

UNIT - III

(1)

Hash Functions and Digital Signatures:-

Authentication requirement - (2)

Authentication function - (2)

MAC (Message Authentication Code) - (4)

Hash function - (6)

Security of hash function and MAC - (5)

MD5 (Message Digest 5) - (9)

SHA (Secure Hash Algorithm) - (11)

HMAC - (13)

CMAC - (15)

Digital signature and Authentication Protocols } - (16)

DSS - (19)

El-Gamal - (23)

Schnorr - (26)

UNIT-III

2

HASH FUNCTIONS AND DIGITAL SIGNATURE

Authentication requirements :-

- * Disclosure
- * Traffic analysis
- * Masquerade
- * Content modification
- * Sequence "
- * Timing "
- * Source repudiation
- * Destination "

Message Authentication Function :-

- * Hash function
- * Message encryption
- * Message authentication code (MAC).

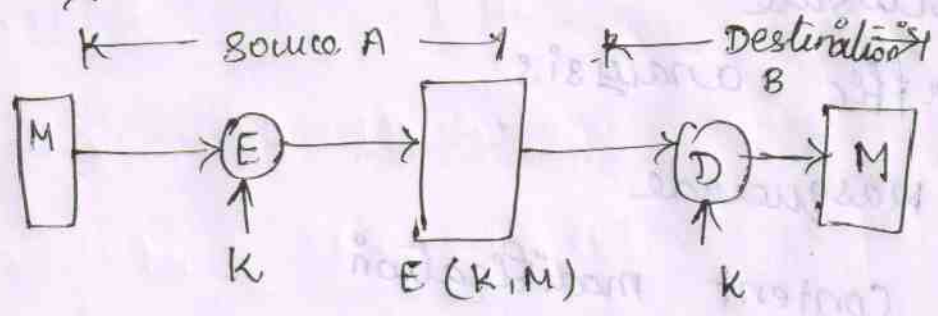
Message Encryption :-

Symmetric message encryption :-

- * Encryption provides authentication
- * Receiver know sender must have created it.

* know content cannot be altered. (3)

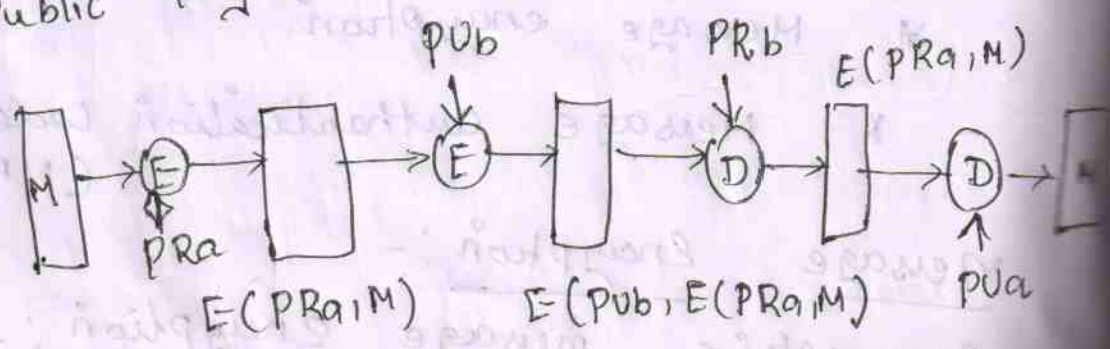
* If msg has suitable structure, redundancy (or) a checksum to detect any changes.



Confidentiality & authentication

Public-key Message Encryption :-

* Encryption provides no confidence of Sender. * Sender signs msg using their private key. then encrypts with recipient's public key.



Confidentiality, authentication & Signature.

3

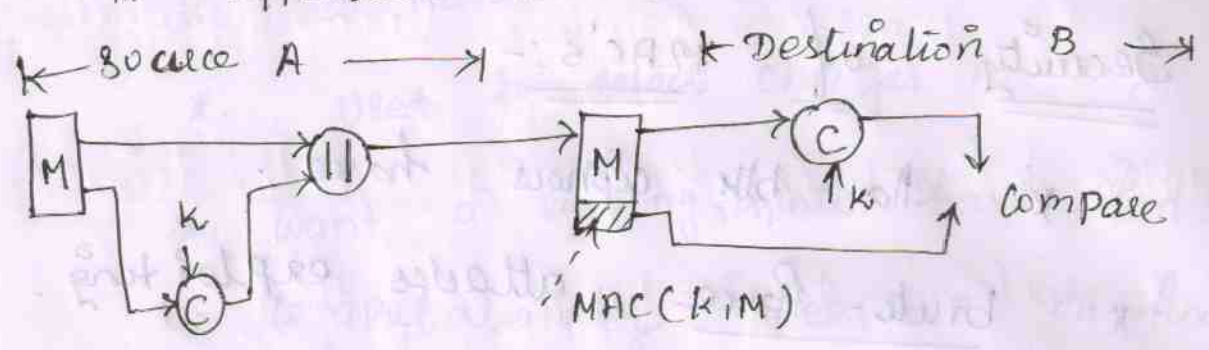
Message Authentication Code (MAC)

* A small fixed-sized blk of data

4

$$MAC = C(K, M)$$

* appended to msg when sent.



