Introduction to Cryptography

Xavier Belanger

xavier@belanger.fr

January 2020

About the Speaker

- Network & System Administrator with 20 years of experience.
- Certified Information Systems Security Professional (CISSP).

Creative Common License - Attribution 4.0 International (CC BY 4.0)

You are free to:

- **Share** - copy and redistribute the material in any medium or format
- **Adapt** - remix, transform, and build upon the material for any purpose, even commercially.

The licensor cannot revoke these freedoms as long as you follow the license terms.

Under the following terms:

- **Attribution** - You must give appropriate credit, provide a link to the license, and indicate if changes were made. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.
- **No additional restrictions** - You may not apply legal terms or technological measures that legally restrict others from doing anything the license permits.

`https://creativecommons.org/licenses/by/4.0/legalcode`

Summary

- Vocabulary
- History
- Steganography
- Legal Aspects
- General Principles
- Hashing

- Symmetric Encryption
- Asymmetric Encryption
- Digital Signature
- TLS
- PGP, GPG and email encryption

Vocabulary and Definitions

- **encrypt**: converting plain text to an unreadable format.
- **decrypt**: converting a encoded text to plain text.
- **cryptology**: science of studying cryptology.
- **cryptanalysis**: researching weaknesses in cryptographic systems.

Few Historical Milestones

- Cryptography has been used since the Antiquity (Caesar’s cypher, …).
- It has been a decisive element during World War II.
- It has been revolutionzied during the 20th century with new algorithms and computing.

The Enigma Machine

Enigma Machine

Imperial War Museum

Londres

(source Wikimedia Commons)

