Cryptography II

ICS lec 6

Cryptographic algorithms

MD5 }
SHA } Integrety

HMAC - MD5 }
RSA and DSA } Authentication.

DES }
3DES } Confidentiality.
AES }

Hash functions.

- take a input as message and convert it to a fixed length message.
  - MD5 - 128 bit (Message diagest)(Digital fingerprint
  - SHA - 160 bit.
- a message can be converted to a fixed length but harder to reverse it. (one way)

hashing provids.

- Data integrity
- Authentication.

- if hash function generate same values for 2 or more it called Collision.
- dont have keys in hash function.

Usage of hash functions.

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

$\boxed{H(x)}$ → 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

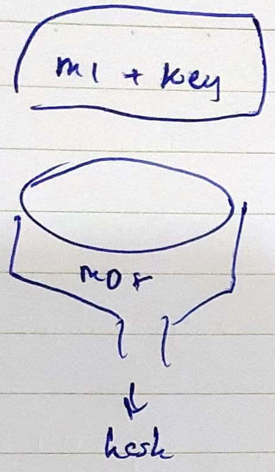
SHA → high secure / slow.

keyed hash message Authentication Code (HMAC / HAMAC)

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

HMAC has → hash function + secret key.

- Same key for both ends.



Charasteristics of key managment

- key generation
- Verification
- Storage
- exchange
- key ~~[illegible]~~ 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
-