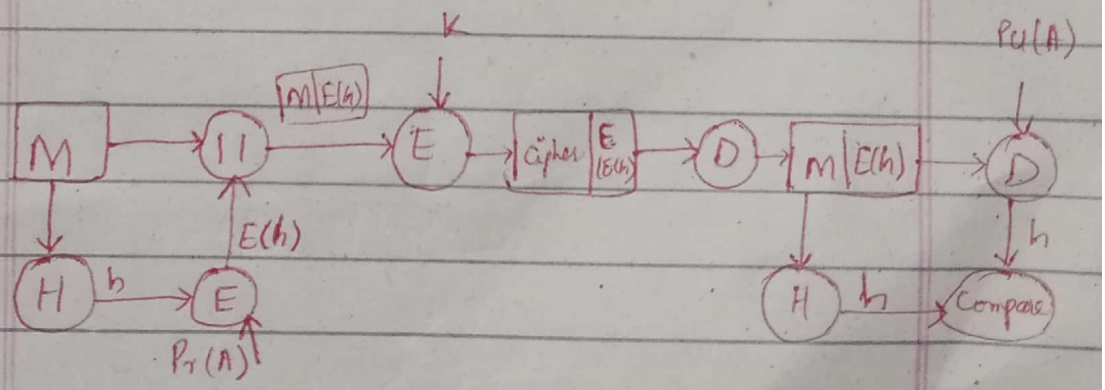
Receiver :



(3)



(4)



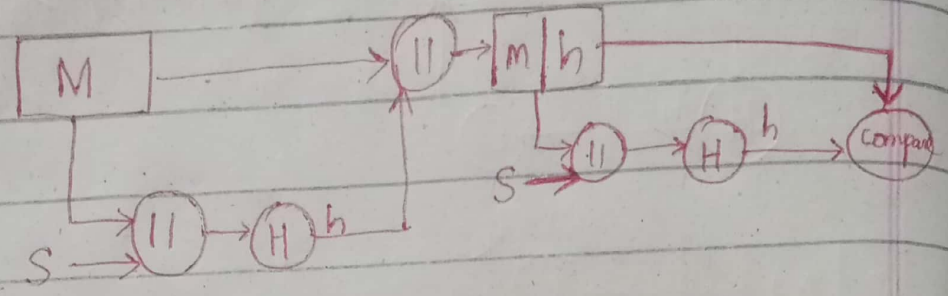
Sender A

Receiver B

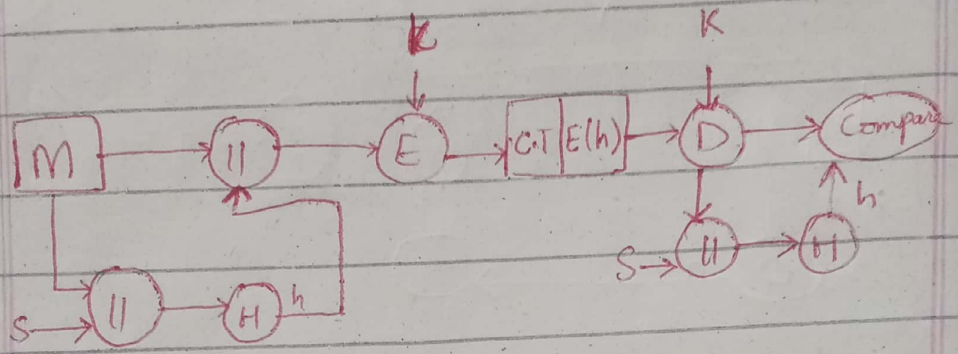
→ Authentication ✓

→ Confidentiality ✓

(5)



(6)



Sender.

Basic Concepts of IS

→ Asset: any valuable thing of Company
→ Vulnerability: Weakness and defect
→ Threat: potential danger to asset
→ Threat agent: entity which causes threat
→ Exposure Factor / Impact: %age of asset loss
→ Risk
Control / counter Measurement / Safegaurd

Security Control

Control:
implemented to reduce the risk.
e.g: fire extinguishers, password policy, firewall.

Types of Control:

i- Physical (Guards, Id badges etc)
ii - Logical (Administrative → Policy & Procedure)

intrusion detection system

(Technical ⇒ firewall, IDS, antivirus

→ Policies requires procedures to implement them.

Standards:

mandatory actions, activities and rules.

eg: ISO 2001 etc

Baselines:

refers to a point in time that is used as a comparison for future changes.

Guidelines:

recommended actions and operational guide.

Control functionalities:

Deterrent : discourage a potential attacker

Preventive : avoid an incident from occuring

Corrective : fixes systems after incident has occured

Recovery : bring back to regular operations

Detective : helps identify intruder/activities

Compensative : provide

Preventive : Technical

- → Passwords, Biometric, smart cards
- → encryption, secure protocols, call-back systems, DB, UI
- → Antimalware software, ACL, firewalls intrusion protection systems.

Preventive : Physical

- → Badges, swipe cards
- → Guards, dogs
- → Fences, locks, mantraps

Preventive : Administrative

- → Policies and procedures
- → Effective hiring practices
- → Pre-employment background checks
- → Controlled termination processes
- → Data classification & labeling
- → Security awareness.

CamScanner

Defense In Depth

Physical Security

SLE: Single Loss Expectency:
asset value x exposure factor

ARO: Annualize Rate of occurance
Yearly based Threat

ALE: Analyze Loss Expectency:
ARO* SLE

Access Control chapter 05

1- identification:
→ Recognize one from many

2- Authentication:
→ act of identity verification
Something you know (Passwords)
Something you have (Cards)
Something you are (biometric)

3- Authentication:
Verifying the uses authority

Access Control Model:
i- Mac (Mandatory Access Control Model)
ii- DAC (Discretionary Access Control) Model

3. iii Role Base Access Control (RBAC):

iv Access Control lists:

4. Rule Based Access control

4- Accountability:

Non-repudiation