An introduction to

Cryptography

Girindro Pringgo Digdo

Whoami

- Seven years in Information Security
- Lecturer
- Author

Agenda

- What is Cryptography
- Encryption
- Private and Publick Key

Do you understand what is it?

UgHmWnqes6Fum7Ie8uTKpJl06ohCwOKm
GBhhu3AhMTAh/V5DybghMTMh5mJes1JB
mLx2+MHYYFchMCFs9+xrPRwYiTAGAeQYl8
XJ+CExMCGfiP6w1ei6zOfHmvJqdj9jphxJt1U
QEwVzITEyIerMjQLkR/ty0CEzOSFcnCEzMyE
vHW5Nl/UlMOiiEcI7I3spmWmpwu1KeE2cX
j+LJtsH9q88cDK5BPB04HI9uK4zZVKaPAaQ+
z68o9VnS5kYEH11GYIHVuCJkK6+dgihMCR
NXqKIaRUSF9fSCFi4zMxsYKQbrqvM+N8y9h
OSGzldwErEZwKTciExMCE167X20odDOmoF
bK5Ez1itukX1mcFe71DQ5CpFZNshMTEhnm
GzSX4hMTIhm5qZdq2cZjh4A6fgam8+iGUsS
e7Q3oTnS2BgjoRSRXM8qSEzOSFQ99Gcx9E
hMzQh4DuL4T7csc01jhVoV4BTg/q4HG2Ia6
RRxg+dITkhe5Dp+g==

(a)

(b)

Or this…

(c)

If you could not read, so this is the fact

One fine evening a young princess put on her bonnet and clogs, and went out to take a walk by herself in a wood; and when she came to a cool spring of water with a rose in the middle of it, she sat herself down to rest a while.

(a)

(b)

If you could not read, so this is the fact

(c)

What is Cryptography?

“The practice and study of techniques for secure communication in the presence of third parties.”

Wikipedia.

What is Cryptography?

- Crypto = Secret
- Graphy = Writing
- Such a scheme is known as a Cryptographic System or a Cipher

Cryptography

- Until end of 1970's, there is only simetric cryptographic system
- Problem: how to send a secret key to the receiver?
- If you send a secret key through public channel (telephone, internet) is not secure
- Thus, a secret key must be send through second channel that would be secure
- A secure channel is expensive

Objective

- Confidentiality
- Integrity
- Authentication
- Non-Repudiation

Terminology

- Encryption

  The process of encoding messages or information in such a way that only authorized parties can read it.

- Decryption

  The reverse, in other words, moving from the unintelligible ciphertext back to plaintext.

Terminology

- Plain Text

  An original messages.

