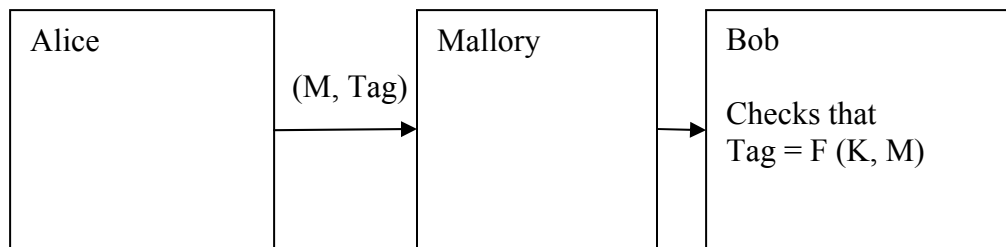


Faisal Islam

Notes for Tuesday, 21 Feb 2006

Symmetric Key Integrity Mechanisms

Message Authentication Code (MAC)



Goal: Mallory can't modify or construct valid messages.

- Replay Attacks
- Garbage Attacks

One time Pad:

$$C = C_0, C_1, \dots$$

$$K = K_0, K_1, \dots$$

$$M = K_0 + M_0, K_1 + M_1, \dots$$

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

$$H(K \oplus \text{opad} \parallel H(K \oplus \text{ipad} \parallel M))$$

ipad = $0x36$ x 64 bytes

opad = $0x5c$ 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

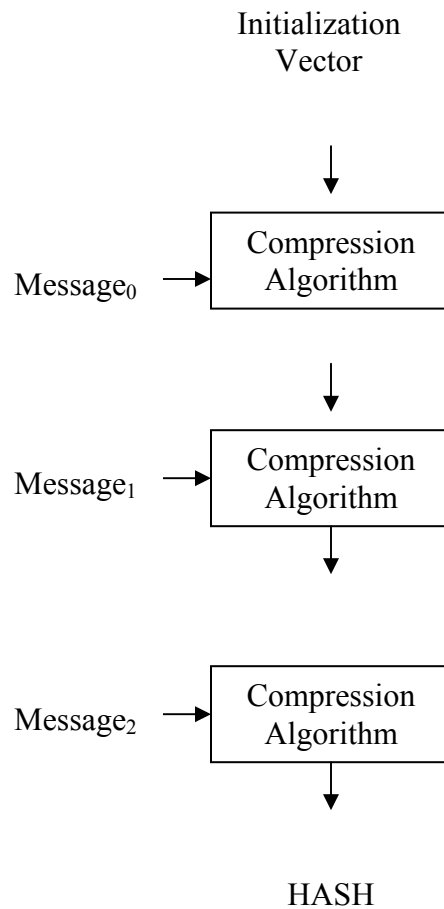
$$\text{MAC}(K, M) = H(K \parallel M)$$

Mallory sees: Tag = $(K \parallel M)$

Then Mallory can compute:

$$H((K \parallel M) \parallel M') = \text{MAC}(K, M \parallel M') \text{ From } H(K \parallel M) \text{ and } M' = \text{Tag}$$

Hash



To send M secretly and unalterably I can:

1. Encrypt – then- MAC

$$C = E_k (M)$$

$$T = MAC_k (C)$$

Send (C, T)

2. MAC – then – Encrypt

$$T = MAC_k (M)$$

Send $E_k (M \parallel T)$

3. MAC and Encrypt

$$T = MAC_k (M)$$

$$C = E_k (M)$$

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)

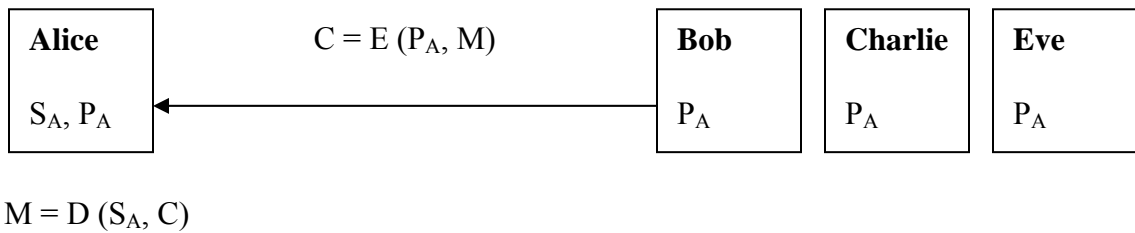
(1) as of yet still works. It has not been broken.

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 nC_2 key $< n^2$

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



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: $Z_n^* = (Z/nZ)^*$
 $= \{r \mid 0 < r < n, \gcd(r, n) = 1\}$

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

$\varphi(pq) = ??$

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



$$\begin{aligned} \varphi(pq) &= pq - (q-1) - (p-1) - 1 \\ &= pq - q - p + 1 \\ &= (p-1)(q-1) \end{aligned}$$

Defn:

Let, $*$: $Z_n^* \times Z_n^* \rightarrow Z_n^*$

by $a*b = a \times b \pmod n$

$n = 15, a = 13, b = 7$

$a*b = 1$

Defn:

A group is a non empty set G with a binary operator o such that,

(i) $\exists e \in G, \forall a \in G, e o a = a$ [Identity]

(ii) $\forall a \in G, \exists b \in G, a o b = e$ [Inverse]

(iii) $\forall a, b, c, (a o b) o c = a o (b o c)$ [Associatively]

Z_n^* is a group with $*$

Identity: 1

Is associative

Inverses: Given a find b such that $(ab \equiv 1) \pmod n$

$$\text{Iff } ab = kn + 1$$

$$ab - kn = 1$$