Digital signature

2021-05-11

1 Digital signature

A *digital signature* is a piece of information (i.e. a sequence of bits) attached to a message which provides the three following properties:

- **Message authentication** - the receiver of the message can verify the origin of the message
- **Message integrity** - if the message gets modified the receiver is able to detect it
- **Non repudiation** - the signer cannot later claim that he or she didn't sign it[1].

1.1 Digital signature scheme

A digital signature scheme consists of the following three probabilistic algorithms:

- `Gen(n)` - generate a simmetric key pair `(pk, sk)` of `n` bits, where `n` is a security parameter.
- $\texttt{Sign}_{\texttt{sk}}\texttt{(m)}$ - generate a digital signature σ from the *secret key* `sk` and the *message* `m`.
- $\texttt{Vrfy}_{\texttt{pk}}\texttt{(m,}\sigma\texttt{)}$ - input `pk`, `m` and σ, output 1 if the signature is valid, 0 if the signature is invalid.

It's important to notice that while the key `pk` is public and available to everyone, the secret key `sk` must be kept, indeed, secret.

1.1.1 Security of the digital signature scheme

A digital signature scheme `(Gen, Sign, Vrfy)` is *secure* if an adversary knowing `pk` and other valid signatures $(m_1, \sigma_1), (m_2, \sigma_2), \ldots$ is not able to produce a new message m and a valid signature σ for it.

[1] Actually, to gain non-repudiation we also need a public key certificate, but we won't explore technical details in this paper, and we'll suppose that the key used to sign is unequivocally linked to the signer.

Exercise 10.2.1 What is the difference between a MAC and a digital signature?

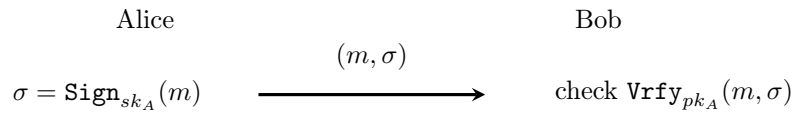
- MAC guarantees only authentication and integrity, while digital signature (in principle) also guarantees non-repudiation.
- A digital signature is created with a key pair `(pk, sk)`, while the MAC is based on a secret key, shared between the sender and the receiver.

1.2 Digital signature protocol

Let's consider a sender and a receiver (Alice and Bob).

Alice wants to send a message m to Bob by using her secret key $\mathtt{sk_A}$.

Bob knows Alice's public key (which is indeed public) and is able to verify the signature.



Properties:

- The signature is *authentic* - Bob knows that Alice signed the message.
- The signature is *unforgeable* - only Alice knows her private key.
- The signature is *not reusable* for any other message - because it's a function of the message.
- Any *alteration* of the message would invalid the signature - it won't be possible to verify the signature with Alice's public key anymore.
- The signature cannot be *repudiated* - Alice cannot claim not having signed the message because she was the only one knowing her private key.

1.3 Digital signature and timestamp

Digital signatures should also include timestamps (attach a timestamp to the message and sign the whole document).

Let's consider the following *example*, taken from the Bruce Schneier's book "Applied Cryptography":

> Alice sends Bob a signed digital check for $100. Bob takes the check to the bank, which verifies the signature and moves the money from one account to another. The following week, Bob takes the same check to the bank, which again verifies the signature and moves the money from one account to another. And so on.

But if date and time of signature are attached to the message, then the bank could store this timestamp into a database, and when Bob takes the check for the second time, the bank checks the timestamp against its database.

1.4 RSA digital signature

1.4.1 Naive RSA-signature

Alice's public key $\mathtt{pk}_A = (n, e)$ and secret key is $\mathtt{sk}_A = d$.

Exercise 10.2.2 Show that the above signature is not secure. Hint: choose any $\sigma \in \mathbb{Z}_n$ and consider $m = \sigma^e (mod\ n)$