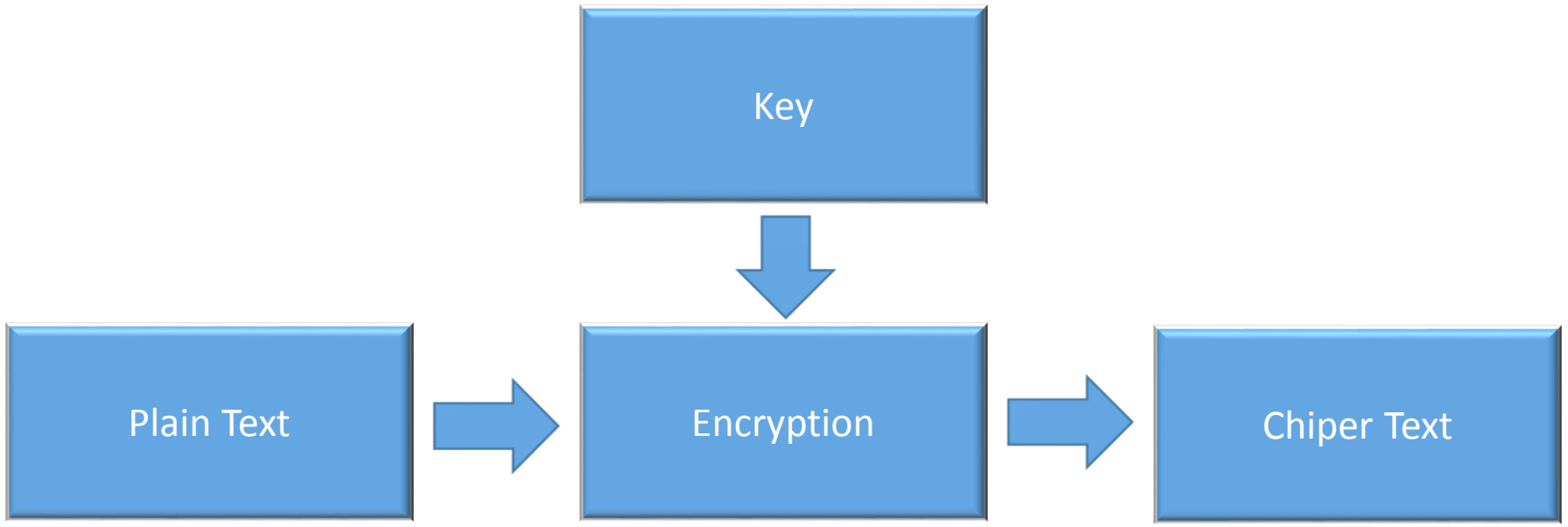
- Chiper Text

  The coded messages.

- Cryptanalysis

  Techniques used for deciphering a message without any knowledge of the enciphering details. Cryptanalysis is what the layperson calls “breaking the code”.

