Public Key Cryptography

Federico Casu

December 27, 2023

1 Introduction

As we are becoming familiar with it, let's delve into the application of public key cryptography in securing communications. Figure 1 illustrates the fundamentals of a public key-based communication system:

1. 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 $\mathsf{K}^{\mathsf{B}}_{\mathsf{pub}}$.
2. Bob, who wants to read the incoming message, 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 establish a formal definition of a public key encryption scheme: a public key encryption scheme is a triple of algorithms, $\langle \mathsf{E}, \mathsf{D}, \mathsf{G} \rangle$, such that they fulfill the following properties:

1. G is a randomized algorithm that outputs a pair of keys, namely $\langle \mathsf{K}_{\mathsf{pub}}, \mathsf{K}_{\mathsf{priv}} \rangle$.
$$\mathsf{G} \ : \ \{0,1\}^{\mathsf{k}} \to \mathsf{K} = \{0,1\}^{\mathsf{n}} \times \{0,1\}^{\mathsf{n}}$$
2. E is a randomized algorithm that, given inputs of a plaintext $\mathsf{x} \in \mathsf{M}$ and a public key $\mathsf{K}_{\mathsf{pub}}$, outputs a ciphertext $\mathsf{y} \in \mathsf{C}$.
$$\mathsf{E} \ : \ \mathsf{K} \times \mathsf{M} \to \mathsf{C}$$
3. D is a **deterministic** algorithm that, given inputs of a ciphertext $\mathsf{y} \in \mathsf{C}$ and a private key $\mathsf{K}_{\mathsf{priv}}$, outputs a plaintext $\mathsf{x} \in \mathsf{M}$.
$$\mathsf{D} \ : \ \mathsf{K} \times \mathsf{C} \to \mathsf{M}$$
4. The encryption scheme fulfills the **consistency property**, *i.e.*
$$\forall \ \langle \mathsf{K}_{\mathsf{pub}}, \mathsf{K}_{\mathsf{priv}} \rangle, \ \forall \ \mathsf{x} \in \mathsf{M} \to \mathsf{E}^{-1}(\mathsf{K}_{\mathsf{priv}}, \mathsf{E}(\mathsf{K}_{\mathsf{pub}}, \mathsf{x})) = \mathsf{x}$$

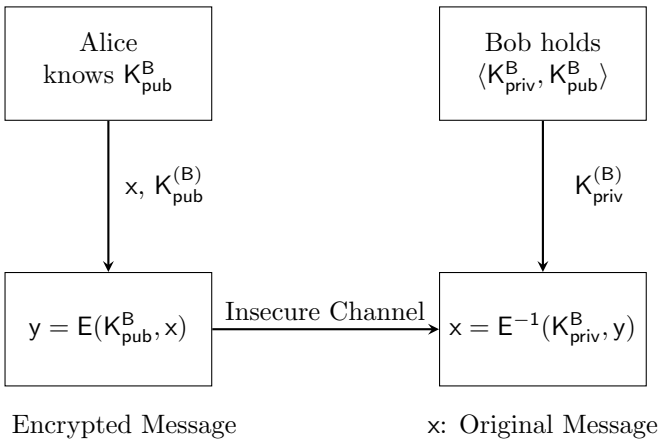

Figure 1: Public Key Cryptography - Simple communication scenario.

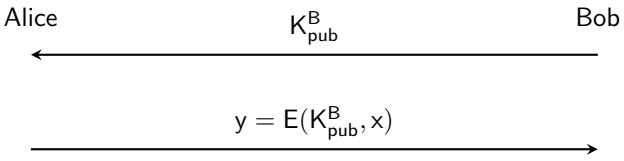

Figure 2: Simple Public Key Encryption (PKE) scheme.

Being an encryption scheme means provide some 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 $y = E(K_{pub}, x)$.
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 functions called **one-way** functions. The *one-wayness* property states that a function f is said to be one-way if:

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

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

Example 1. 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. RSA key generation algorithm security rely on the integer factorization problem.