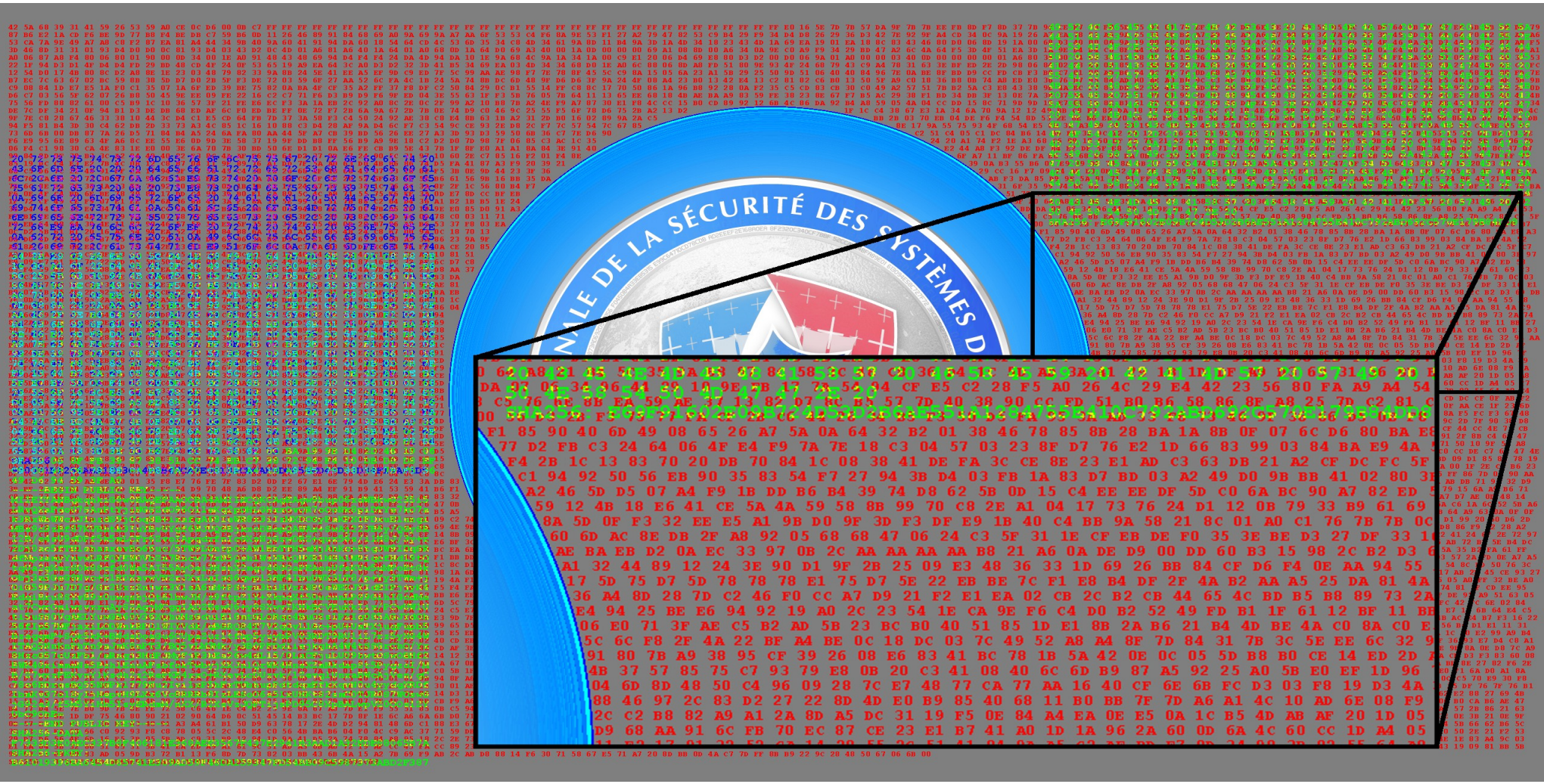
Cryptography in Recent Years

- 2009 - Bitcoin and cryptocurrencies
- 2011 - Diginotar Incident
- 2012 - HeartBleed, Freak, Poodle, Beast
- 2013 - Wannacry and other ransomwares
- 2013 - Edward Snowden’s Revelations
- 2015 - San Bernardino Attack
- 2016 - Let’s Encrypt
- 2018 - TLS 1.3

Steganography

- Steganography is a way to hide a message under another one, less important.
- In itself, it doesn’t protect the content. Once it is revealed, the content is in plaintext.


AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI


DE LA SÉCURITÉ DES SYSTÈMES D

Legal Aspects

- Using cryptographic tools is limited or illegal in certain countries.
- At the international level, import and export of cryptography is regulated by the Wassenaar Arrangement.

General Principles

- Any system is as secured as its weakest link.
- Encryption benefits only from regular usage.
- Only keys should be kept secret,
  not algorithms (*Kerckhoffs' Principle*).
- **Do not build your own cryptosystem**,
  use only proven, reliable tools and libraries.

Cryptography Benefits

Depending now how your are using cryptography, you can obtain the following benefits:

- **Encryption** will provide you:
  - confidentiality,
  - integrity,
  - authentification.
- A **digital signature** will provide you integrity and authentification.

Cryptography Limits

- Mathematical and technical improvements will require to keep your solution current.
- Systems and applications must be maintained up-to-date; security best practices must be enforced.
- Keys can be copied or stolen.
- The *National Security Agency*.

