Message Authentication Code (MAC)

The purpose of MAC is to create a tag t for a message m & a key k such that no adversary can create a new message m_1 & t_1 pair without the key ie. $Verify_k(m,t) = 1$ but $Verify_k(m_1,t_1) \neq 1$ unless m_1 & t_1 were generated with key k.

No efficient adversary should succeed in creating a message & tag pair without the correct key.

Instead of using the complicated variable length MAC scheme, the CBC-MAC was used which is simpler to understand and implement while also being more space efficient.

CBC-MAC Algorithm –

$Gen(1^n)$: uniformly dist key k

$Mack(m)$: key k & message m of length $l \cdot n$

1. $m = m_1 \cdots m_l$; m_i = n-bit
2. For $i=1$ to l

$$t_i = F_k(t_{i-1} \oplus m_i) \qquad F \in PRF$$

3. Output t_l.

$Vrfy_k(m,t)$: key k, & m of length l & output 1 when $t = Mack(m)$