

**Message Integrity:**

- MACs
- $(t, q, q', \varepsilon)$  - MACs
- PRFs are MACs

**Today:**

- HMAC
- IND-CCA2
- Hash Function

**Hash Function:**

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

A hash function maps a variable length string onto a fixed length string. In a way it works as a compression function except for the collisions.

**Properties:**

- Publicly known
- No secret key

Example:

- MD5 (broken)
- SHA1 (broken)
- SHA256 (not broken yet)
- SHA512
- [RIPEMD-160](#)

**Properties:**

- Ideally Collision Free
- Collision Resistant
  - Weak Collision Resistance
  - Strong Collision Resistance
- Small Output
- Fast
- hash value should not divulge any information of the hashed string

**Remark:** The last property includes the property that input should not be recoverable from output. In fact this is a stronger notion. If hash value does not divulge anything about the hashed input then not only it is impossible to reconstruct the input from it but no other information related to input e.g. some meta information like input size can be determined.

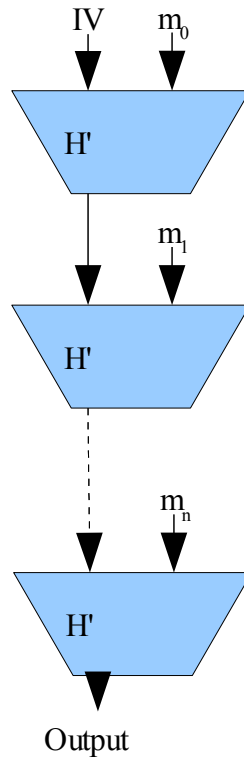
**Def: Random Oracle**

A Random Oracle is a deterministic random function such that:

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

**Remark:** If something is proven in a random Oracle model, the prover has used some hash function and the proof depends on the security of the hash function.

**A Sample Hash Construction:**



**HMAC:**

HMAC uses a hash function in order to build a MAC.

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

Where H is the hash function and ipad and opad are magic numbers such that

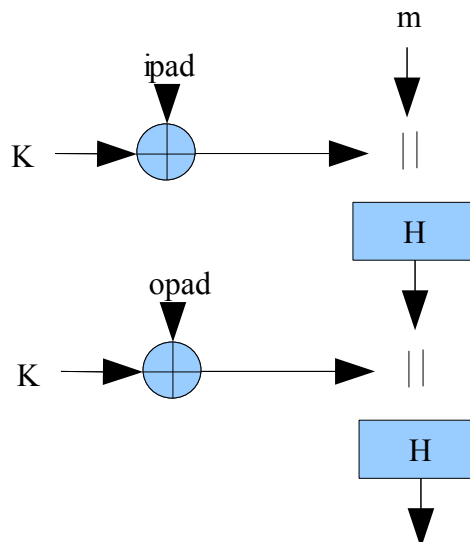
$$\mathbf{\text{opad} = [0x53 * \text{blocksize of H}]}$$

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

**Theorem:**

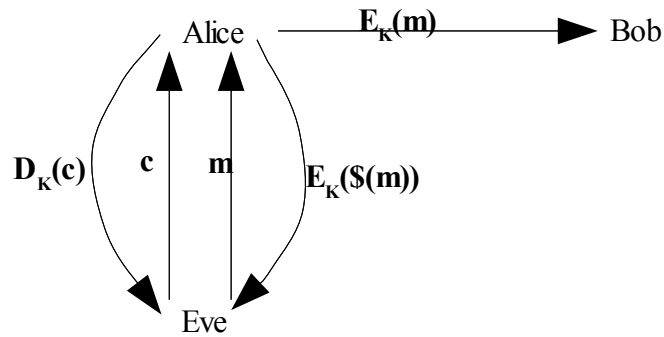
HMAC is secure if H is collision resistant and the key is chosen uniformly randomly.

**Construction:**



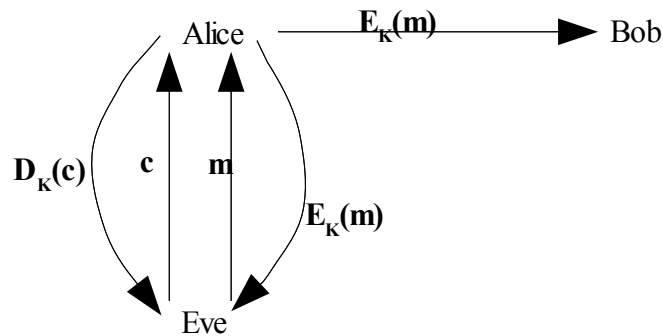
**IND-CCA2 (INDistinguishability under adaptive Chosen Ciphertext Attack):**

**Ideal World:**



$D_k$  is the Decryption Oracle, which returns nothing if the input was invalid and the ciphertext if it was valid.

**Real World:**



Eve cannot query the Decryption Oracle on a ciphertext that she obtained from the Encryption Oracle for a message that she submitted to it. We place this restriction on Eve because this attack, despite successfully distinguishing real world from ideal world, does not reveal any insecurity in the encryption scheme itself. It can be a valid attack on some system and there are mechanisms to deal with it but in our discussion it is not a valid attack because our aim is to prove the security of the encryption scheme.