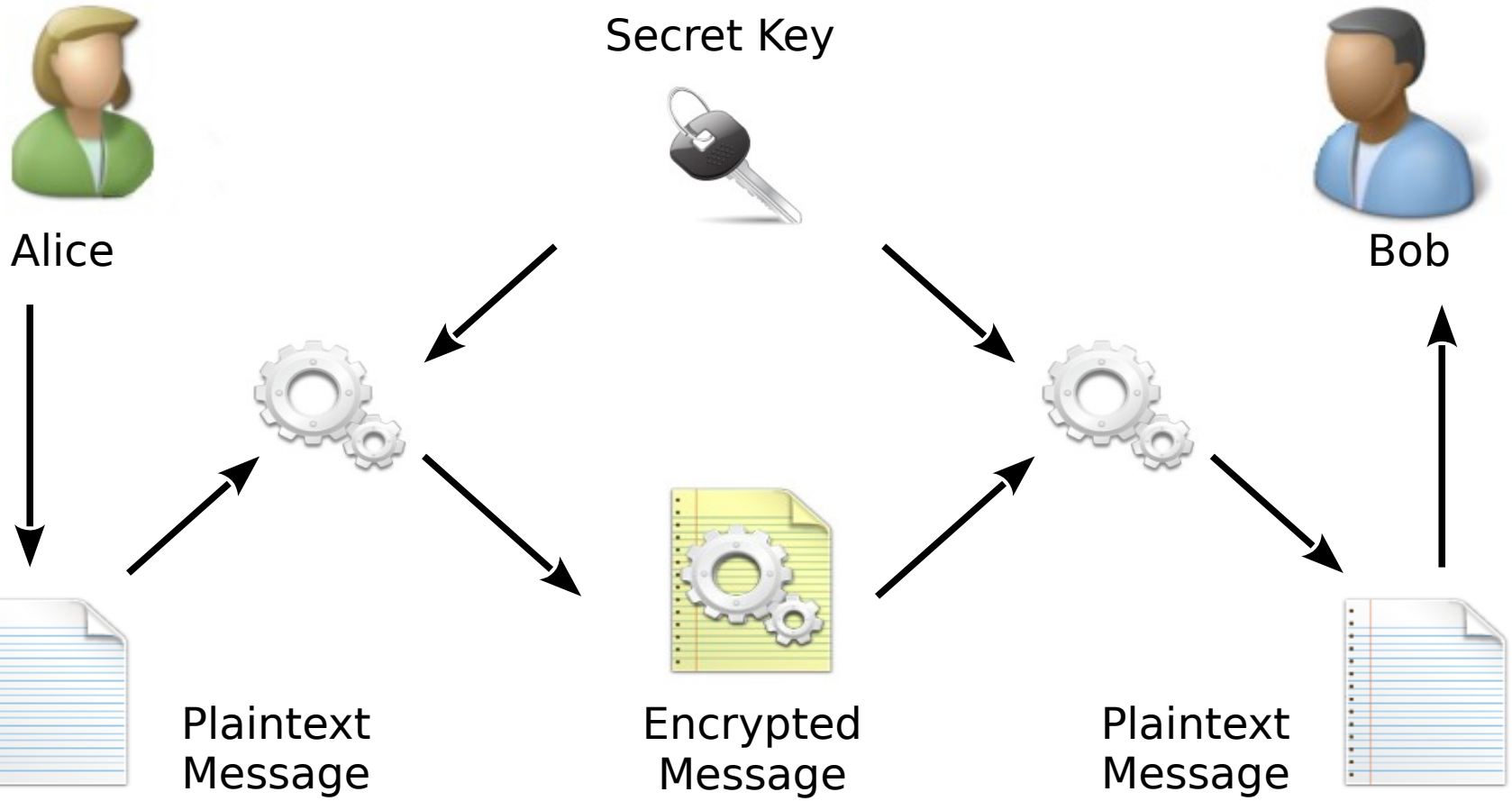
Hashing

- A cryptographic hash is a one way function that convert a message into a fixed size string.
- Hashes are used to check messages integrity.
- *MD5, SHA-1, SHA-2 (SHA-256), SHA-3*

Symmetric Encryption

- Also called "secret-key encryption".
- An encryption key is defined between the two parties.
- The same key is used to encrypt and to decrypt messages.

Using Symmetric Encryption



Symmetric Encryption Algorithms

- **DES**: *Data Encryption Standard*
- **AES**: *Advanced Encryption Standard* (*Rijndael*)
- **Salsa20/Chacha**
- **Vernam Cipher** *(One Time Pad)*