Why use a MAC?

* Sometimes only authentication is needed.

* Sometimes need authentication to persist longer than the encryption.

Ex: archival use.

* MAC is not a digital signature.

Properties:-

* a MAC is a cryptographic checksum

$$MAC = C_K(M)$$

* Many-to-one fun.

Requirements:-

* Knowing a msg & MAC is

infeasible to find another msg with same MAC.

of



* MAC should be uniformly distributed

* MAC should depend equally on all bits of the msg. (5)

Security of MAC's:-

x. No blk ciphers have:

x. brute-force attacks exploiting.

> Strong collision resistance hash have

cost $2^{m/2}$,

(i) 128 bit hash looks vulnerable,

160-bit better

> MAC's with known msg-MAC pairs

(i) Can either attack key space (or)

MAC. At least 128-bit MAC is needed for security.

* Cryptanalytic attacks exploit

Structure like blk ciphers want brute-

force attacks to be the best alternative

* More variety of MACs so hard

to generalize abt cryptanalysis.

Hash Functions

(6)

* Condenses arbitrary msg to fixed size

$$h = H(M)$$

* Assume hash fun is public.

* Used to detect changes to msg.

* Want a cryptographic hash fun.

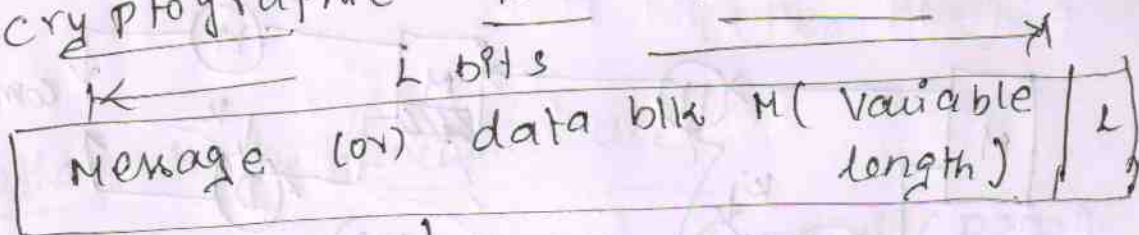
↳ computationally infeasible to find data mapping to specific hash.

(one-way property).

↳ computationally infeasible to find two data to same hash.

(collision-free property).

cryptographic hash function:-



Hash value h
(fixed length).

Hash function Uses:-

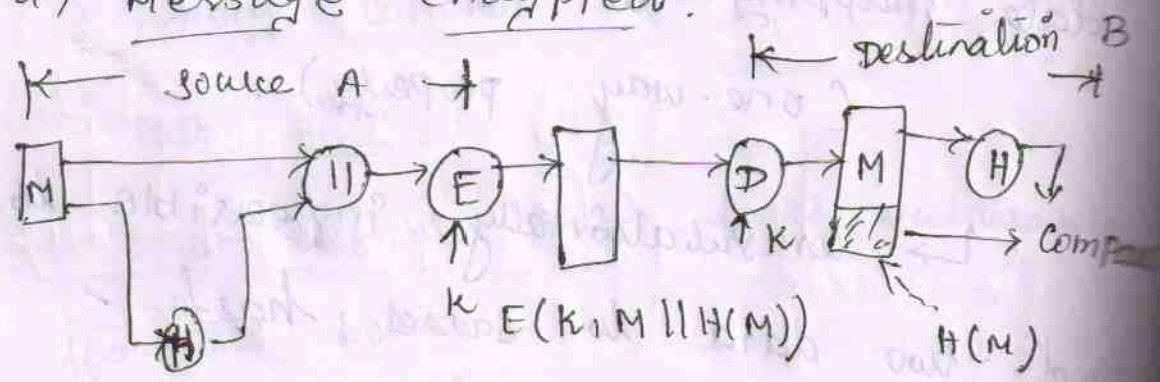
(7)

