

## Network Security

Sumeet P Dash

October 5, 2009

### Hash Function:

A hash function  $H$  can be defined as:

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

- The details of a hash function are publicly known.
- The hash function uses no secret key to produce its output.

Some of the examples of a hash function are the following.

- MD5 (broken)
- SHA1 (broken)
- SHA-256 (Secure for now)
- SHA-512
- RIPEMD-160

### Desirable Properties of a Hash Function:

- Collisions in output values should be rare or should be very hard to locate.
- Output should be small and manageable.
- Should be fast in execution.
- Should conceal all information about its input (that could be a file).
- Input mustn't be recoverable from the output.

Some of the hashing schemes exhibit strong collision resistance while some others have weak resistance towards collisions. In order to build a secure system, a hashing scheme with strong resistance is desirable.

### Random Oracle:

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

### HMAC (keyed-Hash Message Authentication Code):

A HMAC is a type of MAC built upon a combination of a cryptographic hash function and a secret key.

$$\text{HMAC}(\text{key}, \text{message}) = H(\text{key} \oplus \text{opad} \parallel H(\text{key} \oplus \text{ipad} \parallel \text{message}))$$

Where  $H$  = component hash function

$$\text{opad} = [0x5c * \text{blocksize}] \text{ [blocksize is that of the underlying hash function]}$$

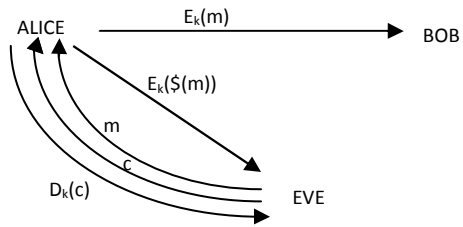
$$\text{ipad} = [0x36 * \text{blocksize}]$$

### Theorem:

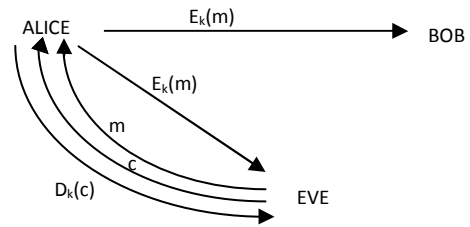
HMAC is secure if  $H$  is collision resistant and the key is chosen uniformly randomly.

## Decryption Oracle in Ideal vs. Real World:

Ideal world:



Real World:



Eve can't query  $D_k$  on  $C$ , if  $C$  is returned by the encryption oracle.