

# NETWORK SECURITY

## 10/5/09 Class Notes

By: Aman Jain

### Hash Functions:

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

- a) Hashing Algorithm is Publicly Known
- b) They don't require a key.

Some examples of Hash functions:

- a. MD5(very broken)
- b. SHA1(broken)
- c. SHA256 (ok for now)
- d. SHA512
- e. RIPEMD-160

### PROPERTIES:

- a. Collisions in hash values should be rare.
- b. Should be fast to compute.
- c. Output should be small
- d. Collisions should be very hard to find.

- e. Should conceal the information about the input
- f. Can't recover input from output

**Def:** A Random Oracle is a random and deterministic function,

$$R: \{0,1\}^* \longrightarrow \{0,1\}^L$$

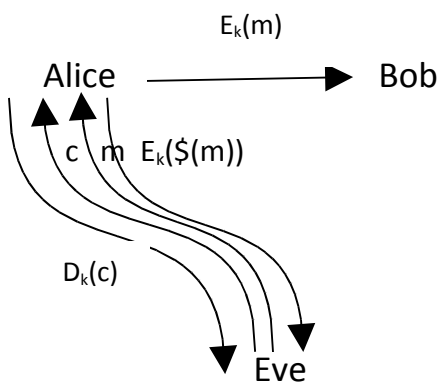
**HMAC:**

$$\text{HMAC}(k,M) = H(k \oplus \text{opad} \parallel H(k \oplus \text{ipad} \parallel M))$$

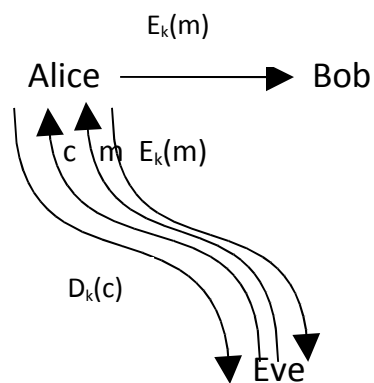
where ipad and opad are some 64 byte constants

**Theorem:** HMAC is secure if H is collision resistant.

Ideal World



Real World



Assumption: Eve can't query  $D_k$  on 'C' if C is returned by encryption oracle