- * Msg Integrity check (MIC)
- * Msg Authentication code (MAC)
- * Digital signature (non-repudiation)

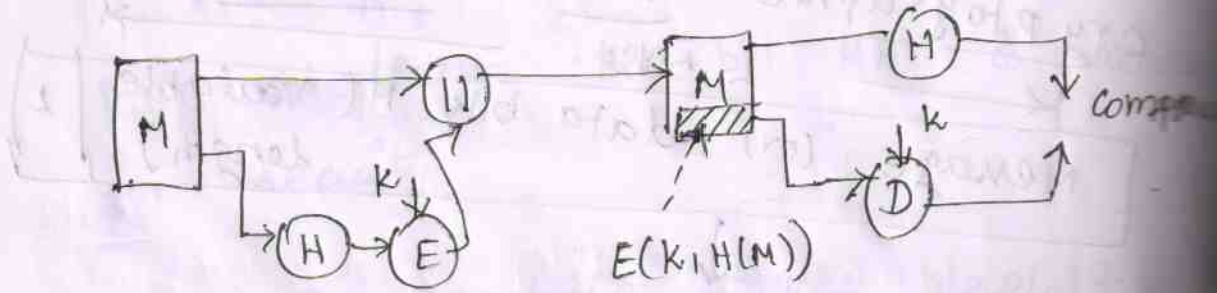
Hash functions & Message Authentication

Symmetric key Un-keyed Hash:-

a) Message encrypted.

