

Network Security Notes (October 5 2009)

By Supreet Padhi

Message Integrity

- MAC which is defined over (t, q, q', ϵ)
- INT-PTXT.
- PRFs are good MACs.
- HMAC- Hash functions used for MAC.
- IND-CCA security.

Hash Functions

A hash function usually means a function that compresses, meaning the output is shorter than the input. Such a function takes an input of arbitrary or almost arbitrary length to one whose length is a fixed number like 128 bits.

$$H : \{0,1\}^* \longrightarrow \{0,1\}^l$$

- Publicly known
- No key is used.

Example

- MD5
- SHA1
- SHA-256
- SHA-512

Properties

- Collision rare
- Small output
- Fast
- Collisions very hard to find i.e. strong collision resistant
- Should conceal all information about the input/file.
- Input can't be recovered from output

Randomness of hash functions is also used as a design methodology towards achieving collision-resistance.

Definition: A random oracle is a function $R: \{0,1\}^* \longrightarrow \{0,1\}^l$

HMAC

Hash functions are used to build MACs. It is used for internet security protocols. It is used in SSH and SSL.

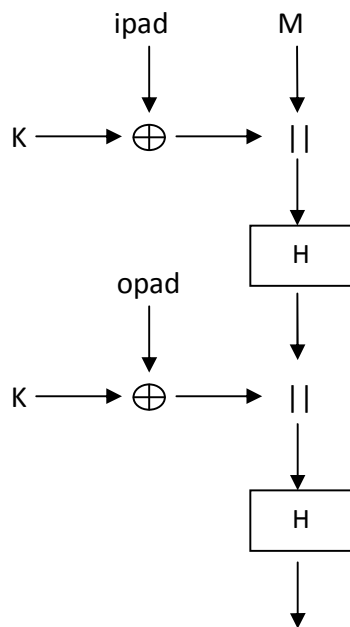
$$\text{HMAC}(K,M) = H(K \oplus \text{opad} || H(K \oplus \text{ipad} || M))$$

where ipad= the byte 0x36 repeated 64 times

opad= the byte 0x5C repeated 64 times.

K = message authentication secret key

H = Hash function (SHA-1, SHA-256 etc)



- HMAC uses H as a black box. This makes easier to implement HMAC since H can be replaced with the desired hash function.
- HMAC is secure if H is collision resistant and key is chosen as uniform random function.