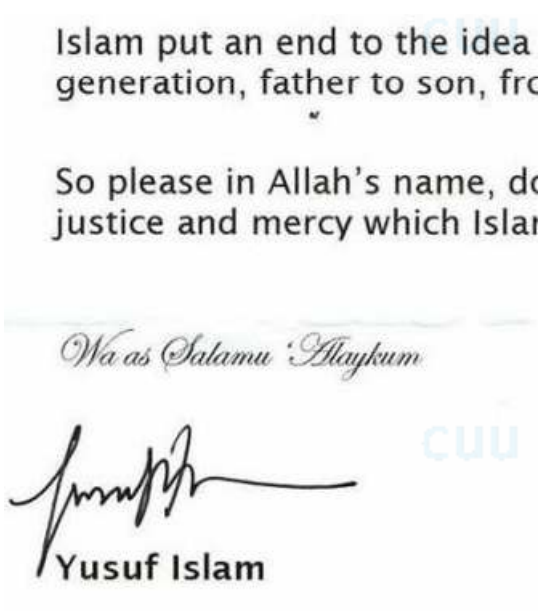
Signature schemes

Introduction

A signature scheme is a method of signing a message stored in electronic form.

Conventional signature



Digital signature

```
Signature:        [c=]
  125831719576202698311415601167093217610124910902417569020303319933409810        [d=]
     779012925150162001006582911504547126084771614879514744953619459824421453
        Signature length:  476
                                  Algorithm:       ECSP-DSA
                Hash function:
SHA-1
 Key:       [HybridEncryption][Bob][EC-prime239v1][1178702474][PIN=1234]                    Message:       CrypTool....CrypTool is a comprehensive educational program about cryptography and cryptanalysis.....This is a text file, shown in order to help you to make your first steps with CrypTool.....1) As a first
```

The signature scheme

Definition 7.1: A *signature scheme* is a five-tuple $(\mathcal{P}, \mathcal{A}, \mathcal{K}, \mathcal{S}, \mathcal{V})$, where the following conditions are satisfied:

1. $\mathcal{P}$ is a finite set of possible *messages*
2. $\mathcal{A}$ is a finite set of possible *signatures*
3. $\mathcal{K}$, the *keyspace*, is a finite set of possible *keys*
4. For each $K \in \mathcal{K}$, there is a *signing algorithm* $\mathbf{sig}_K \in \mathcal{S}$ and a corresponding *verification algorithm* $\mathbf{ver}_K \in \mathcal{V}$. Each $\mathbf{sig}_K : \mathcal{P} \rightarrow \mathcal{A}$ and $\mathbf{ver}_K : \mathcal{P} \times \mathcal{A} \rightarrow \{true, false\}$ are functions such that the following equation is satisfied for every message $x \in \mathcal{P}$ and for every signature $y \in \mathcal{A}$:

$$\mathbf{ver}_K(x, y) = \begin{cases} true & \text{if } y = \mathbf{sig}_K(x) \\ false & \text{if } y \neq \mathbf{sig}_K(x). \end{cases}$$

A pair (x, y) with $x \in \mathcal{P}$ and $y \in \mathcal{A}$ is called a *signed message*.

Example

Cryptosystem 7.1: *RSA Signature Scheme*

Let $n = pq$, where p and q are primes. Let $\mathcal{P} = \mathcal{A} = \mathbb{Z}_n$, and define

$$\mathcal{K} = \{(n, p, q, a, b) : n = pq, p, q \text{ prime}, ab \equiv 1 \pmod{\phi(n)}\}.$$

The values n and b are the public key, and the values p, q, a are the private key.

For $K = (n, p, q, a, b)$, define

$$\mathbf{sig}_K(x) = x^a \bmod n$$

and

$$\mathbf{ver}_K(x, y) = \text{true} \Leftrightarrow x \equiv y^b \pmod{n}$$

$(x, y \in \mathbb{Z}_n)$.

Types and goals of attacks

Types of attacks

- Key-only
- Known message
- Chosen message

Goals of attacks

- Total break
- Selective forgery
- Existential forgery

An example of existential attack

Ex: Textbook RSA signature

$\mathbf{sig}_K(x) = x^a \bmod n$ $\quad\quad$ $\mathbf{ver}_K(x, y) = \text{true} \Leftrightarrow x \equiv y^b \pmod{n}$

C1: Choose any signature y, then compute $x = y^b \bmod n$.

C2:

$y_1 = \mathbf{sig}_K(x_1)$ and $y_2 = \mathbf{sig}_K(x_2)$ are any two messages previously signed

$$\mathbf{ver}_K(x_1 x_2 \bmod n, y_1 y_2 \bmod n) = \text{true},$$

→ Choose $y_2 = y/y_1$.

→ Need to be hashed.