Cryptographic hash functions

Lecture 5

Hash functions

- A hash function is a function that is easy to compute, but hard to invert.
- Hash: {arbitrary size documents} → $\{0, 1\}^k$ that satisfies:
  - One-way function: it is easy to compute h=Hash(D), but hard to invert h from H(D).
  - Collision resistance: it is very difficult to find to distinct input D and D’ whose output Hash(D) and Hash(D’) are the same.

Hash function implementation

- Common hash: MD5, SHA
- Using an encryption function: symmetric/asymmetric encryptions.
- If H1 and H2 are two different hashes, then $H1 \circ H2$ and $H2 \circ H1$ are hashes.

Modular Arithmetic Secure Hash

- MASH-2: generate a n-bit hash value from a document of size b bits, $1 \leq b \leq 2^{n/2}$.

(1)Generate two m-bit primes p and q, and set M= pq

(2)Get n = 16k: $16k \leq m \leq 16(k+1)$

(3)H = 0, A = 11110000…0000

(4)Split document D to t (n/2)-bit blocks $x_1,\ldots, x_t$. Let x_{t+1} = binary(b)

(5)For i=1 to t: split x_i to 4-bit blocks $x_{i1},\ldots, x_{ij}$,
and let $y_i = 1111x_{i1}\ldots 1111x_{ij}$.
With (t+1)th block x_{t+1} to $y_{t+1}= 1010x_{(t+1)1}\ldots 1010x_{(t+1)j}$.
Let $y = y_1\ldots y_{t+1}$.

(6) For i=1 to t+1: F = (H XOR y_i) OR A$)^{257}$ (mod M).
Let G be the lowest n bits of F, and H=G XOR H;

(7) Return H

Application of hash

1. Hash is used to authenticate messages: MAC=Hashed Code.
2. Hash is used in digital signature schemes: Signature(d, D)=E(d, Hash(D)) and verification is whether Hash(D)==E(e, Signature),where e is the public key and d, the private key of signer.
3. Hash is used to protect password which stored on servers.