Public key cryptography is not *perfect*. Let's prove it:

1. Let's consider that an attacker managed to obtain a ciphertext y.
2. Let's consider a plaintext $\hat{x} \in M$ such that $0 < P(X = x) < 1$. Knowing the receiver's public key (by definition, as the name suggests, is public), we encrypt the choosen plaintext $\hat{x}$ with the public key, *i.e.*, $\hat{y} = E(K_{pub}, \hat{x})$. Now we are in front of two scenarios:
   (a) $y = \hat{y} \rightarrow x = \hat{x} \rightarrow P(X = \hat{x} \mid Y = y) = 1 \neq P(X = x)$
   (b) $y \neq \hat{y} \rightarrow x \neq \hat{x} \rightarrow P(X = \hat{x} \mid Y = y) = 0 \neq P(X = x)$

A public key encryption scheme is *not* perfect because it's always possible to find a plaintext whose a-posteriori probability is either 0 or 1, which is different from $P(X = x)$.

Let's explore some real-world applications of public key cryptography:

1. The first application is in digital communications. The primary distinction between a symmetric key encryption scheme and a public key encryption scheme is that the former requires an initial phase during which the communicating parties securely agree on the key used for encryption. In a public key encryption scheme, there is no need to securely agree on a session key. The encryption phase utilizes the public key, and the decryption phase uses the private key. Importantly, even if the public key is publicly known, the private key does not need to be transmitted over an insecure channel: only the owner can decrypt any messagge encrypted with the corresponding public key.
2. Moving forward, we will delve into the study of digital signatures. The asymmetric nature of the encryption scheme makes public key cryptography more suitable for digital signature schemes compared to symmetric ones.

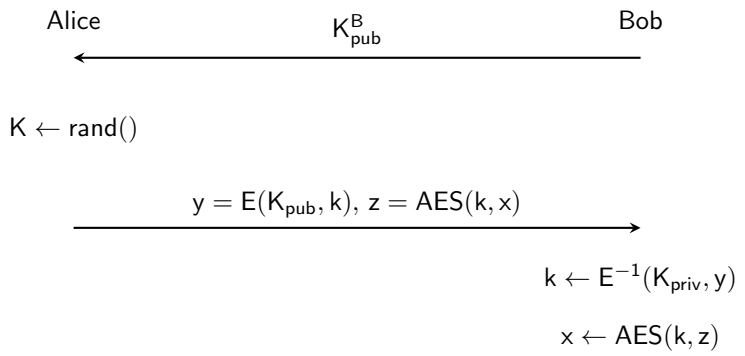

Figure 3: Digital Envelope communication protocol.

Algorithm Family	Cryptosystem	Security Level			
		80	128	192	256
Integer Factorization	RSA	1024 bit	3072 bit	7680 bit	15360 bit
Discrete Logarithm	DH, DSA, ElGamal	1024 bit	3072 bit	7680 bit	15360 bit
Elliptic curves	ECDH, ECDSA	160 bit	256 bit	384 bit	512 bit
Symmetric key	AES, 3DES	80 bit	128 bit	192 bit	256 bit

Figure 4: Security level of the most used encryption schemes.

Public key encryption schemes have a big problem: public key encryption is 2-3 orders of magnitude slower than symmetric key encryption! A very simple communication scheme based on public key cryptography (Figure 2) cannot not be used in practice. A solution to this problem is given by the digital envelope: public key cryptography is used only to encrypt the symmetric key (Figure 3).

What about the *security level* of a public key encryption scheme? The formal definition of security level is the following:

Definition 1. An encryption scheme has security level of n bits if the best known algorithm to break it requires 2^n steps.

The relationships between the key length and the security level in a symmetric encryption scheme is straightforward: if the key is n bits long then the encryption scheme has security level of n bits. For public key encryption schemes is a bit different: there is no linear relation between key lenght and security level: as a rule of thumb, the computational complexity grows roughly with the cube bit length.

1.1 Key Authentication: MITM Attacks

With respect to a passive attacker, any public key encryption scheme is secure. If an attacker intercepts any ciphertext, they must solve the underlying mathematical problem to be able to decrypt the intercepted cyphertext. Therefore, if the encryption scheme is well-designed (meaning that the encryption scheme exploits a good *one-way* function), the attacker will not be able to decrypt or obtain the private key in a reasonable amount of time.

