Lecture 15: Authentication codes

Thomas Johansson

Authentication codes

- *Authenticate* our messages. We need to check that they are indeed sent by the claimed sender and that they have not been modified during transmission.
- Error correcting codes will not help...
- We must introduce secret *keys* that are known to the sender/receiver but unknown to the enemy.

Three types of protection

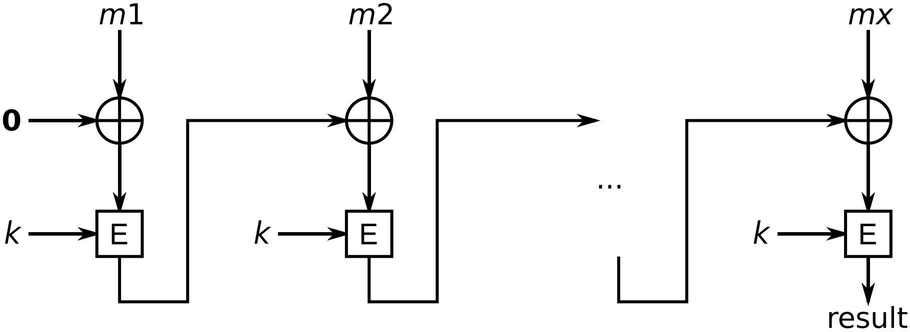
- *unconditionally secure authentication codes*
- *message authentication codes*
- *digital signatures*

MACs

- authentication techniques that use symmetric cryptographic primitives, i.e. block ciphers and hash functions, to provide authentication.
- sender and receiver are here assumed to share a common secret key.
- MACs appear in many standards, and some common modes of operations for block ciphers provide MACs.
- MACs are not secure against an unlimited enemy. But they have other practical advantages, such as being able to authenticate many messages without changing the key.

CBC-MAC

- CBC-MAC is secure for fixed-length messages but not secure for variable-length messages.
- A mistake is to reuse the same key k for CBC encryption and CBC-MAC.

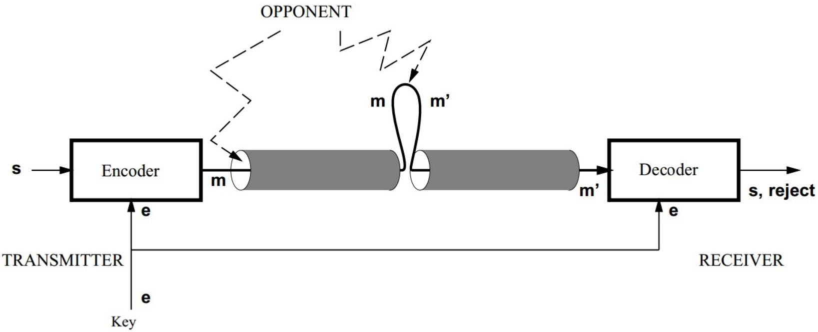


Digital signatures

- an asymmetric solution.
- Several advantages compared to the other two authentication techniques.
- no need to distribute or establish a common secret key.
- *nonrepudiation*. If the receiver has received an authentic message, the sender cannot deny having sent it.
- Drawbacks: Signature schemes rely on the hardness of problems like factoring, work with very large numbers, which make the solutions slow compared to the other techniques.

An unconditionally secure solution

- The transmitted information is a *source message*, s from $\mathcal{S}$.
- mapped into a (channel) *message*, denoted by m and taken from $\mathcal{M}$.
- the secret *key*, e and taken from the set $\mathcal{E}$.



Authentication Codes - the model

- Mapping

$$f : \mathcal{S} \times \mathcal{E} \to \mathcal{M}, \quad (s, e) \mapsto m. \tag{1}$$

  An important property of f is that if $f(s, e) = m$ and $f(s', e) = m$, then $s = s'$ (injective for each $e \in \mathcal{E}$).
- The mapping f together with $\mathcal{S}$, $\mathcal{M}$ and $\mathcal{E}$ define an *authentication code* (A-code).

Authentication Codes - the model

- The receiver must check whether a source message s exists, such that $f(s, e) = m$.
- If such an s exists, m is accepted as authentic (m is called valid).
- Otherwise, m is not authentic and thus rejected.

Attacks

The opponent has two possible attacks at his disposal:

- The *impersonation attack*: Inserting a message m and hoping for it to be accepted as authentic.
- *substitution attack*: opponent observes the message m and replaces this with another message m', $m \neq m'$, hoping for m' to be valid.

Definitions of attack success

the opponent chooses the message that maximizes his chances of success when performing an attack.

