Public Key Cryptosystem

Math 4176

§5.1. Symmetric Key Cryptosystem

In this first course of Cryptography, we studied so far several cryptosystems, where a secret key k is selected to derive both encryption rule e_k and decryption rule d_k.

§5.1. Symmetric Key Cryptosystem

In this first course of Cryptography, we studied so far several cryptosystems, where a secret key k is selected to derive both encryption rule e_k and decryption rule d_k.

Recall that the decryption rule d_k can be easily derived from e_k in all the cryptosystems we have studied until now, because the same key is used for both e_k and d_k.

§5.1. Symmetric Key Cryptosystem

In this first course of Cryptography, we studied so far several cryptosystems, where a secret key k is selected to derive both encryption rule e_k and decryption rule d_k.

Recall that the decryption rule d_k can be easily derived from e_k in all the cryptosystems we have studied until now, because the same key is used for both e_k and d_k.

A Cryptosystem of this type is known as a private key cryptosystem or symmetric cryptosystem.

§5.1. Symmetric Key Cryptosystem

In this first course of Cryptography, we studied so far several cryptosystems, where a secret key k is selected to derive both encryption rule e_k and decryption rule d_k.

Recall that the decryption rule d_k can be easily derived from e_k in all the cryptosystems we have studied until now, because the same key is used for both e_k and d_k.

A Cryptosystem of this type is known as a private key cryptosystem or symmetric cryptosystem.

Drawback: When Bob receives an encrypted message from Alice, he also needs to know the secret key used by Alice.

§5.1. Symmetric Key Cryptosystem

In this first course of Cryptography, we studied so far several cryptosystems, where a secret key k is selected to derive both encryption rule e_k and decryption rule d_k.

Recall that the decryption rule d_k can be easily derived from e_k in all the cryptosystems we have studied until now, because the same key is used for both e_k and d_k.

A Cryptosystem of this type is known as a private key cryptosystem or symmetric cryptosystem.

Drawback: When Bob receives an encrypted message from Alice, he also needs to know the secret key used by Alice.

There is a possibility that Oscar (a third party) may intercept the key when Alice tries to send it to Bob through any channel or at least able to guess the encryption rule even if Alice used reasonably secured channel.

§5.1. Public Key Cryptosystem

Alternate option is to use a system where it is computationally infeasible to derive the decryption rule even if the encryption rule is known.

§5.1. Public Key Cryptosystem

Alternate option is to use a system where it is computationally infeasible to derive the decryption rule even if the encryption rule is known.

Such a system is known as a publice key cryptosystem or an asymmetric cryptosystem.

§5.1. Public Key Cryptosystem

Alternate option is to use a system where it is computationally infeasible to derive the decryption rule even if the encryption rule is known.

Such a system is known as a publice key cryptosystem or an asymmetric cryptosystem.

An asymmetric cryptosystem uses a pair of keys, one is a public key which is used for encryption and another one is a private key that is needed for decryption.

§5.1. Public Key Cryptosystem

Alternate option is to use a system where it is computationally infeasible to derive the decryption rule even if the encryption rule is known.

Such a system is known as a publice key cryptosystem or an asymmetric cryptosystem.

An asymmetric cryptosystem uses a pair of keys, one is a public key which is used for encryption and another one is a private key that is needed for decryption.

For example, Bob provides a (public) key to Alice through an unsecured channel to encrypt a message. Though Alice uses the public encryption rule, it is very difficult for Oscar to decrypt the message sent by Alice. But Bob knows a 'trapdoor' (called private key) which he can use to decrypt the message.

§5.1. Public Key Cryptosystem

Example: Bob publicly asks Alice to use the encryption rule

$$e(x) = x^{85} \mod 851$$

§5.1. Public Key Cryptosystem

Example: Bob publicly asks Alice to use the encryption rule

$$e(x) = x^{85} \mod 851$$

- So the public key for the encryption is the pair of numbers $(851, 85)$.

§5.1. Public Key Cryptosystem

Example: Bob publicly asks Alice to use the encryption rule

$$e(x) = x^{85} \mod 851$$

- So the public key for the encryption is the pair of numbers $(851, 85)$.
- Suppose Alice sends the encrypted message '395'.

§5.1. Public Key Cryptosystem

Example: Bob publicly asks Alice to use the encryption rule

$$e(x) = x^{85} \mod 851$$

- So the public key for the encryption is the pair of numbers $(851, 85)$.
- Suppose Alice sends the encrypted message '395'.
- Suppose Oscar intercepts this message. How can he recover the plaintext x by knowing the encryption rule?

§5.1. Public Key Cryptosystem

Example: Bob publicly asks Alice to use the encryption rule

$$e(x) = x^{85} \mod 851$$

- So the public key for the encryption is the pair of numbers $(851, 85)$.
- Suppose Alice sends the encrypted message '395'.
- Suppose Oscar intercepts this message. How can he recover the plaintext x by knowing the encryption rule?
- In other words, what is the solution for $395 = x^{85} \mod 851$?