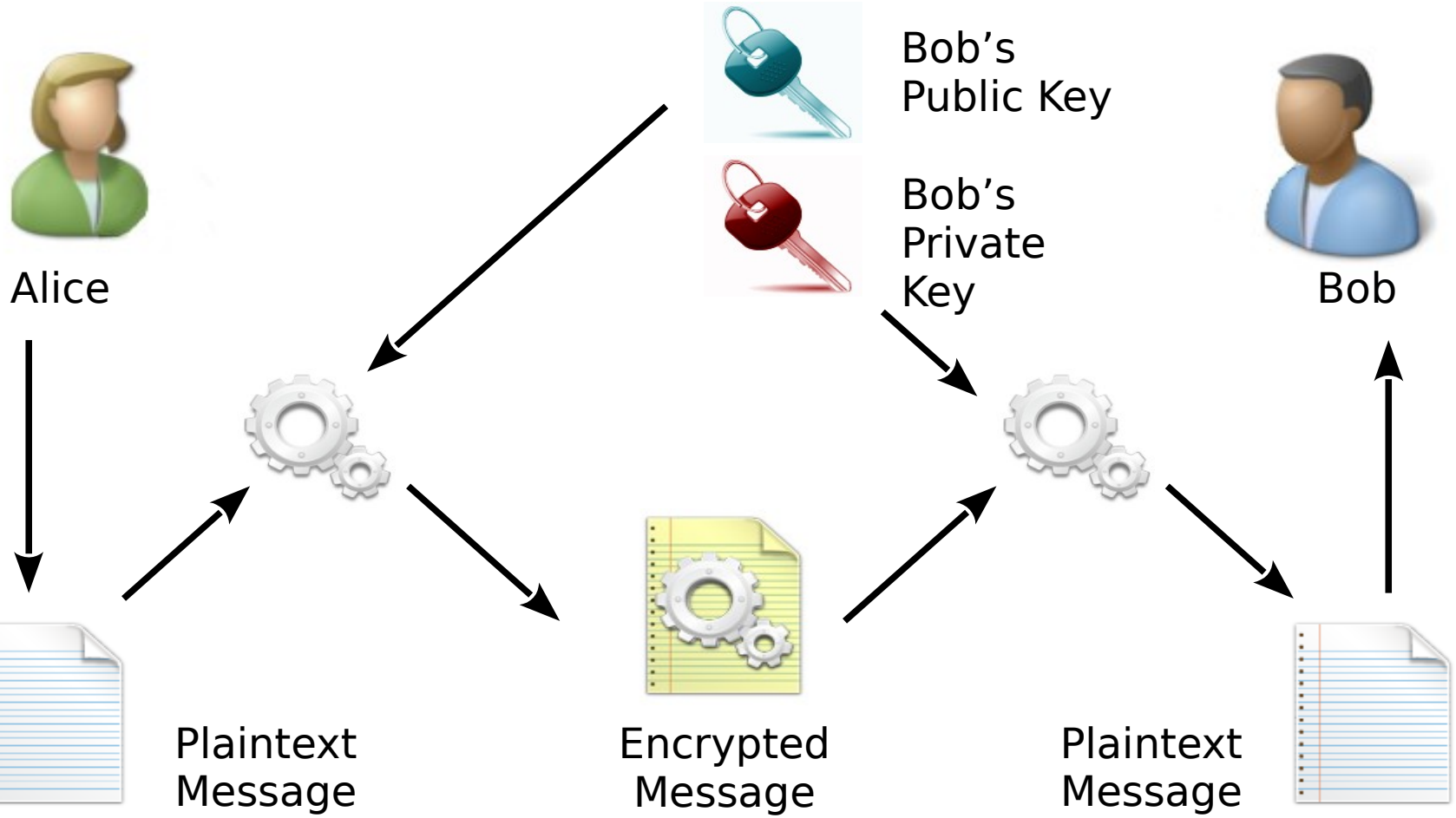
Symmetric Encryption Limits

- You must be able to share the key privately.
- When the number of participants increase, key management becomes an issue.
- For 10 people you will need:
  10x(10-1)/2 = 45 keys

Asymmetric Encryption

- Also called "public-key encryption"
- Each participant generate a private key, and a public key. That public key can be communicated to anyone.
- To send an encrypted message, you must use the public key of the recipient.

