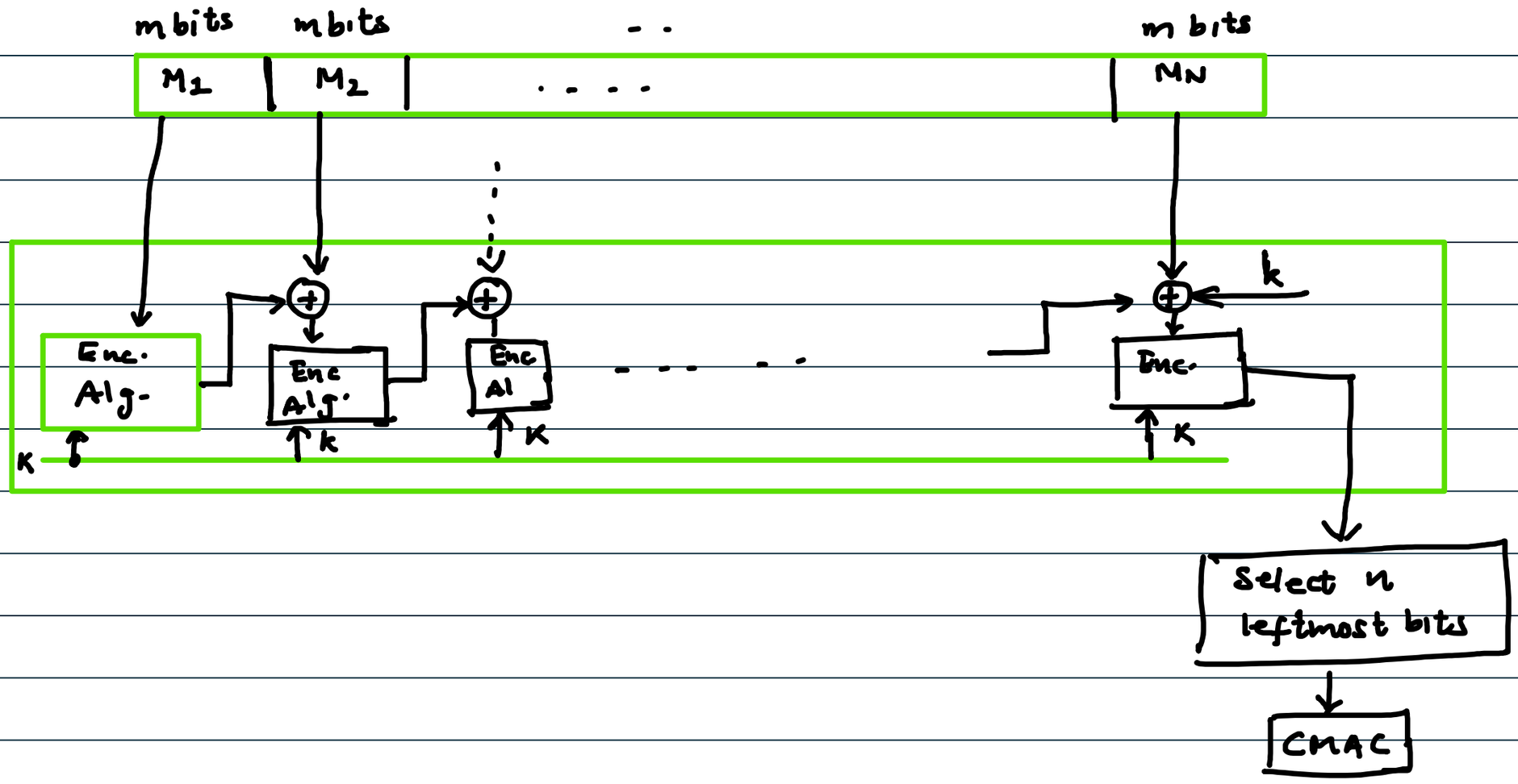
CMAC (Data Authentication Algorithm)



Step 1: Divide the msg into N blocks of m bits

Step 2: Pad the last block with a 1 bit followed by enough 0 bits to m-bits

Step 3: Find $C_1 = E_K(M_1)$, $C_2 = E_K(C_1 \oplus M_2)$, $C_3 = E_K(C_2 \oplus M_3)$, ---,

$$C_{N-1} = E_K(C_{N-2} \oplus M_{N-1}), \quad C_N = E_K(C_{N-1} \oplus M_N \oplus k)$$

where E_K is the encryption alg with the key K

Step 4: Select n leftmost bits of C_N. It would give us the n-bit CMAC

Key Generation for the Last Step

Step 1: Find $C = E_K(\underbrace{000\cdots0}_{m \text{ bits}})$

Step 2:
$$k = \begin{cases} xC & \text{if no padding in } M_N \\ x^2C & \text{if padding is applied in } M_N. \end{cases}$$

Here, the multiplication is in the field $GF(2^m)$ with the irreducible poly of degree m selected by the particular protocol

Note: 1. MACs provides msg integrity & msg auth.

