Symmetric Key Integrity Mechanisms

Message Authentication Code (MAC)

Goal: Mallory can’t modify or construct valid messages.
- Replay Attacks
- Garbage Attacks

One time Pad:

\[ C = C_0, C_1, \ldots \]
\[ K = K_0, K_1, \ldots \]
\[ M = K_0 + M_0, K_1 + K_2, \ldots \]
Bit flipping can be done to change it.

MAC

\[ F(K, M) = \text{Tag} \]
\[ F: \{0, 1\}^p \times \{0, 1\}^* \rightarrow \{0, 1\}^m \]
- Mallory can’t guess Tag for any message.
- Mallory can’t combine previous messages/tags to construct new messages.
Hash Functions:

H: \{0, 1\}^* \rightarrow \{0, 1\}^M
H (M) = h
- given y, infeasible to find any x such that H (x) = y.
- infeasible to find x and x’, such that H (x) = H (x’).

Examples

MD4, MD5, SHA-0, SHA-1: Has been broken
SHA-256, SHA-512: Hasn’t been broken yet
RIPEMD – Okay to use

HMAC

H (K \oplus opad || H (K \oplus ipad || M))

ipad = Ox36 x 64 bytes
opad = Ox5c x 64 bytes
K is any L bit key. Example: HMAC - SHA-256

Fact: If H is secure then HMAC-H is secure.
You can compute H (M_1 \parallel M_2) from H (M_1) and M_2

MAC (K, M) = H (K \parallel M)
Mallory sees: Tag = (K \parallel M)

Then Mallory can compute:
H ((K \parallel M) \parallel M’) = MAC (K, M \parallel M’) From H (K \parallel M) and M’ = Tag
To send M secretly and unalterably I can:

1. Encrypt – then- MAC
   \[ C = E_k (M) \]
   \[ T = \text{MAC}_k (C) \]
   Send (C, T)

2. MAC – then – Encrypt
   \[ T = \text{MAC}_k (M) \]
   Send \( E_{k'} (M || T) \)

3. MAC and Encrypt
   \[ T = \text{MAC}_{k'} (M) \]
   \[ C = E_k (M) \]
   Send (C, T)

(3) does not work because it gives attacker double opportunity to get M.

(2) does not work under some abnormal settings. (Ask Professor)

(1) as of yet still works. It has not been broken.
Public Key Cryptography

So far, Alice & Bob both know K
- can’t distinguish Alice from Bob
- either party can betray other
- for n parties need \( \binom{n}{2} \) key < \( n^2 \)

In Public Key Cryptography, every person has a key that just they know.

\[
\begin{align*}
\text{Alice} & \quad C = E \left( P_A, M \right) \\
S_A, P_A & \quad \text{Bob} \\
& \quad P_A \\
& \quad \text{Charlie} \\
& \quad P_A \\
& \quad \text{Eve} \\
& \quad P_A
\end{align*}
\]

\[
M = D \left( S_A, C \right)
\]

Alice
- buys a safe
- keeps keys
- mails open safe to Bob
- uses secret key to open the safe when received

Bob
- stuffs M in the safe
- closes door
**Number Theory**

Defn: \( Z_n^* = (\mathbb{Z}/n\mathbb{Z})^* \)
\[ = \{ r \mid 0 < r < n, \gcd(r, n) = 1 \} \]

Defn: \( \varphi(n) = |Z_n^*| \)
Example: \( \varphi(7) = 6 \quad \varphi(p) = p-1 \)

\( \varphi(pq) = ?? \)

\[ Z_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\} \quad \varphi(15) = 8 = (3-1) (5-1) \]

\[ \varphi(pq) = pq - (q-1) - (p-1) - 1 \]
\[ = pq - q - p + 1 \]
\[ = (p-1)(q-1) \]

Defn:
Let, \( \cdot : Z_n^* \times Z_n^* \to Z_n^* \)
by \( a \cdot b = a \times b \mod n \)

\( n = 15, a = 13, b = 7 \)
\( a \cdot b = 1 \)
Defn:
A group is a non empty set $G$ with a binary operator $o$ such that,
(i) $\exists e \in G, \forall a \in G, e \circ a = a$ [Identity]
(ii) $\forall a \in G, \exists b \in G, a \circ b = e$ [Inverse]
(iii) $\forall a, b, c, (a \circ b) \circ c = a \circ (b \circ c)$ [Associatively]

$Z_n^*$ is a group with $\ast$
Identity: 1
Is associative
Inverses: Given a find $b$ such that $(ab \equiv 1) \mod n$
    Iff $ab \equiv kn + 1$
    $ab - kn = 1$