Using Asymmetric Encryption



Asymmetric Encryption Algorithms

- **RSA**: *Rivest, Shamir, Adleman*
- **Elliptic Curves**
- **ElGamal**

Asymmetric Encryption Limits

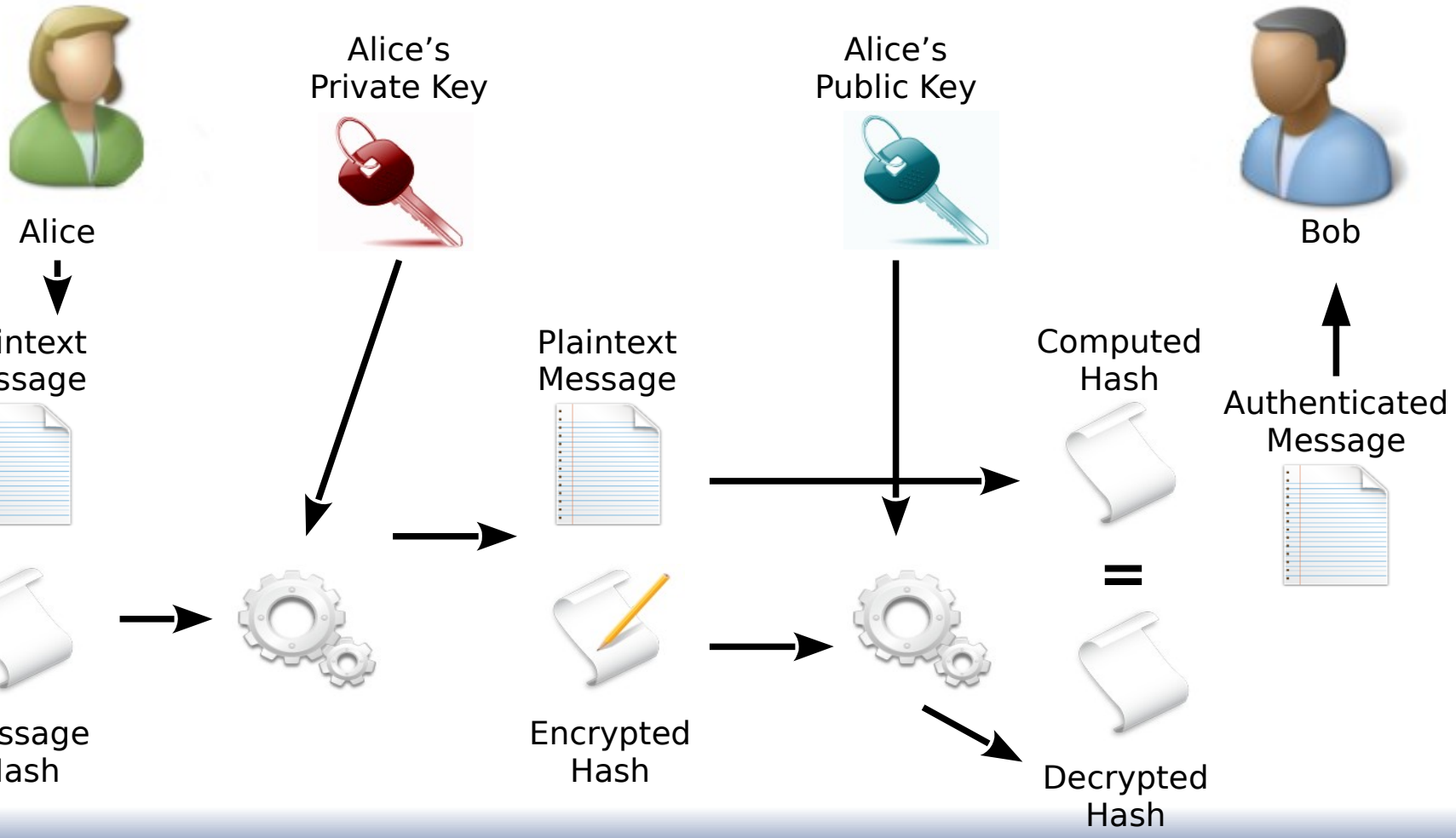
- Asymmetric encryption computation is much slower than symmetric encryption.
- You need to have a reliable and trustable way to distribute keys.

Digital Signature

- A digital signature can prove who wrote the message and that it has not been modified.

  The message itself is still readable by anyone.
- A digital signature will hash the message and then will rely on the same type of keys than for asymmetric encryption.