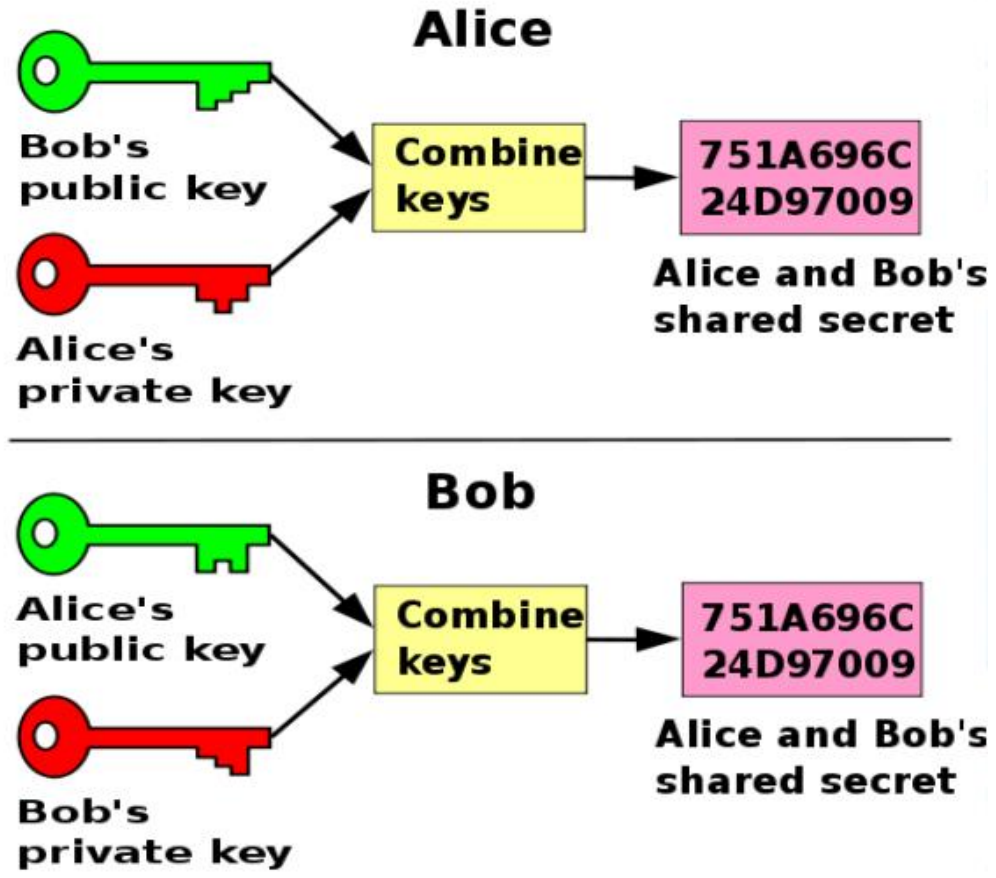
Mechanism



According to the type of Key

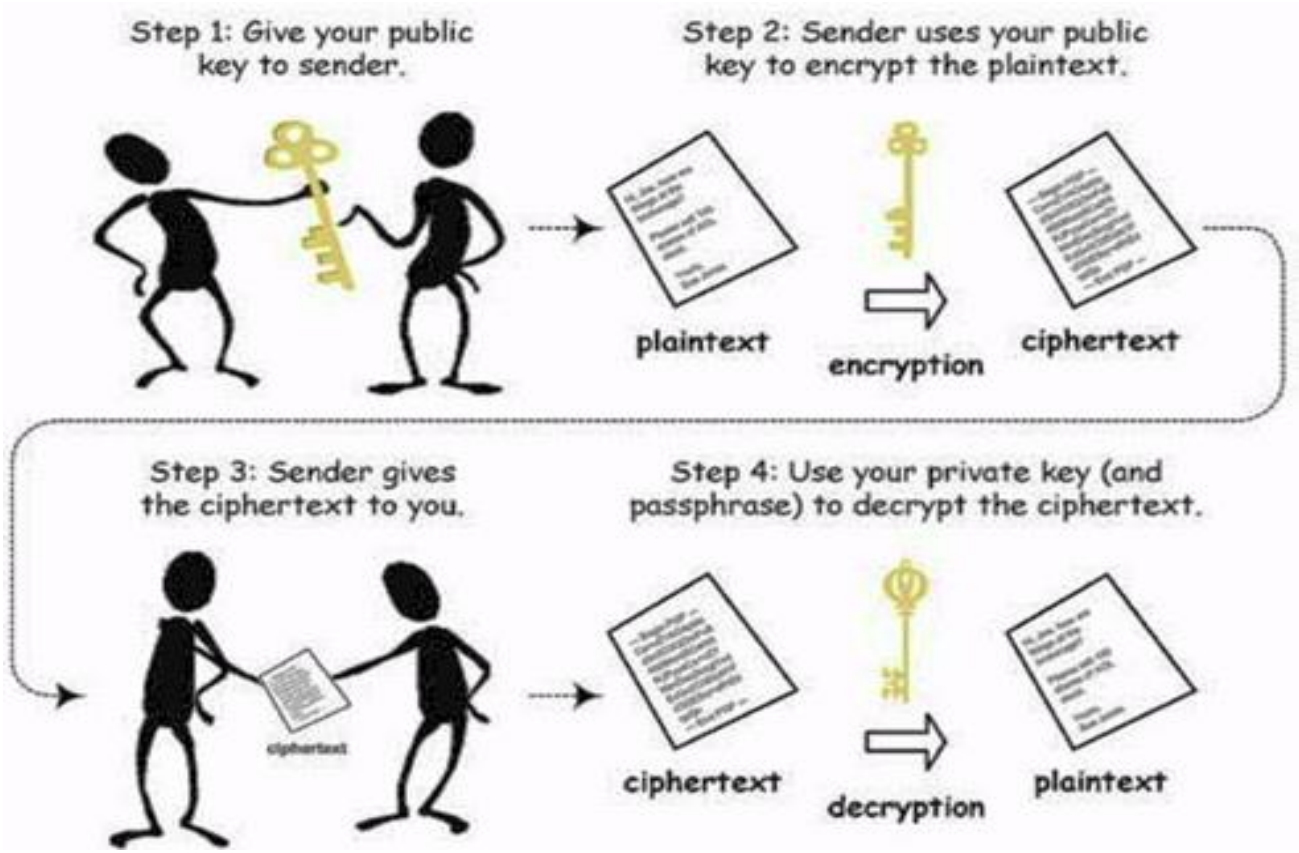
- Simetric Algorithm
- Asimetric Algorithm (Public and Private Key)

Public and Private Key



Source: http://en.wikipedia.org/wiki/Public-key_cryptography

Public and Private Key



Source: http://www.data-processing.hk/uploads/images/public_key_encryption%281%29.jpg

Analogy of Public and Private Key

- Alice and Bob have an unlock of padlock
- Bob give his padlock to the Alice
- When Alice want to send a message, she use Bob’s padlock to lock the message
- Only Bob can read the message because he has a key

Comparing of Simetric and Asimetric

- Simetric
  - For the process of encryption and decryption, the key are same.
  - For the process of encryption and decryption, it’s not take a long time
  - Size of simetric key is small
  - Simetric key must be send through secure channel
  - A key must be changed for a session
  - Example of Alogrithm: Twofish, Rijndael, Camellia, etc

Comparing of Simetric and Asimetric

- Asimetric
  - For the process of encryption and decryption, the key are different
  - No issue in distribution of keys
  - Easy to manage key because it’s use just a little of key
  - Only private key is secret
  - Asimetric key are not necessary to change in everytime even it’s can be use in long time
  - Asimetric can be used to secure simetric key
  - It can be used to give a digital signature

Comparing of Simetric and Asimetric

- Asimetric
  - Low of speed
  - The size of cipher text is bigger than plain text
  - The size of key is bigger than simetric key
  - Example of Algorithm: RSA, DSA, ELGamal, etc

Task

- Make your public and private key
- Send an encrypted email using my public key
  - Download my pubkey http://omega.or.id/girindigdo.tar.gz
- Content
  - Subject : Cryptography – IP – NIM – Name
  - Attachment : Your public key
- Send your task before

  September 30, 2015 at 10.00 p.m.