Security of Information Systems "Fundamentals"

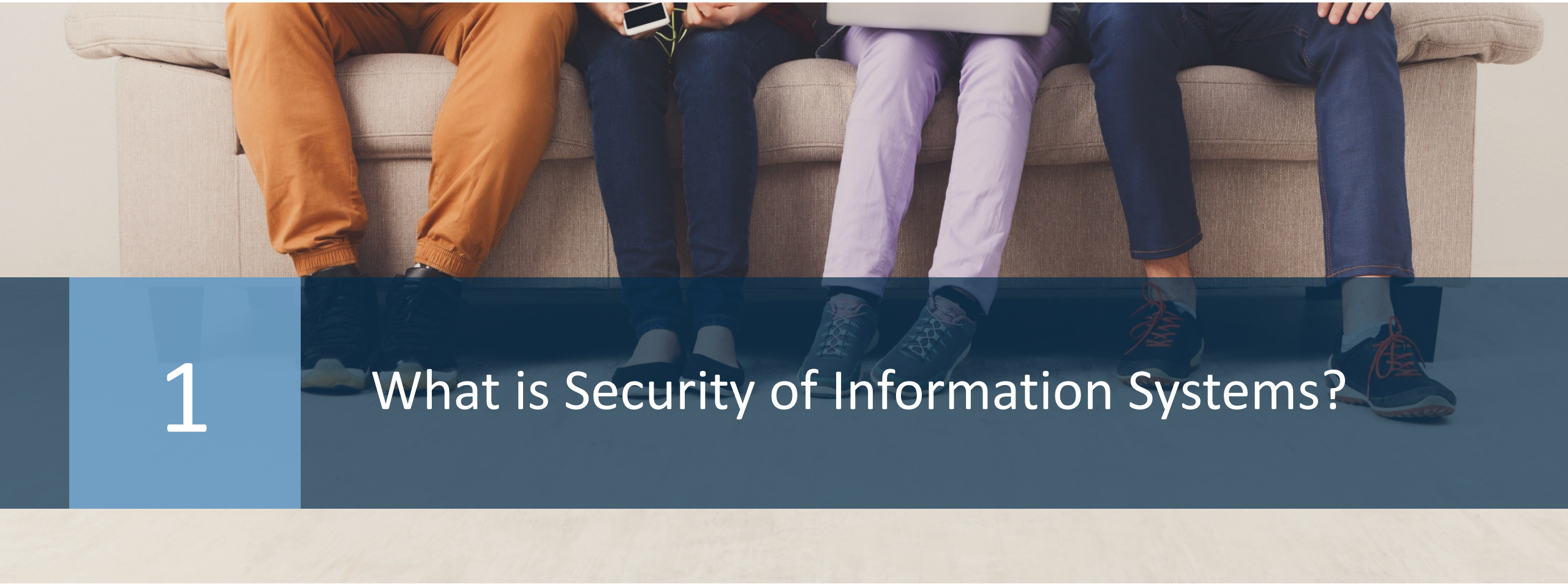
ECE Paris – Engineering School

Ali HAIDAR.

JAN 2019.

Security of Information Systems

Agenda



1 What is Security of Information Systems?

What is Security of Information Systems?

- The Security of information systems is a set of technical, organizational, legal and human necessary for the establishment of means to prevent unauthorized use, misuse , modification or diversion of the information system. Ensuring the security of the information system is an activity of the management of the information system.
- Security is the protection of computing systems/Asset and the data that they store or access.

Security of Information Systems, Why?

- In the past, computer networks were used in universities and companies
- Nowadays, millions of users (ordinary) use networks for banking, shopping, paying taxes.
- Network security is crucial and critical
- Most security issues are caused by malicious people trying to:
  - Gain some benefit
  - Get attention
  - Harm someone
- Security is concerned by protecting information (messages) from malicious people, to make sure that they can not read or modify content.
- It is concerned with people trying to access remote services that they are not authorized to use.
- It deals with ways to tell whether messages reported by your bank is really from your bank and not from thieves.