2. MACs are much faster than the digital sign

Hash Function

This is a function that creates a fixed sized digest out of a variable size msg.

Desirable Properties

1 Hash function should be computationally efficient.

2 Hash function should be of fixed length and it should be independent of the input length.

(In practice, output length of the hash value is b/w 128 bits to 512 bits

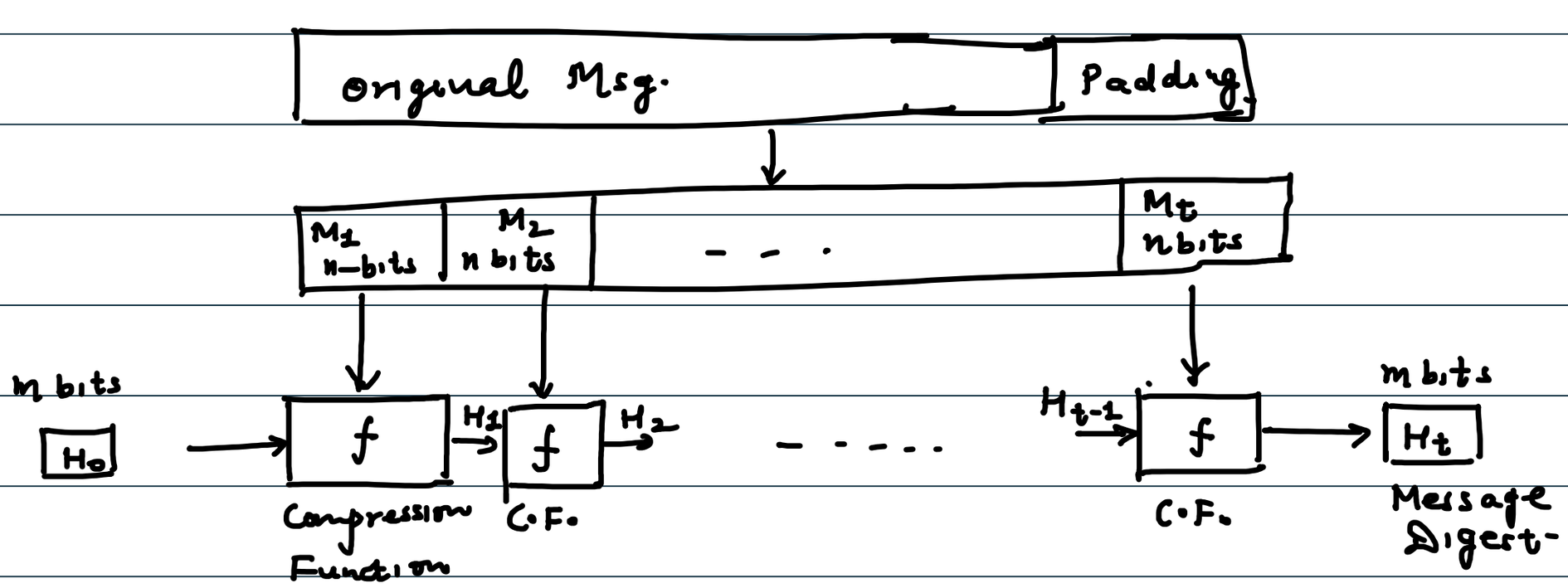
3 The computed hash value should be highly sensitive to all input bits

Security Requirements:

1 Preimage Resistance 2 Second Preimage Resistance 3 Collision Resistance

1. Given $h(x)$, it should be computationally infeasible to find x
2. Given $h(x)$, it should " " " " x' s.t. $h(x) = h(x')$
3. " " " " " " x & x' s.t. $h(x) = h(x')$

Merkle-Damgard scheme



Step 1 : Divide the msg into t blocks of n bits each after apply the padding if required

Step 2 : Compute $H_i = f(H_{i-1}, M_i)$, $i = 1, 2, \cdots, t$

Here H_0 is a fixed value which is called the intial value or intial vector

H_t is the cryptographic Hash function of the original msg.

$$H_t = h(M)$$

Note : If the compression function f is collision res. then hash function is collision resistant

Message Digest (MD) (Family of Hash alg.)

Ex : MD2, MD4, MD5

SHA (Secure Hash Algorithm)