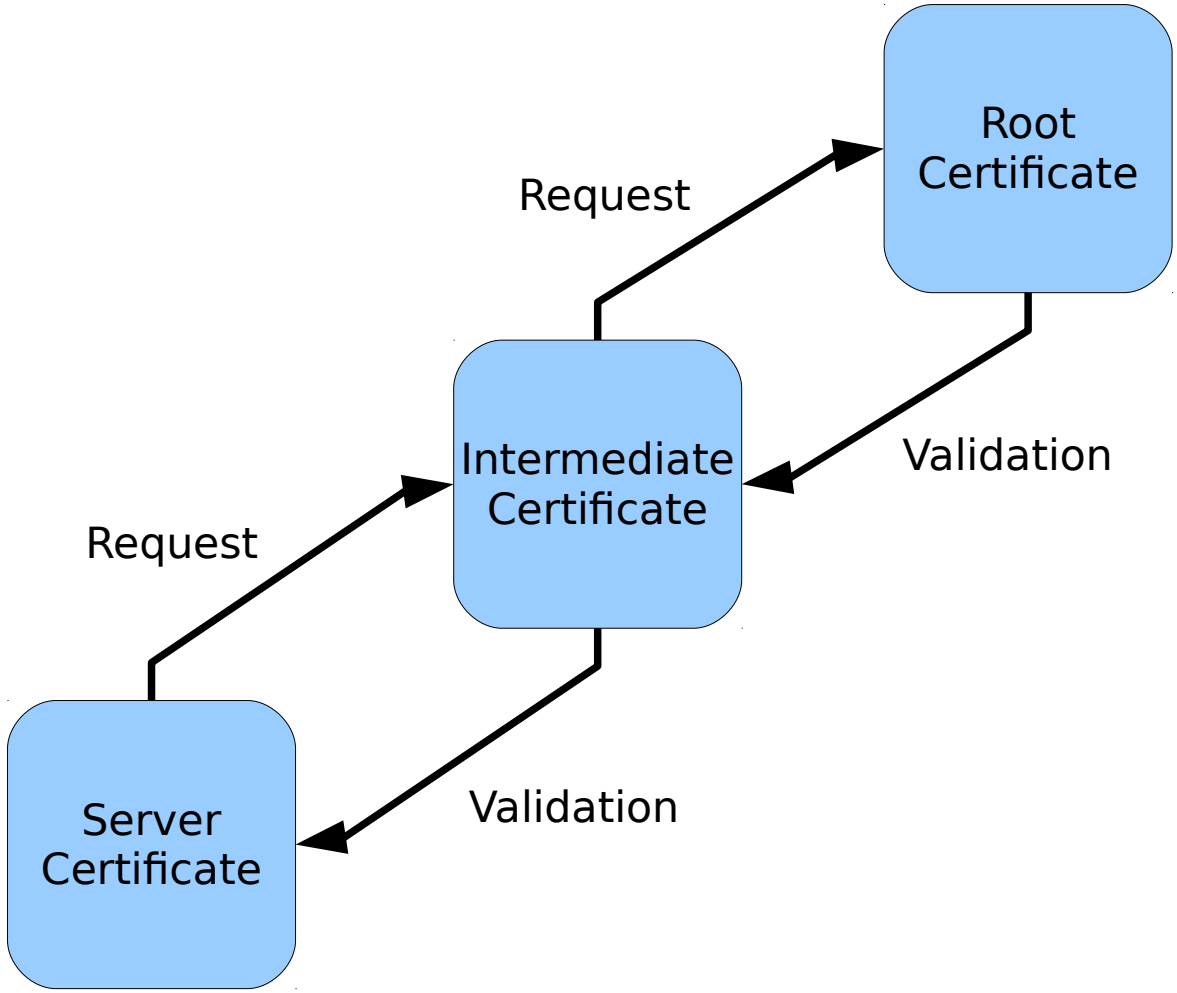
Using Digital Signature



TLS Certificates

X.509 Certificate

- Issuer
- Serial Number
- Validity (After)
- Validity (Before)
- Subject
- Subject Public Key
- Issuer's Signature



TLS Session Example

Client

Known Authorities

Client Hello (cipher suites)

Server Hello (certificate)

Key Exchange (pre-master secret)

Client Finish

Key Exchange (pre-master secret)

Server Finish

Server

X.509 Certificate

Pretty Good Privacy (PGP)

- Written by Philip Zimmermann in 1991.
- It was the first popular cryptographic software.
- PGP usage and popularity created more interest for cryptography.
- First versions were available for free; PGP is now a commercial software.

GNU Privacy Guard (GPG)

- GPG is the free software equivalent of PGP.
- It is using free, not patented algorithms.
- GPG is available on many systems and comply with the OpenPGP standard (*RFC 4880*).

Using GPG

- GPG is a command line application, with a high number of options.
- Various graphical interfaces are available for day to day use:
  - *KGPG* for KDE,
  - *Seahorse* for Gnome,
  - *WinGPG* and *Gpg4Win* for MS Windows,
  - *MacGPG2* for Apple Mac OS X.

Protecting E-mail

- Your e-mail client must be able to use GPG to verify, encrypt or decrypt messages
- Some e-mail clients have native OpenGPG support, other would require an extension.
- Email encryption will usually protect the message itself, but not the meta-data (headers).

Key Distribution

- Attending *key signing parties*
- Using key servers
- Using PKI (Public Key Infrastructure)

Questions
&
Discussion

Graphical Assets

- Aero Icons / gnome-look.org

  `http://www.gnome-look.org/content/show.php/Aero?content=35437`

- Nobile Font

  `https://fonts.google.com/specimen/Nobile`