Why do I need to learn about Computer Security?

Isn’t this just an IT Problem?

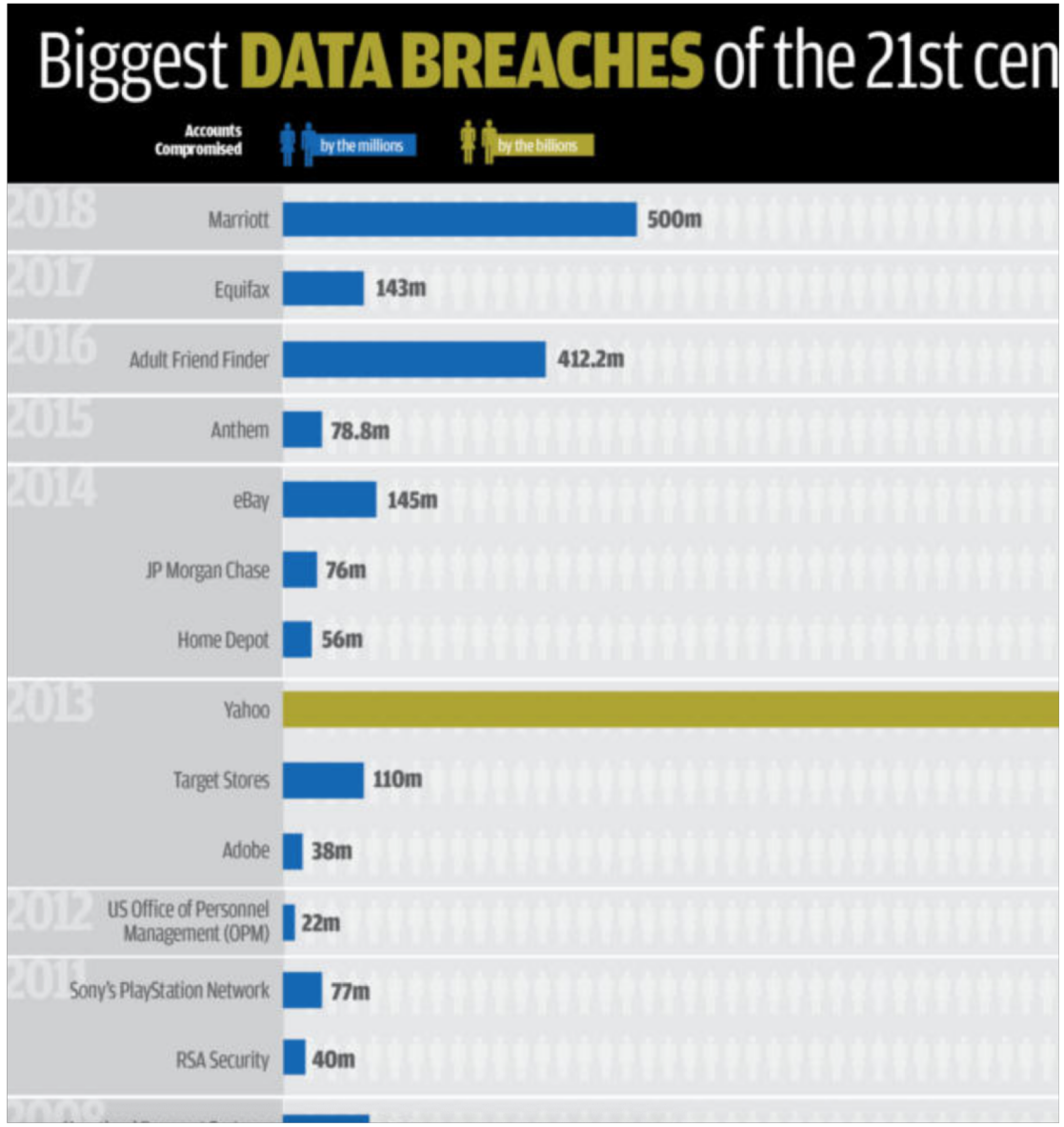
Good Security Standards follow the "**90/10**" Rule:

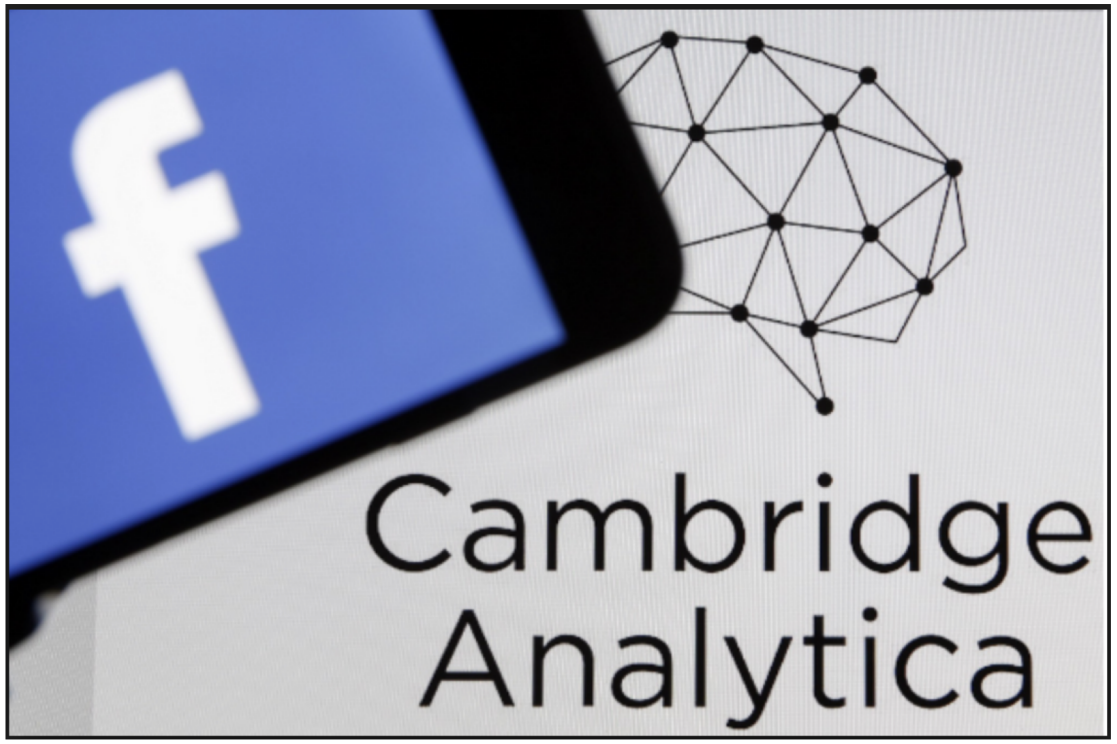
- **10%** of security safeguards are technical
- **90%** of security safeguards rely on the computer user ("YOU") to adhere to good computing practices
- Example: The lock on the door is the 10%. You remembering to lock the lock, checking to see if the door is closed, ensuring others do not prop the door open, keeping control of the keys, etc. is the 90%. You need both parts for effective security.

Data Leakage

- Data leakage is the unauthorized transmission of data from within an organization to an external destination or recipient. The term can be used to describe data that is transferred electronically or physically. Data leakage threats usually occur via the web and email, but can also occur via mobile data storage devices such as optical media, USB keys, and laptops.
- Barely a day goes by without a confidential data breach hitting the headlines. Data leakage, also known as low and slow data theft, is a huge problem for **data security**, and the damage caused to any organization, regardless of size or industry, can be serious. From declining revenue to a tarnished reputation or massive financial penalties to crippling lawsuits, this is a threat that any organization will want to protect themselves from.
- **Types:**
  - **The Accidental Breach**
  - **The Disgruntled or Ill-Intentioned Employee**
  - **Electronic Communications with Malicious Intent**

