# Secure MAC

**Chosen Cipher text Attack**

In CCA attack, the adversary has the ability to encrypt any messages of his choice and also to decrypt any cipher texts of his choice.

CCA security actually implies a very important property called non-malleability. A non-malleable encryption scheme offers has the property that if the adversary tries to modify a given cipher text, he either gets an illegal cipher text or the irrelated encryption of plain text message to the original one.

**Message Authentication Code(MAC)**

The aim of message authentication code is to verify that the message sent by the sender is not modified in between. Both the parties will share the secret key cryptography; therefore this notion of Message Authentication Code belongs to the world of Private Key Cryptography. The MAC tuple consists of probabilistic polynomial time algorithms (Gen, Mac, Vrfy).

**Gen:** The Algorithm Gen outputs the uniformly distributed random key of length n{0,1}.

**Mac:** The Algorithm Mac on input key 'k' of length n and a message 'm' of arbitrary length, outputs a tag t of arbitrary length. The value t is called Mac tag.

**Vrfy:** The Algorithm Vrfy on input key 'k' of length n, a message 'm' of arbitrary length, a tag t of arbitrary length outputs a bit b {0,1}. If the message is not modified, then the value of b is 1, otherwise 0.

A message authentication code (Gen,MAC,Vrfy) is secure if for all probabilistic polynomial-time adversaries ***A***:

$$Pr[\text{Mac-Game}(n) = 1] \leq \text{negl}(n)$$

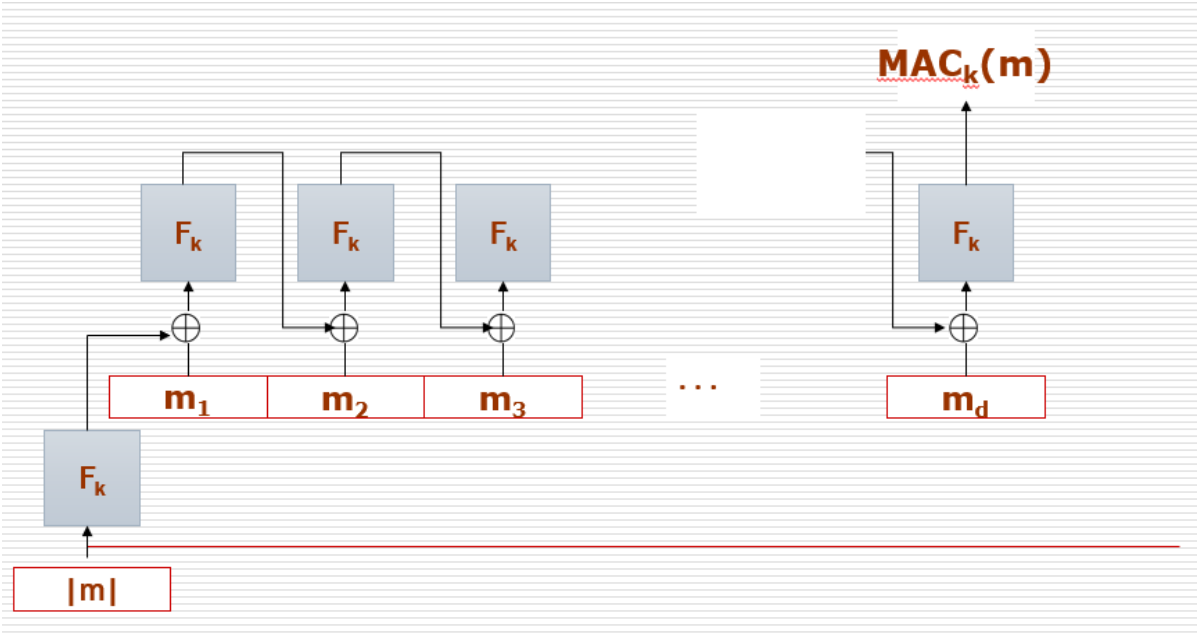
**Construction of MAC using PRF:**

**Gen**: Takes the input of $1^n$ and outputs a key of length n.

**MAC**: Takes the key k and message m as input and output $F_k(m)$ as output where F is a Pseudo Random Function.

**Vrfy**: Takes the message m, key k and tag t as input and outputs ACCEPT if $F_k(m) == t$

The above scheme is used for fixed length MAC.
In order to construct variable length MAC which is secure, the message length is prepended to the message.


MAC_k(m)
F_k
F_k
F_k
F_k
m_1
m_2
m_3
...
m_d
F_k
|m|