Message Integrity

Yan Huang
CPA Recap

1. \(k \leftarrow \text{KeyGen}(1^n). \ b \leftarrow \{0,1\}. \ \text{Give} \ \text{Enc}(k, \cdot) \ \text{to} \ \mathcal{A}.
2. \ \mathcal{A} \ \text{chooses as many plaintexts as he wants, and receives the corresponding ciphertexts via} \ \text{Enc}(k, \cdot).
3. \ \mathcal{A} \ \text{picks two plaintexts} \ M_0 \ \text{and} \ M_1. \ (\text{Picking plaintexts for which} \ A \ \text{previously learned ciphertexts is allowed!})
4. \ \mathcal{A} \ \text{receives the ciphertext of} \ M_b, \ \text{and continues to have accesses to} \ \text{Enc}(k, \cdot).
5. \ \mathcal{A} \ \text{outputs} \ b'.

\ \mathcal{A} \ \text{wins if} \ b' = b.
For all efficient adversary $\mathcal{A}$, 
\[ \left| \Pr[ b=b' ] - 0.5 \right| \] is “negligible”. 

Challenger:

\[
k \leftarrow \mathcal{K}, \\
b \leftarrow \{0,1\}
\]
Motivating Example

Is the request indeed coming from Alice?

Elec. Fund Transfer:
From: Alice
To: Bob
Amount: $100
Does Encryption Solve the Problem?

Enc(M)
A Simple Solution using MAC

$(\text{KeyGen}, \text{Mac}, \text{Vrfy})$

tag $\leftarrow \text{Mac}(k, m)$

Vrfy$(k, \text{tag})$
Message Integrity Game

1. $k \leftarrow \text{Gen}(1^n)$.

2. $\mathcal{A}$ is given polynomial time and an oracle access to query $\text{Mac}(k, \cdot)$. Let $t_i = \text{Mac}(k, m_i)$ and $Q = \{(m_1, t_1), \ldots, (m_q, t_q)\}$.

3. $\mathcal{A}$ outputs $(m, t)$.

$\mathcal{A}$ wins the game if $\text{Vrfy}(m, t) = 1$ and $(m, t) \not\in Q$. 
Message Integrity

(Gen, Mac, Vrfy) --- a message authentication code scheme.

Def: (Gen, Mac, Vrfy) is a **Secure Message Authentication Code** if for all “efficient” $\mathcal{A}$:

$$\text{Adv}_{\text{Mac}}[\mathcal{A}] = \Pr[\text{Chal. outputs 1}] \text{ is “negligible.”}$$
Let $F$ be a secure block cipher (i.e., AES).

\[
\text{Mac}(k,m) = F(k,m)
\]

\[
\text{Vrfy}(k,m \parallel t) = 1 \text{ iff } F(k,m) = t
\]
MAC arbitrary number of blocks

Does this work?

Let $F$ be a secure block cipher (i.e., AES).

\[
\text{Mac}(k, m) = F_k(m_1), F_k(m_2), F_k(m_3)
\]
MAC arbitrary number of blocks
Is CBC a good MAC?

\[ F_k \oplus m_1 \]

\[ F_k \oplus m_2 \]

\[ F_k \oplus m_3 \]

\[ t \]
MAC arbitrary number of blocks

Scheme I

\[ |m| \quad m_1 \quad m_2 \quad m_3 \]

\[ F_k \quad F_k \quad F_k \quad F_k \]

\[ t \]
MAC arbitrary number of blocks
Scheme II

\[(k1, k2) \leftarrow \text{Gen}(1^n)\]

No need to know the length of the message in advance.
Warning!

Even harmless-looking modifications to cryptographic constructions can render them insecure!