Data Leakage/Breaches



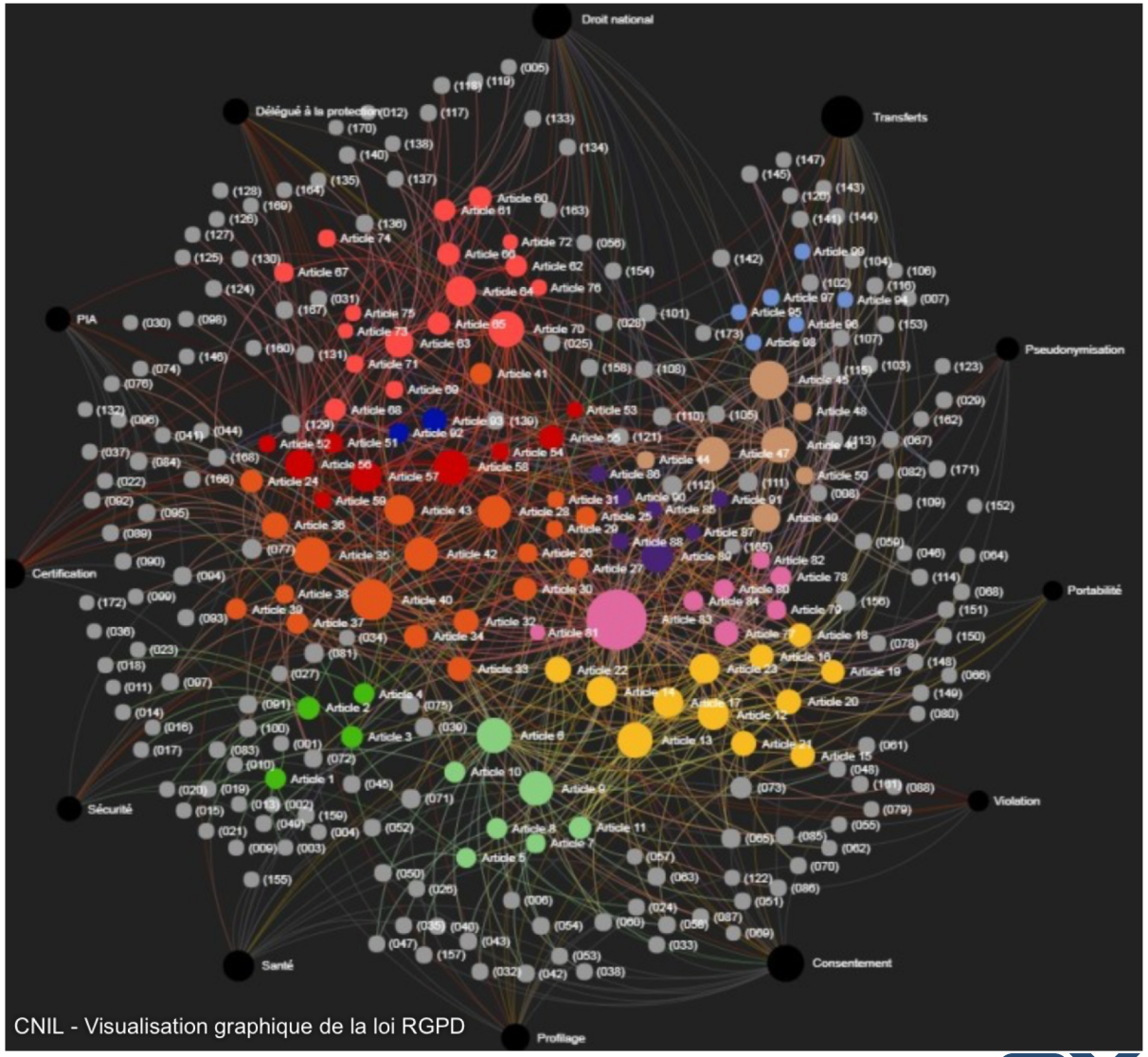


GDPR- General Data Protection Regulation

Main Objectives:

- Standardize data protection regulations at European level.
- Empowering businesses by developing self-control (Data officer, etc.).
- Strengthen the right of people (right to access, right to be forgotten, right to portability, etc.).