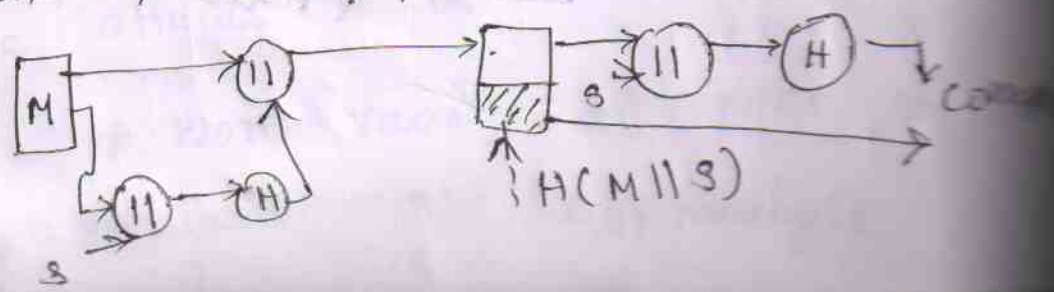


b) Message unencrypted:-

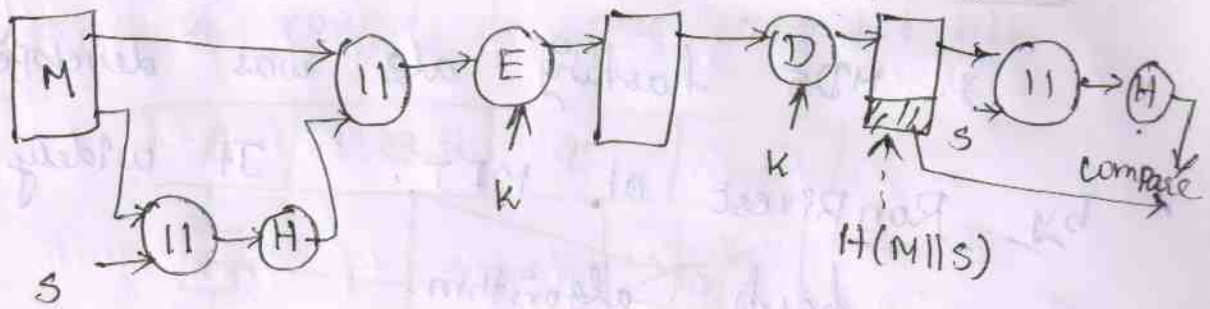


Symmetric key - keyed Hash:-

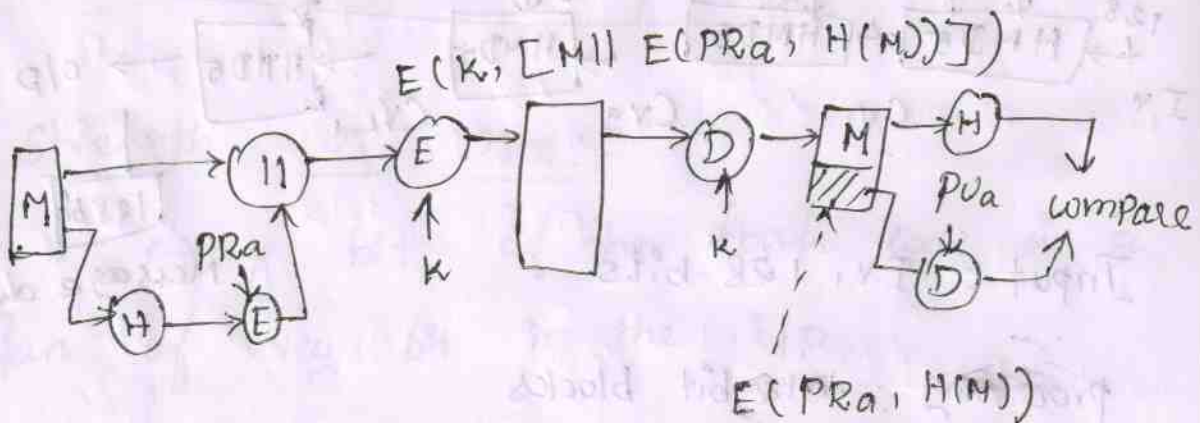
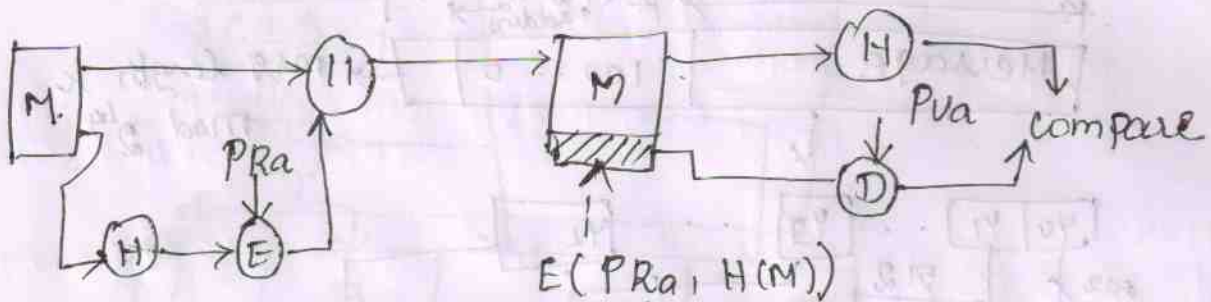
a) Msg unencrypted:-



b) Msg Encrypted :- $E(K, [M || H(M || S)])$ (8)



