

Foundations of Computer Security

Andrea Pintér-Husztí

Contents

- Hash functions, Digital signatures
 - Hash functions
 - Digital Signature Schemes

Hash functions

Cryptographic hash functions

Definíció

By a hash function, we mean a map $H : \{0, 1\}^ \rightarrow \{0, 1\}^n$, $n \in \mathbb{N}$.*

Thus, hash functions map arbitrarily long strings to strings of fixed length.

- e.g.: MD5, SHA-1, SHA-256, SHA-512, SHA-3 (Keccak, 2015)
- verifying data integrity: Cryptographic hash functions can be used to check whether a file has been changed. The hash value of the file is stored separately. The integrity of the file is checked by computing the hash value of the actual file and comparing it with the stored hash value. If the two hash values are the same, then the file is unchanged.
- hash value is called message digest
- **avalanche effect**: If an input is changed slightly (for example, flipping a single bit), the output changes significantly (e.g., half the output bits flip)

Requirements

Hash functions are never injective.

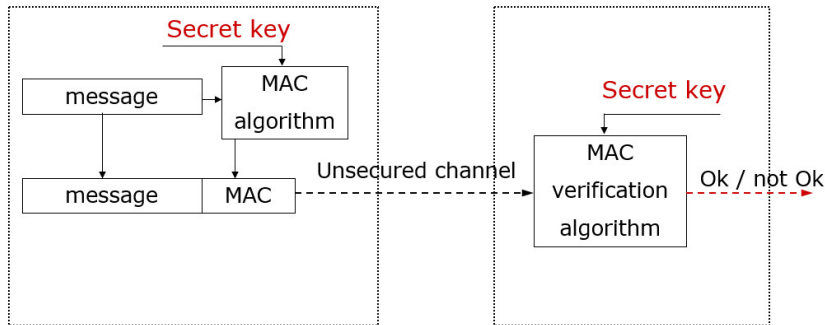
Definíció

A collision of H is a pair $(x, x') \in \{0, 1\}^$ for which $x \neq x'$ and $h(x) = h(x')$.*

Typically, a cryptographic hash function $H : X \rightarrow Y$ has three properties:

- **Preimage resistance:** Given $y \in Y$, it's computationally infeasible to find $x \in X$ such that $H(x) = y$.
- **Second preimage resistance**(weak collision resistant): Given x , it's computationally infeasible to find another x' such that $x \neq x'$ and $H(x) = H(x')$.
- **Collision resistance**(strong collision resistant): It's computationally infeasible to find any two distinct values $x, x' \in X$ such that $H(x) = H(x')$.

Message Authentication Codes



Properties:

- data integrity and
- authenticity of the message

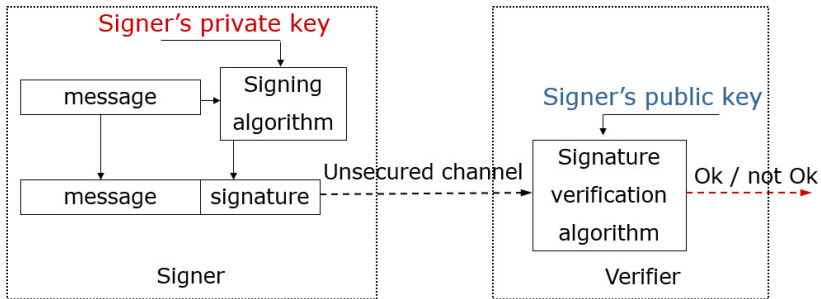
Message Authentication Codes

e.g.: $HMAC_K(m) = H((K' \oplus opad) || H((K' \oplus ipad) || m))$, where H is a cryptographic hash function, m is the message to be authenticated,

K is the secret key, K' is another secret key, derived from the original key K

$||$ denotes concatenation, $\oplus$ denotes exclusive or (XOR)
 $opad$ is the outer padding, $ipad$ is the inner padding.

