Public Key Cryptography

Federico Casu

December 21, 2023

Public Key Cryptography: a brief introduction

As we are becoming familiar with it, let's study how public key cryptography is used to protect communications. Figure 1 illustrates the fundamentals of a public key-based communication system:

- Alice, who wants to send a confidential message to Bob, knows Bob's public key $\mathsf{K}^{\mathsf{B}}_{\mathsf{pub}}$. To encrypt the message x, Alice executes the encryption algorithm $\mathsf{E}(\cdot)$, taking as input the plaintext x and Bob's public key $\mathsf{K}^{\mathsf{B}}_{\mathsf{pub}}$.
- Bob, who wants to read the incoming message (and correctly decrypt y), executes the decryption algorithm $\mathsf{E}^{-1}(\cdot)$, taking as input the ciphertext y and Bob's private key $\mathsf{K}^{\mathsf{B}}_{\mathsf{priv}}$.

Let's give a formal definition of a public key encryption scheme.

> A public key encryption scheme is composed of a triple of algorithms, $\langle \mathsf{E}, \mathsf{D}, \mathsf{G} \rangle$, such that they fulfill the following properties:
>
> G is a randomized algorithm that outputs a pair of keys, namely $\langle \mathsf{K}_{\mathsf{pub}}, \mathsf{K}_{\mathsf{priv}} \rangle$.
>
> $$\mathsf{G} \ : \ \{0,1\}^{\mathsf{k}} \rightarrow \mathsf{K} = \{0,1\}^{\mathsf{n}} \times \{0,1\}^{\mathsf{n}}$$
>
> E is a randomized algorithm that, given inputs of a plaintext $\mathsf{x} \in \mathsf{X}$ and a public key $\mathsf{K}_{\mathsf{pub}}$, outputs a ciphertext $\mathsf{y} \in \mathsf{Y}$.
>
> $$\mathsf{E} \ : \ \mathsf{K} \times \mathsf{X} \rightarrow \mathsf{Y}$$
>
> D is a **deterministic** algorithm that, given inputs of a ciphertext $\mathsf{y} \in \mathsf{Y}$ and a private key $\mathsf{K}_{\mathsf{priv}}$, outputs a plaintext $\mathsf{x} \in \mathsf{X}$.
>
> $$\mathsf{D} \ : \ \mathsf{K} \times \mathsf{Y} \rightarrow \mathsf{X}$$
>
> The encryption scheme fulfills the **consistency property**, *i.e.*
>
> $$\forall \ \langle \mathsf{K}_{\mathsf{pub}}, \mathsf{K}_{\mathsf{priv}} \rangle, \ \forall \ \mathsf{x} \in \mathsf{X} \rightarrow \mathsf{E}^{-1}(\mathsf{K}_{\mathsf{priv}}, \mathsf{E}(\mathsf{K}_{\mathsf{pub}}, \mathsf{x})) = \mathsf{x}$$

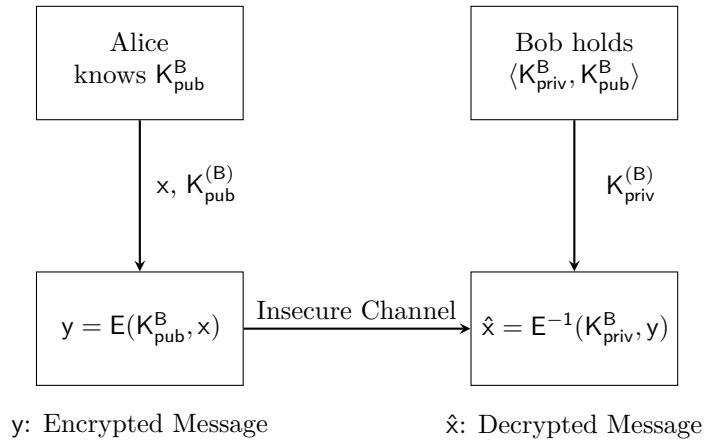

Figure 1: Public Key Cryptography - Simple communication scenario.

Being an encryption scheme, the previously defined public key scheme must provide certain security properties. We would like to give you an informal definition of the security properties of a public key encryption scheme:

1. Given any ciphertext y and the public key used to encrypt it, K_{pub}, it must be infeasible to obtain the plaintext x such that $\mathsf{y} = \mathsf{E}(\mathsf{K}_{\text{pub}}, \mathsf{x})$.
2. Given any public key, it must be infeasible to obtain the corresponding private key.

Such properties rely on some algebraic constructs. In particular, public key cryptography exploits a certain type of mathematical function called **one-way functions**.

The *one-wayness* property states that a function f is said to be one-way if:

- f is easy to compute
- f^{-1} is hard to compute

In what way one-way functions are related to public key cryptography? Let's make an example:

- The RSA cryptosystem exploits the integer factorization as the underlying one-way function: multiplying two primes is easy but factoring the resulting product is computationally infeasible.