§5.1. Public Key Cryptosystem

Example: Bob publicly asks Alice to use the encryption rule

$$e(x) = x^{85} \mod 851$$

- So the public key for the encryption is the pair of numbers $(851, 85)$.
- Suppose Alice sends the encrypted message '395'.
- Suppose Oscar intercepts this message. How can he recover the plaintext x by knowing the encryption rule?
- In other words, what is the solution for $395 = x^{85} \mod 851$?
- Of course, 851 is not a very large number. Though it is not obvious, Oscar may find the solution by checking all the numbers $0 \leq x \leq 850$ by using a powerful enough computer.

§5.1. Public Key Cryptosystem

Example: Bob publicly asks Alice to use the encryption rule

$$e(x) = x^{85} \mod 851$$

- So the public key for the encryption is the pair of numbers $(851, 85)$.
- Suppose Alice sends the encrypted message '395'.
- Suppose Oscar intercepts this message. How can he recover the plaintext x by knowing the encryption rule?
- In other words, what is the solution for $395 = x^{85} \mod 851$?
- Of course, 851 is not a very large number. Though it is not obvious, Oscar may find the solution by checking all the numbers $0 \leq x \leq 850$ by using a powerful enough computer.
- How about if 851 is replaced with very large number?

§5.1. Public Key Cryptosystem

- Recall that the encryption rule should be an injective function. Is the above encryption injective?

§5.1. Public Key Cryptosystem

- Recall that the encryption rule should be an injective function. Is the above encryption injective?
- Bob needs to have the knowledge of a 'trapdoor'(private key) that decrypts the message lot faster.

§5.1. Public Key Cryptosystem

- Recall that the encryption rule should be an injective function. Is the above encryption injective?
- Bob needs to have the knowledge of a 'trapdoor'(private key) that decrypts the message lot faster.
- Bob's private key is $(851, 205)$, that is, the decryption function is

$$d(y) = y^{205} \mod 851$$

§5.1. Public Key Cryptosystem

- Recall that the encryption rule should be an injective function. Is the above encryption injective?
- Bob needs to have the knowledge of a 'trapdoor'(private key) that decrypts the message lot faster.
- Bob's private key is $(851, 205)$, that is, the decryption function is

$$d(y) = y^{205} \mod 851$$

- So $d(395) = 395^{205} \mod 851 = 583$.

§5.1. Public Key Cryptosystem

- Recall that the encryption rule should be an injective function. Is the above encryption injective?
- Bob needs to have the knowledge of a 'trapdoor'(private key) that decrypts the message lot faster.
- Bob's private key is $(851, 205)$, that is, the decryption function is

$$d(y) = y^{205} \mod 851$$

- So $d(395) = 395^{205} \mod 851 = 583$.
- One can check that $583^{85} \mod 851 = 395$ and so 583 is the correct plaintext! (see slide 11 in 5.3)

§5.1. Public Key Cryptosystem

- Recall that the encryption rule should be an injective function. Is the above encryption injective?
- Bob needs to have the knowledge of a 'trapdoor'(private key) that decrypts the message lot faster.
- Bob's private key is $(851, 205)$, that is, the decryption function is

$$d(y) = y^{205} \mod 851$$

- So $d(395) = 395^{205} \mod 851 = 583$.
- One can check that $583^{85} \mod 851 = 395$ and so 583 is the correct plaintext! (see slide 11 in 5.3)
- Our calculators may not handle such high exponents, but they can be computed by square-and-multiply algorithm that we will discuss later.

§5.1. Public Key Cryptosystem

Question: What is the extra information that helped Bob to come up with the private key $(851, 205)$?

§5.1. Public Key Cryptosystem

Question: What is the extra information that helped Bob to come up with the private key $(851, 205)$?

- The encryption function given above is an example of RSA Cryptosystem (invented in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman).

§5.1. Public Key Cryptosystem

Question: What is the extra information that helped Bob to come up with the private key $(851, 205)$?

- The encryption function given above is an example of RSA Cryptosystem (invented in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman).
- They were motived by the private-public key cryptosystem concept introduced by Whitfield Diffie and Martin Hellman an year earlier in 1976.

§5.1. Public Key Cryptosystem

Question: What is the extra information that helped Bob to come up with the private key $(851, 205)$?

- The encryption function given above is an example of RSA Cryptosystem (invented in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman).
- They were motived by the private-public key cryptosystem concept introduced by Whitfield Diffie and Martin Hellman an year earlier in 1976.
- It should be noted that Clifford Cocks, an English mathematician, described a similar system in 1973. However, it was kept classified by a British intelligence agency until 1997.

§5.1. Public Key Cryptosystem

Question: What is the extra information that helped Bob to come up with the private key $(851, 205)$?

- The encryption function given above is an example of RSA Cryptosystem (invented in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman).
- They were motived by the private-public key cryptosystem concept introduced by Whitfield Diffie and Martin Hellman an year earlier in 1976.
- It should be noted that Clifford Cocks, an English mathematician, described a similar system in 1973. However, it was kept classified by a British intelligence agency until 1997.
- We will now study in a little bit more detail the RSA cryptography.