Usage of hash functions.

- to confirm dowloaded the correct file.
- to provide message integrity
- to provide authentication.

H(x) → hash function.

- from hash function can identify unintentional modification, Cant identify intentional modification.
- There is no way to identify the unique sender.

MD5
SHA-256 → mostly used.

- SHA can have 2^{64} valued input and produce 160 bit hash value.
- MD5 have 2^{128} valued outputs.

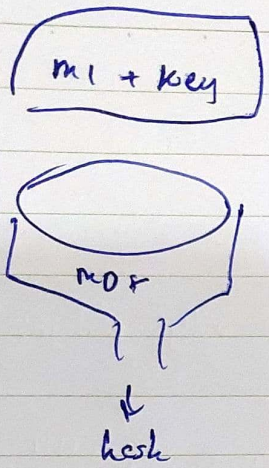
MD5 - low secure / fast
SHA → high secure / slow.

keyed hash message Authentication code (HMAC / KHMAC)

- not as regular hash function this has keys to overcome the identifying the issue of unintentional modifications.

HMAC has → hash function + Secret key.

- Some key for both ends.



Characteristics of key managment

- key generation
- Verification
- Storage
- exchange
- key ~~dest~~ revocation and destruction.

2 term that used to describe a key.

- key size - no of bits in a key (length)
  ex : MD5 = 128 bit.
- key space - all possible keys that can be generated
  ex : MD5 = 2^{128}

Symmetric - great for bulck data encryption

Choosing Cryptographic keys.

- Performance
- Security
-

Date No

Cryptography III

ICS lec 7

Symetric encryption keys

- DES (Weaker)
- 3DES
- AES (Stronger)

} Confidentiality

- Confidentiality may depending on keys, in Symetric key always give confidentiality.

IPsec - Network Layer Confidentiality
SSL/TLS - Session Layer Confidentiality.
Secure messaging - application layer confidentiality.

Symmetric key Algorithm.

- Same key used to enc/DEC. (shared secret key)
- key length 80/256 bit
- Speed
- DES, 3DES, AES

Asymetric key algorithm.

- public key algorithm
- key length 512 - 4096 bits
- have private and public key
- public key shared private key not.
- RSA, DH.

Date No

2 type of Symetric Encryption techniques

- block ciphers
- Stream ciphers

Block ciphers,

- devide the cipher text to fixed length parts and encrypt all parts at once.
- each block 64 or 128 bit.

Ex : DES → 64 bit block
AES → 128 bit block / 192 / 256

Stream ciphers,

- encrypt plain text one byte or one bit at a time. (character by character).
- Can be faster than Block ciphers. (Data transit)

Ex : A5 - used in mobile communication.
RC4

Compare block, stream ciphers based on speed of enc, size of output, and security.

	Block cipher		Stream Cipher
Speed	data at rest	faster	slower
	data at trans	slower	faster
size of output		~~Same~~ Can be larger	Same
Security		Secure than stream	

Choosing an algorithm

- algorithm is trusted by Cryptographic community.
- trusted algorithem or not.
- Does it protect against brute-force attack.
- Does it support variables and long length keys.
- Does it have export or import restrictions

Data encryption Standard (DES)

- not used these days. only 64 bit key length actually 56 bit. convert it to 64 bit.

(2^{56})

Date No

DES operation modes,

- ECB
- CBC

ECB - not suitable to use large data encryptions.

CBC -