

Network Security

Lecture Notes, Oct 5th 2009

Message Integrity:

- MAC
- (t, q, q', ϵ) – MACs : Integrity of plain text
- PRF is a MAC
- HMAC
- IND-CCA
- Hash Functions

Hash Functions:

A Hash function generates a fingerprint. $H: \{0, 1\}^* \longrightarrow \{0, 1\}^l$.

The hash function is publicly known and has no key.

Some of the examples of hash functions are: MD5, SHA-1, SHA-256, SHA-512 etc..

Properties of Hash functions:

- Collisions are rare
- Small output
- Fast
- Collisions are very hard to find.
- Should conceal all information about a file.
- Strong vs Weak Collision Resistance
- Cannot recover input from output.

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

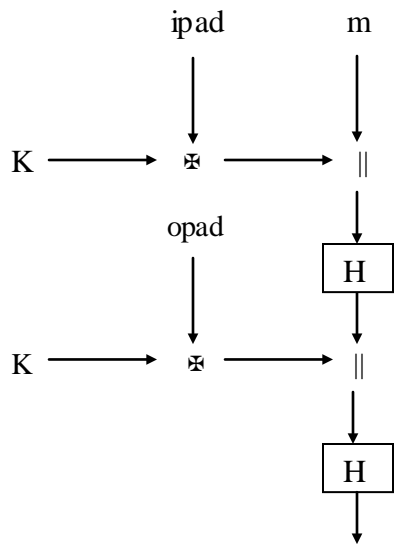
HMAC:

HMAC uses any hash function to build a MAC.

$HMAC(K, m) = H(K \oplus \text{opad} \parallel H(K \oplus \text{ipad} \parallel m))$

Where $\text{ipad} = 0x530x53 \dots 0x53$

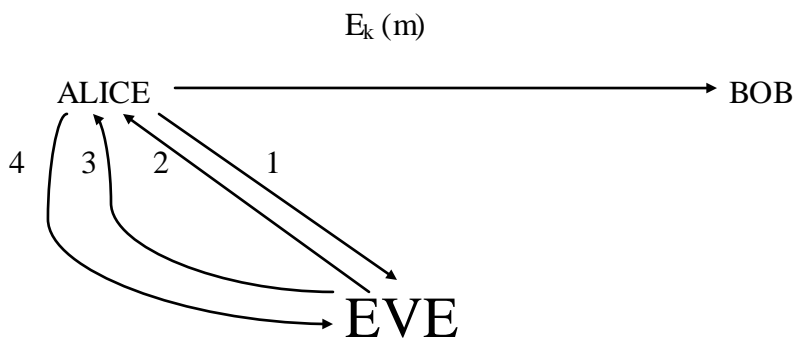
and $\text{opad} = 0x360x36 \dots 0x36$



Theorem:

HMAC is secure if H is collision resistant and key is chosen uniformly randomly.

CHOSEN CIPHER TEXT SECURITY:



In the ideal world,

- 1: $E_k(m)$
- 2: Encrypt m
- 3: Decrypt c
- 4: $D_k(c)$

In the real world,

- 1: $E_k(m)$
- 2: Encrypt m
- 3: Decrypt c
- 4: $D_k(c)$