Now, considering an active attacker, let's explore the following scenario (Figure 5):

1. Oscar is a "bad guy" who wishes to secretly read the messages that Alice and Bob are going to exchange.

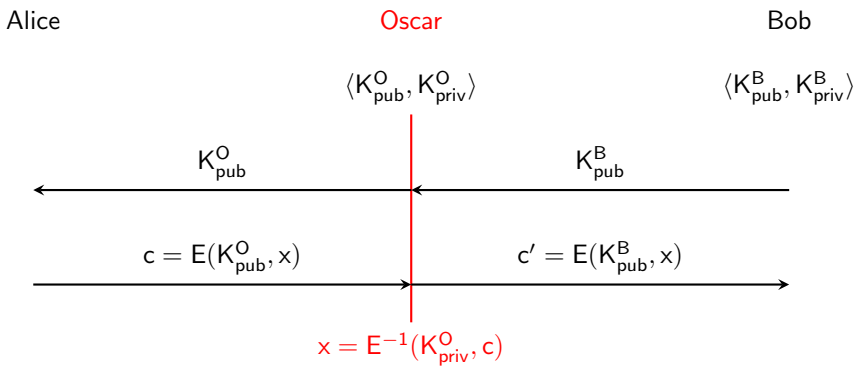

Figure 5: Man In The Middle (MITM) attack.

2. Bob needs to let Alice know his current public key: he simply sends his public key through an insecure channel. Bob doesn't worry about the public key and he thinks that Alice correctly receives his public key.

3. Oscar manages to intercept Bob's public key. He's a smart guy and he thinks to impersonate Bob by sending to Alice a freshly generated public key K^O_{pub}.

4. Alice receives Oscar's public key but she thinks that it was Bob who sent the message. So she encrypts the confidential message with the received public key and sends it through the insecure channel.

5. Oscar, once again, intercepts the encrypted message. Since the latter was encrypted using his public key, he is able to correctly decrypt Alice's message, read x and send $c' = E(K^B_{pub}, x)$ to Bob.

6. Bob receives Oscar's messagge thinking that it was sent by Alice: both Alice and Bob are scammed by Oscar and no one knows it!

How can we prevent a *man-in-the-middle* attack? Let's study a possible solution:

Example 2. Instead of sending their own public key, each user registers their public key with a *trusted read-only repository*. Whenever Alice wants to send a confidential message to Bob, she queries the trusted repository, asking for Bob's public key.

Note that a trusted repository does not secure a public encryption scheme from MITM attacks: an adversary could intercept the query for a public key and craft a fake response substituting the legit public key with any key they want. Later on, we will study how public key encryption schemes exploit digital signatures to mitigate MITM attacks.

1.2 Encryption Randomization

There are some scenarios that require to be studied because a plain public key encryption scheme is vulnerable. Let's examine it:

1. Consider an auction. Alice, a bidder participating in Bob's auction, sends her bid to Bob by encrypting it with Bob's public key.

2. Oscar, a bad guy, wishes to win the auction by spending the least amount of money possible. He does this by sending a bid with an amount equal to the maximum bid from honest bidders plus 1 dollar. Since Oscar knows the market value of the goods being auctioned, he knows that the bids can be represented with 10 bits, meaning each bid is 10 bits long.

3. Oscar manages to obtain each bid sent to Bob. Since Oscar knows Bob's public key (if Oscar couldn't obtain Bob's public key, then the latter would be a private key!), he performs the attack described in Algorithm 1.

4. The attack complexity is very low: $O(2^{10})$. Oscar can brute-force each intercepted message (perhaps in parallel) and obtain the highest bid that was sent to Bob. Once he has done that, he can device all the participants by sending to Bob $y = E(K^B_{pub}, \max + 1)$.

Algorithm 1 Small plaintext attack: algorithm

```
for i ← 0 to 2^10 do
    y' ← encrypt(K_pub, i)
    if y = y' then return i
    end if
end for
```

Is there a way to prevent Bob and the bidders from being scammed? Yes:

1. Each bidder generates a random number $g \in \{0,1\}^r$.
2. Now, instead of encrypting only the bid, the message to be encrypted is the following:

$$x' = x \mid g$$

3. Oscar, to obtain the bid x from the encrypted message, needs to executes Algorithm 2.
4. The attack's complexity gets multiplied by 2^r!