- Success in impersonation attack:

$$P_I = \max_m P(m \text{ is valid}) \tag{2}$$

- Success in substitution attack:

$$P_S = \max_{\substack{m,m' \\ m \neq m'}} P(m' \text{ is valid} | m \text{ is valid}). \tag{3}$$

Probability of deception P_D as $P_D = \max(P_I, P_S)$.

Basic bounds

Theorem

For any authentication code,

$$P_I \geq \frac{|\mathcal{S}|}{|\mathcal{M}|}, \quad (4)$$

$$P_S \geq \frac{|\mathcal{S}|-1}{|\mathcal{M}|-1}. \quad (5)$$

$|\mathcal{M}|$ must be chosen much larger than $|\mathcal{S}|$.

(example)

Simmons' bounds

Theorem (Simmons' bounds)

For any authentication code,

$$P_I \geq 2^{-I(M;E)}, \tag{6}$$

$$P_S \geq 2^{-H(E|M)}, \quad \textit{if } |\mathcal{S}| \geq 2. \tag{7}$$

For a good protection, i.e., P_I small, we must give away a lot of information about the key.

The square root bound

Multiply the two bounds together and get

$$P_I P_S \geq 2^{-I(M;E)-H(E|M)} = 2^{-H(E)}. \tag{8}$$

From $H(E) \leq \log |\mathcal{E}|$ we obtain the *square root bound*.

Theorem (Square root bound)

For any authentication code,

$$P_D \geq \frac{1}{\sqrt{|\mathcal{E}|}}. \tag{9}$$

On the square root bound

Theorem

The square root bound can be tight only if

$$|\mathcal{S}| \leq \sqrt{|\mathcal{E}|} + 1.$$

a large source size demands a twice as large key size. This is not very practical.

An A-code for which the map $f : \mathcal{S} \times \mathcal{E} \to \mathcal{M}$ can be written in the form

$$f : \mathcal{S} \times \mathcal{E} \to \mathcal{S} \times \mathcal{Z}, \quad (s, e) \mapsto (s, z), \tag{10}$$

where $s \in \mathcal{S}, z \in \mathcal{Z}$, is called a *systematic* (or Cartesian) A-code. The second part z in the message is called the *tag* (or authenticator) and is taken from the tag alphabet $\mathcal{Z}$.

Systematic authentication codes

Theorem

For any systematic A-code

$$P_S \geq P_I. \tag{11}$$

Constructing authentication codes

Define $\mathcal{E}(m)$ as the set of keys for which a message m is valid,

$$\mathcal{E}(m) = \{e \in \mathcal{E}; \exists s \in \mathcal{S}, f(s,e) = m\}. \tag{12}$$

The probability of success in a substitution attack can be written as

$$P_S = \max_{\substack{m,m' \\ m \neq m'}} \frac{|\mathcal{E}(m) \cap \mathcal{E}(m')|}{|\mathcal{E}(m)|}, \tag{13}$$

provided that the keys are uniformly distributed.

The vector space construction:

Let $|\mathcal{S}| = q^m$, $|\mathcal{Z}| = q^m$, and $|\mathcal{E}| = q^{2m}$. Decompose the keys as $e = (e_1, e_2)$, where $s, z, e_1, e_2 \in \mathbb{F}_{q^m}$. For transmission of source message s, generate a message $m = (s, z)$, where

$$z = e_1 + se_2.$$

Theorem

The above construction provides $P_I = P_S = 1/q^m$. Moreover, it has parameters $|\mathcal{S}| = q^m$, $|\mathcal{Z}| = q^m$, and $|\mathcal{E}| = q^{2m}$.

Polynomial evaluation construction

Let $\mathcal{S} = \{\mathbf{s} = (s_1, \ldots, s_k)\,;\, s_i \in \mathbb{F}_q\}$. Define the source message polynomial to be $s(x) = s_1x + s_2x^2 + \cdots + s_kx^k$. Let $\mathcal{E} = \{e = (e_1, e_2)\,;\, e_1, e_2 \in \mathbb{F}_q\}$ and $\mathcal{Z} = \mathbb{F}_q$. For the transmission of source message $\mathbf{s}$, the transmitter sends $\mathbf{s}$ together with the tag

$$z = e_1 + s(e_2).$$

Theorem

The construction gives systematic A-codes with parameters

$$|\mathcal{S}| = q^k, \quad |\mathcal{E}| = q^2, \quad |\mathcal{Z}| = q, \quad P_I = 1/q, \quad P_S = k/q.$$