Digital Signature Schemes



Properties:

- data integrity and
- authenticity of the message
- non-repudiation

Formal definition

Definíció

A signature scheme is a tuple of three algorithms

$DS = (\text{Key}, \text{Sign}, \text{Ver})$ satisfying the following:

- *Key: The key-generation algorithm Key takes as input a security parameter k and outputs a pair of keys (PK, SK) . These are called the public key and the secret key, respectively.*
- *Sign: The signing algorithm Sign takes as input a secret key SK and a message $m \in \{0, 1\}^*$. It outputs signature $s = \text{Sign}_{SK}(m)$.*
- *Ver: The deterministic verification algorithm Ver takes as input a public key PK , a message m , and a signature s . It outputs TRUE meaning valid or FALSE meaning invalid.*

$\mathcal{M}$: message space

$\mathcal{S}$: signature space

Goals of the adversary

- **Total break:** The adversary can compute the signer's secret key and therefore forge any possible signature on any message.
- **Universal forgery:** The adversary can create a valid signature for any given message.
- **Selective forgery:** The adversary succeeds in forging the signature of some message of his choice.
- **Existential forgery:** The adversary succeeds in forging the signature of one message, not necessarily of his choice.

Attack Models

- **Key-only attack:** Adversary knows only the public key.
- **Known message attack:** Adversary knows a list of messages previously signed.
- **Chosen message attack:** The adversary is allowed to ask the signer to sign a number of messages of the adversary's choice.
- **Adaptive chosen message attack:** The adversary is allowed to ask the signer to sign a number of messages of the adversary's choice. The choice of these messages depend on previously obtained signatures.

RSA digital signature scheme

$$DS = (Key, Sign, Ver)$$

- Key:

- 1 Randomly choose two large primes: p, q .
- 2 Calculate RSA modulus: $n = p \cdot q$.
- 3 Calculate Euler totient: $\phi(n) = (p-1)(q-1)$.
- 4 Randomly choose an integer e : $1 < e < \phi(n)$ and $(e, \phi(n)) = 1$.
- 5 Calculate d : $1 < d < \phi(n)$ and $ed \equiv 1 \pmod{\phi(n)}$.

$PK = (n, e)$, $SK = d$ and $\phi(n), p, q$ are secret parameters

$$\mathcal{M} = \mathcal{S} = \mathbb{Z}_n$$

- $Sign_{SK}(m) = m^d \pmod{n} \forall m \in \mathcal{M}$ and for a $SK = d$.
- $Ver_{PK}(m, s) = \begin{cases} TRUE, & s^e \equiv m \pmod{n}; \\ FALSE, & \text{otherwise.} \end{cases}$
 $\forall (m, s) \in \mathcal{M} \times \mathcal{S}$ and for a $PK = (n, e)$.

Attack against textbook RSA signature

- RSA is universally forgable under a chosen-message attack.

Input: arbitrary $m, PK = (n, e)$, s' for a chosen m'

Output: s

Algorithm:

- 1 Randomly choose $r \in \mathcal{M}$
 - 2 Calculate $r' \equiv r^e \pmod{n}$
 - 3 Ask the signature of $m' \equiv m \cdot r' \pmod{n}$, s' is received
 - 4 Calculate $s \equiv s' \cdot r^{-1} \pmod{n}$
- RSA is existentially forgable under key only attack.

Input: $PK = (n, e)$

Output: $(m, s) \in \mathcal{M} \times \mathcal{S}$

Algorithm:

- 1 Randomly choose $s \in \mathcal{S}$
- 2 Calculate $m \equiv s^e \pmod{n}$

RSA-FDH (Full Domain Hash) digital signature scheme

$DS = (\text{Key}, \text{Sign}, \text{Ver})$

- *Key*:

- 1 Randomly choose two large primes: p, q .
- 2 Calculate RSA modulus: $n = p \cdot q$.
- 3 Calculate Euler totient: $\phi(n) = (p-1)(q-1)$.
- 4 Randomly choose an integer e : $1 < e < \phi(n)$ and $(e, \phi(n)) = 1$.
- 5 Calculate d : $1 < d < \phi(n)$ and $ed \equiv 1 \pmod{\phi(n)}$.

$PK = (n, e)$, $SK = d$ and $\phi(n), p, q$ are secret parameters
 $\mathcal{M} = \{0, 1\}^*$, $\mathcal{S} = \mathbb{Z}_n$

- $\text{Sign}_{SK}(m) = H(m)^d \pmod{n} \forall m \in \mathcal{M}$ and for a $SK = d$, where $H: \{0, 1\}^* \rightarrow \mathbb{Z}_n$ a hash function.
- $\text{Ver}_{PK}(m, s) = \begin{cases} \text{TRUE}, & s^e \equiv H(m) \pmod{n}; \\ \text{FALSE}, & \text{otherwise.} \end{cases}$
 $\forall (m, s) \in \mathcal{M} \times \mathcal{S}$ and for a $PK = (n, e)$.