Algorithm 2 Small plaintext attack: algorithm

```
for i ← 0 to 2^10 do
    for j ← 0 to 2^r do
        y' ← encrypt(K_pub, {i,j})
        if y = y' then return i
        end if
    end for
end for
```

2 RSA Cryptosystem

RSA cryptosystem was invented by a group of researchers (R. L. Rivest, A. Shamir and L. Adleman) working at MIT Laboratory for Computer Science. The encryption scheme was first presented in a paper called "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems" (February 1978). Let's delve into the fundamentals of the RSA encryption scheme.

Key Generation Algorithm Formally, the RSA key generation algorithm is composed by 5 steps:

Algorithm 3 RSA Key Generation Algorithm

1: Choose two large prime numbers, namely p and q.
2: Compute the quantity $\mathsf{n} = \mathsf{p} \cdot \mathsf{q}$ called *modulus*.
3: Compute the quantity $\phi = (\mathsf{p} - 1)(\mathsf{q} - 1)$.
4: Choose e such that $1 < \mathsf{e} < \phi$ and $\mathsf{gcd}(\mathsf{e}, \phi) = 1$.
5: Choose d such that $1 < \mathsf{d} < \phi$ and $\mathsf{e} \cdot \mathsf{d} \equiv 1 \pmod{\phi}$.

The key generation algorithm outputs two quantities:

$$\text{public key} : \langle \mathsf{e}, \mathsf{n} \rangle$$
$$\text{private key} : \langle \mathsf{d}, \mathsf{n} \rangle$$

Encryption and Decryption Algorithm

$$\text{Encryption} : \mathsf{y} = \mathsf{x}^{\mathsf{e}} \mod \mathsf{n}$$
$$\text{Decryption} : \mathsf{x} = \mathsf{y}^{\mathsf{d}} \mod \mathsf{n}$$

Now we need to discuss the performance of the key generation algorithm. In particular, generating a pair of keys $\langle \mathsf{K}_{\mathsf{pub}}, \mathsf{K}_{\mathsf{priv}} \rangle$ involves some operations:

1. Find two large prime numbers. Obviously, each prime needs to be randomly generated (otherwise an attacker could guess the prime with a very high probability).
2. Test whether or not the randomly generated number is truly a prime number.
3. Find a public and a private exponent which fulfill the required properties: $\mathsf{gcd}(\mathsf{e}, \phi) = 1$ and $\mathsf{e} \cdot \mathsf{d} \equiv 1 \pmod{\phi}$.

So the prime generation algorithm could be pseudo coded as follows:

Algorithm 4 Prime Generation Algorithm

```
repeat
    p ← random()
until is_prime(p) == False
```

To establish the complexity of Algorithm 4 we need to answer the following questions:

1. How many iterations do we need to execute? In other words, how likely is to find a prime $\mathsf{p} < \mathsf{x}$?
2. How difficult is it to generate a random number?
3. How difficult is it to test whether a number is prime or not?

Let's answer the previous questions:

Fact 1. Let's call $\pi(\mathsf{x})$ the number of primes which are $\leq \mathsf{x}$. If x is sufficiently big, then $\pi(\mathsf{x})$ could be approximated to $\pi(\mathsf{x}) = \frac{\mathsf{x}}{\ln(\mathsf{x})}$.

If we test only odd integers, meaning that we test half the numbers $\in [1, x]$, the probability to find a prime $p \in [1, x]$ is:

$$P(p \text{ is prime}) = \frac{\pi(x)}{\text{number of odds} \in [2, x]} = \frac{x/\ln(x)}{x/2} = \frac{2}{\ln(x)} = O\left(\frac{1}{\ln(x)}\right)$$

So, the expected number of trials needed to find a prime is $O(\ln(x))$, which is quite good (and easy). What about the complexity of a primality test? Primality tests are computationally much easier than factorization. In particular, practical implementations of primality tests are *probabilistic*: at the question "is $p*$ prime?" they answer

1. $p*$ is composed which is always a true statement;
2. $p*$ is prime, which is only true with a high probability.

Now we need to discuss how difficult is to find a pair of keys such that fulfill the properties:

$$\begin{aligned} \gcd(e, \phi) &= 1 \\ e \cdot d &\equiv 1 \pmod{\phi} \end{aligned}$$