Hash Functions & Digital Signatures - PKCS:-



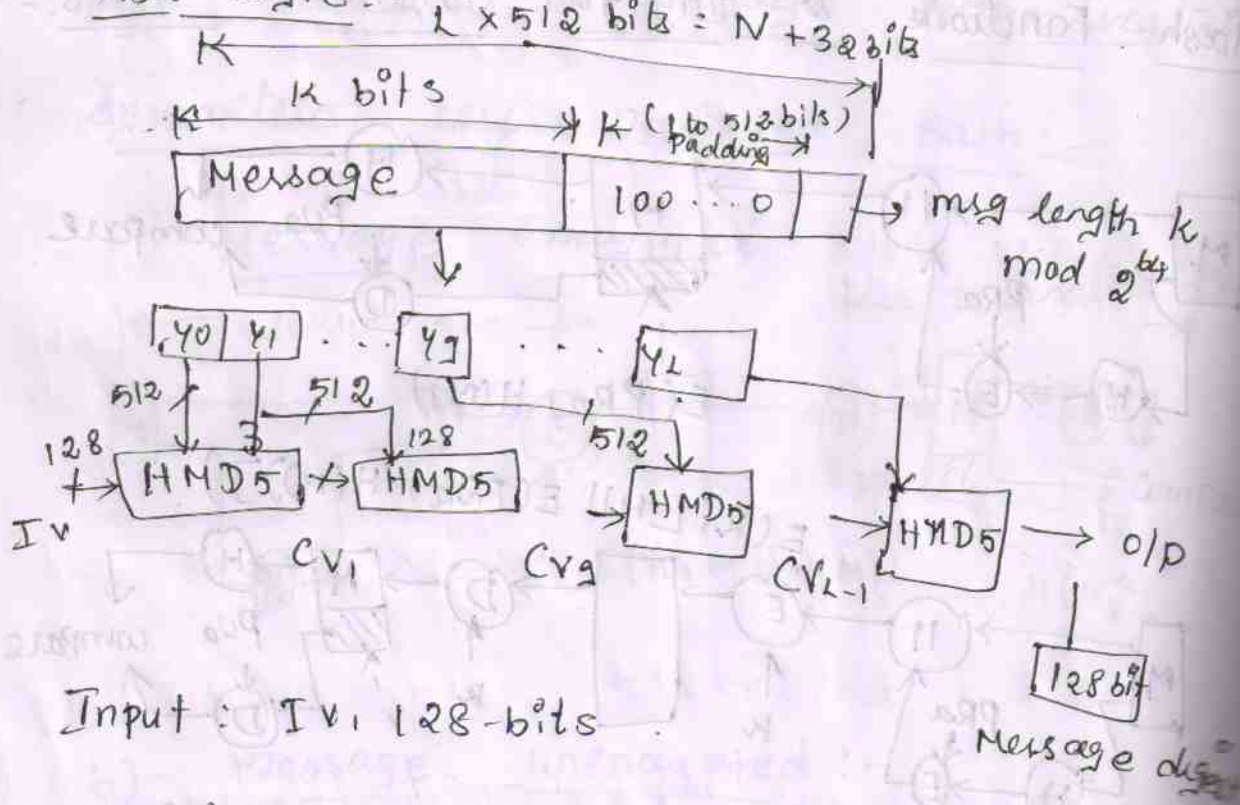
Other Hash function uses :-

- * Pseudo random function (PRF)
- * Pseudorandom number generator (PRNG)
- * To create a one-way Pwd file
- * For intrusion detection & virus detection

MD5 - [Message Digest Algorithm]

* MD5 hashing alg was developed by Ron Rivest at MIT. It widely use secure hash algorithm.

MD5 Logic :-



Input : IV, 128-bits

Processing : 512 bit blocks

output : 128 bit msg digest

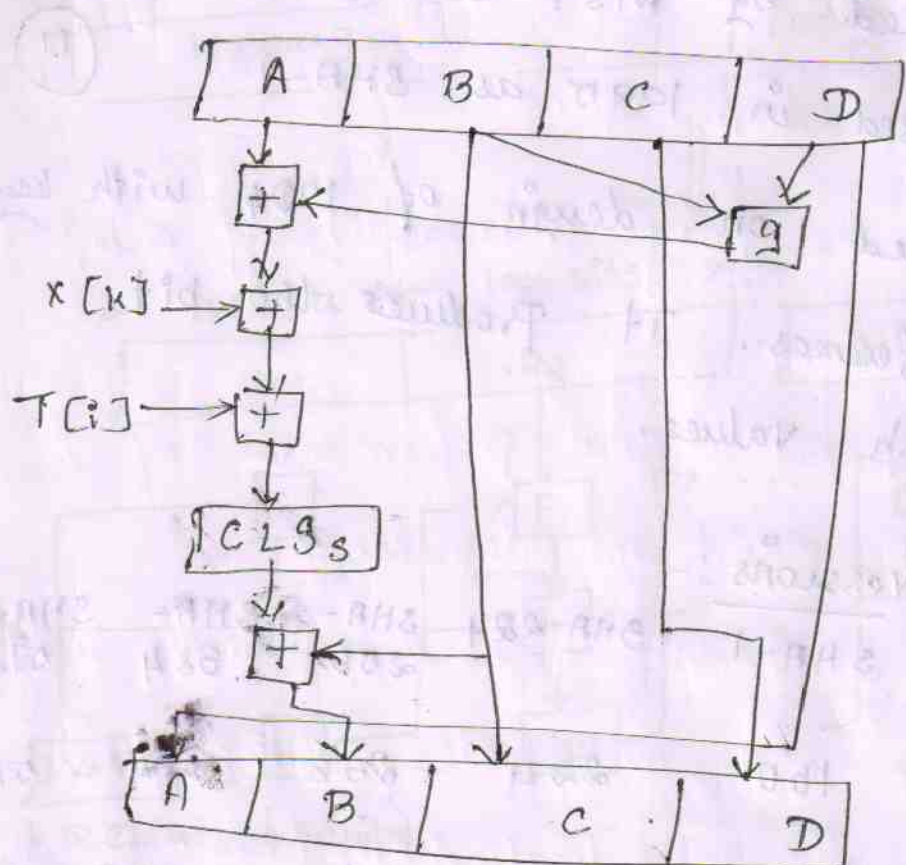
Steps :

- 1) Append padding bits
- 2) Append length
- 3) Initialize the MD Buffer
- 4) processing 512 Bit Block.

MD5 Compression Function :-

(6)

* A round to one 512 bit blk



Strength of MD5 :-

* Every bit of the hash code is a function of every bit in the i/p.

* When 2 msg chosen at random will not have the same hash code.

Attacks on MD5 :-

* Differential crypt analysis.

* Pseudo collision.