Effective : **25th of MAY 2018**



CNIL - Visualisation graphique de la loi RGPD

Stay Open.

What Does This Mean for Me?

- Means that everyone who uses a computer or mobile device needs to understand how to keep their computer, devices and data secure.
- Information Security is everyone’s responsibility

The Internet can be a hazardous place:

How many attacks to computers on campus do you think take place everyday?

The Internet can be a hazardous place

- Thousands of attacks per minute bombard our campus network.
- An unprotected computer can become infected or compromised within a few seconds after it is connected to the network.
- Worldwide spend for cyber security continues to grow: 71.1 billion in 2014 (7.9% over 2013), and 75 billion in 2015 (4.7% from 2014) and expected to reach 101 billion by 2019.

Question: A hacked computer can be used to… (select all that apply)

a) Record keystrokes and steal passwords.

b) Send spam and phishing emails.

c) Harvest and sell email addresses and passwords.

d) Access restricted or personal information on your computer or other systems that you have access to.

e) Infect other systems.

f) Hide programs that launch attacks on other computers.

g) Illegally distribute music, movies and software.

h) Distribute child pornography.

i) Generate large volumes of traffic, slowing down the entire system.

Question: A hacked computer can be used to… (select all that apply)

Of course, the answer is “All of the them.” A compromised computer can be used for all kinds of surprising things.

What are the consequences for security violations?

- Risk to security and integrity of personal or confidential information
- e.g. identity theft, data corruption or destruction; lack of availability of critical information in an emergency, etc.
- Loss of valuable business information
- Loss of employee and public trust, embarrassment, bad publicity, media coverage, news reports
- Costly reporting requirements in the case of a compromise of certain types of personal, financial and health information
- Internal disciplinary action(s) up to and including termination of employment, as well as possible penalties, prosecution and the potential for sanctions / lawsuits

Security Learning Objectives

- l Learn “good computing security practices.”
- l Incorporate these practices into my everyday routine. Encourage others to do so as well.
- l Report anything unusual – Notify your supervisor and the ITS Support Center if you become aware of a suspected security incident.

Security awareness training

- Phishing attacks- SPAM emails (email that wants to get information about you, click on links, identify)
- Social engineering (when you are contacted to reset your password)
- How to prevent data leakage
- Create strong and easy to remember password
- Browsing safe online
- Securing your personal devices

2 Security Practices & Processes

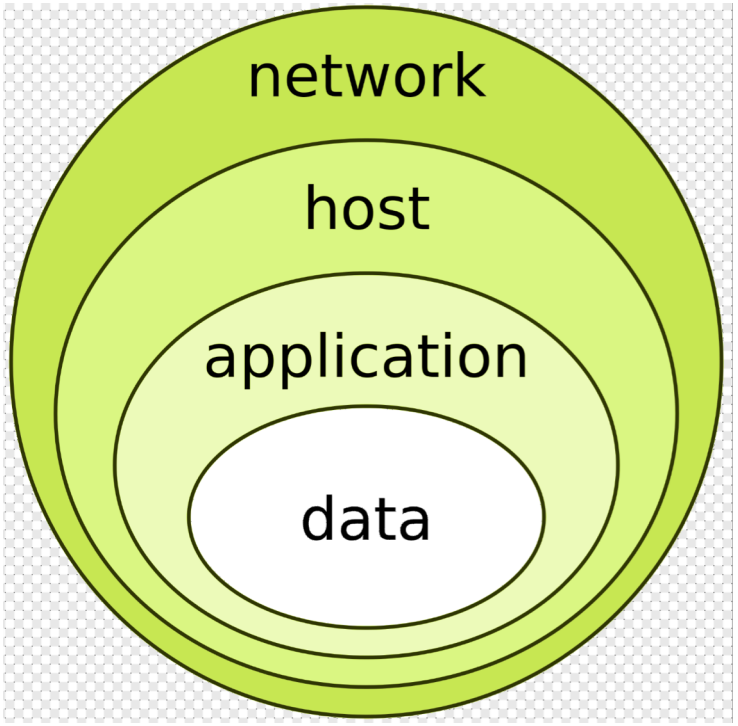
The security of information systems has the following objectives:

- **Confidentiality:** is the property, that information is not made available or disclosed to unauthorized individuals, entities, or processes.
- **Integrity :** means maintaining and assuring the accuracy and completeness of data over its entire lifecycle. This means that data cannot be modified in an unauthorized or undetected manner.
- **Availability:** For any information system to serve its purpose, the information must be available when it is needed. This means the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly.
- **Non-repudiation** : Implies one's intention to fulfill their obligations to a contract. It also implies that one party of a transaction cannot deny having received a transaction, nor can the other party deny having sent a transaction.

Security in the protocol Stack

No one single place. Every where

Information security must protect information throughout its lifespan, from the initial creation of the information on through to the final disposal of the information



- **Physical layer:**
  - Wiretapping can be protected by enclosing transmission lines in tubes containing an inert gas at high pressure. Piercing the tube will change the pressure level and trigger an alarm
- **Data Link Layer:**
  - Data can be encrypted/decrypted at the output/input of a link .
  - The solution is less efficient when data traverses several routers. Data is left vulnerable at router level.
- **Network layer:**
  - Firewalls can be installed to keep good packets and bad packets out
  - IP security also functions at this layer
- **Transport Layer:**
  - Entire connections can be encrypted/decrypted from end to end (process to process).
- **Application layer:**
  - User authentication and non repudiation

