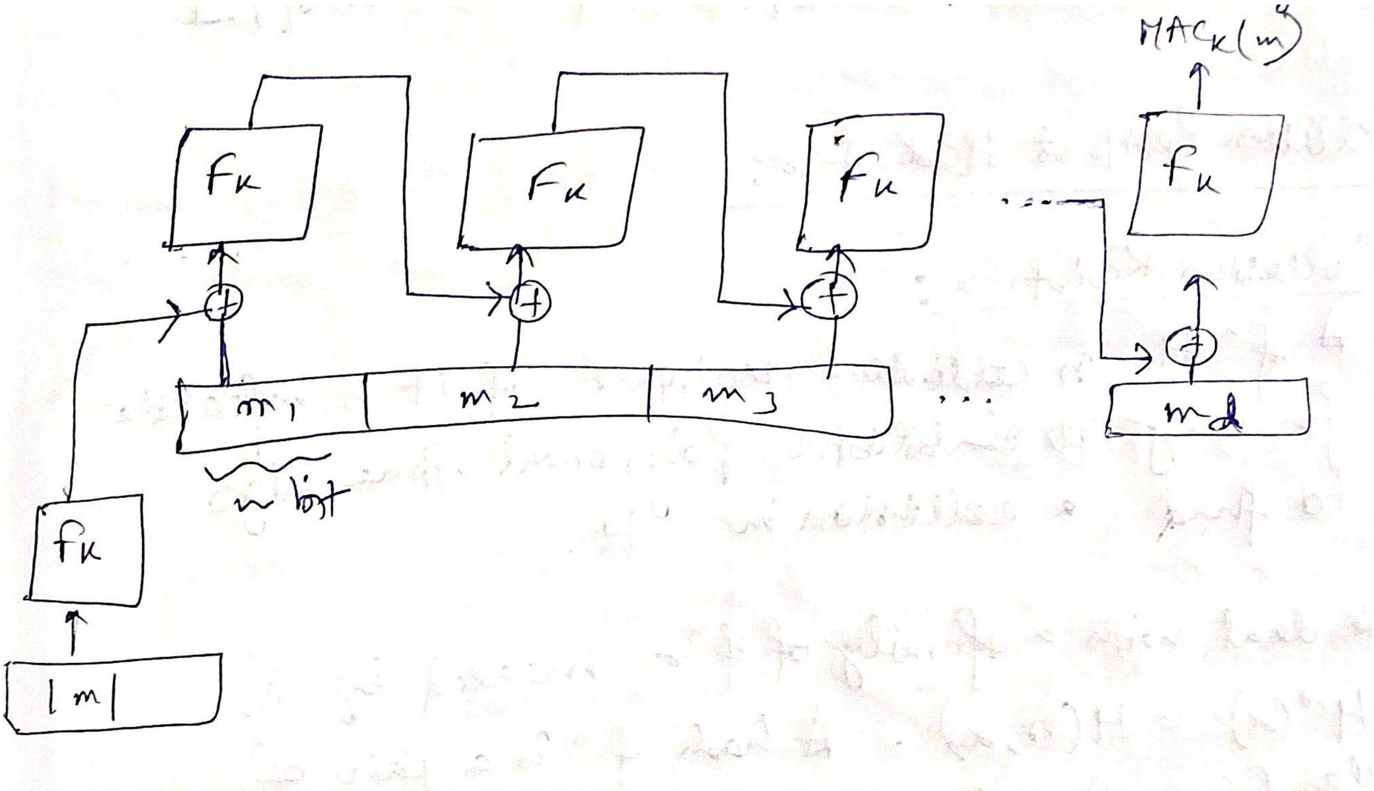
MAC ensures that the message being sent is not modified in the middle by an adversary. The components of this authentication protocol is as follows:

- A key generation algorithm that returns a secret key K.
- A MAC generation algorithm that returns a tag for a given message m. Tag t = $\text{MAC}_k(m)$.
- A verification algorithm that returns a bit b = $\text{Verify}_k(m_1, t_1)$ given a message m_1 and tag t_1.
- If the message is not modified then with high probability the value of b is true, otherwise false.

$$\text{Gen}(1^n) \text{ chooses k to be a random n-bit string.}$$
$$\text{MAC}_k(m) = F_k(m) = t.$$
$$\text{Verify}_k(m,t) = \text{accept iff } t = F_k(m)$$

If F is a PRF, then the above scheme is a secured fixed length MAC.

This works only for messages of n-bit length. For longer messages with several blocks of n-bits, we can use CBC-MAC. In CBC-MAC, the message is divided into blocks of n-bits. The length of the message is encrypted initially. The output is XORed with a block of message and the result is encrypted which serves as the input for the next stage and so on.


MACk(m)
Fk
Fk
Fk
Fk
Fk
m1
m2
m3
...
md
n bit
|m|