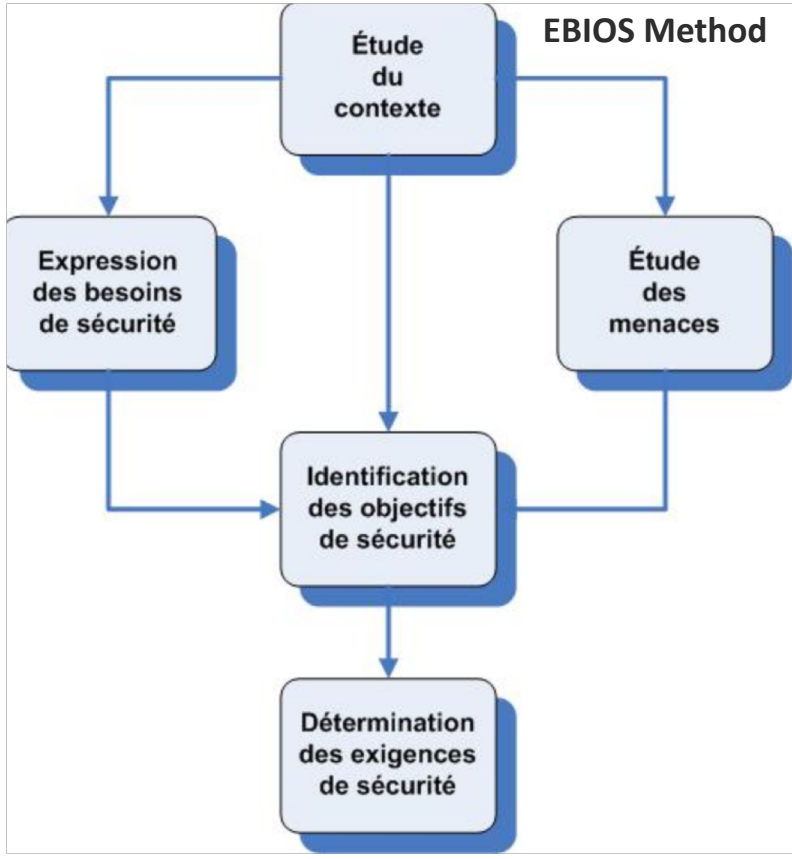
Security Practices

- **Identification**: is an assertion of who someone is or what something is (e.g. Username)
- **Authentication**: is the act of verifying a claim of identity. It deals with determining the identity of whom you are talking to before revealing sensitive information or entering into a deal.
  - Something you know: things such as a PIN, a password, or your mother's maiden name
  - Something you have: a driver's license or a magnetic swipe card
  - Something you are: biometrics, including palm prints, fingerprints, voice prints and retina (eye) scans
- **Authorization**: it must be determined what informational resources they are permitted to access and what actions they will be allowed to perform (run, view, create, delete, or change)

Security Strategy Process

Many tools and standards exist (PLAN, DO, Check & Act)

- **Risk Evaluation and analysis Process :**
  - France : EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) developed by the ANSSI
  - USA : OCTAVE (*Operationally Critical Threat, Asset, and Vulnerability Evaluation*), developed. By Carnegie Mellon University.
  - International : ISO/CEI 27005, et ISO 27001
- **Identify the assests** (material, physical, human, documents, software, etc.)
- **Identify the responsible** (CISO, IT Director, etc.)
- **Identify the vulnerabilities** (weak points)
- **Identify the consequences** (losing confidentiality or availability, etc.)
- **Identify the damages** (financial, brand, legal, ecological, etc.)
- **Estimate the level of risk** (rank it from 0 to 100)



Security Strategy Process

Many tools and standards exist (PLAN, DO, Check & Act)

It’s about deploying measures to fulfill the security objectives (it’s done under project mode)

- Deploying risk measures:
  - Access control mechanism
  - Network control (intrusion detection system, Firewall, antivirus/Antispam, etc.)
  - Application security (retro-engineering, code audit),
  - Authentication (strong authentication, PKI, encryption)
  - DRP (Disaster Recovery Plan)

Security Strategy Process

Many tools and standards exist (PLAN, DO, Check & Act)

- Internal & External Audits
- Simulation exercises : DRP
- Use standards and best practices:
  - COBIT: enables risk analysis and control of investments
  - ITIL: The goal is to promote business efficiency in the use of IS in order to meet organizational demands to reduce costs while maintaining or improving IT services
  - ISO / IEC 27007: Guidelines to assist internal or external auditors in monitoring secuirty activities

Security Strategy Process

Many tools and standards exist (PLAN, DO, Check & Act)

After highlighting a malfunction through the Check phase, it is important to analyze them and put in place:

- **Corrective actions**: It is necessary to act on the dysfunction and to remove its effect
- **Preventive actions**: We act before the malfunction occurs
- **Improvement Actions**: Improves the performance of a process.

3 Cyber Attacks

Motivation and profile of attackers

Adversary	Goal
Student	To have fun snooping on people's e-mail
Cracker	To test out someone's security system; steal data
Sales rep	To claim to represent all of Europe, not just Andorra
Businessman	To discover a competitor's strategic marketing plan
Ex-employee	To get revenge for being fired
Accountant	To embezzle money from a company
Stockbroker	To deny a promise made to a customer by e-mail
Con man	To steal credit card numbers for sale
Spy	To learn an enemy's military or industrial secrets
Terrorist	To steal germ warfare secrets

Cyber Attacks

The 10 most common cyber attack types:

- Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks
- Man-in-the-middle (MitM) attack
- Phishing and spear phishing attacks
- SQL injection attack
- Drive-by attack
- Password attack
- Cross-site scripting (XSS) attack
- Eavesdropping attack
- Birthday attack
- Malware attack

Some Definitions

- **Virus**: is a program or **piece of code** that is loaded onto your computer without your knowledge and runs against your wishes. Viruses can also replicate themselves. All computer viruses are man-made.
- **Warm**: is **self-replicating program** that duplicates itself to spread to uninfected computers. Worms often use parts of an operating system that are automatic and invisible to the user. It is common for worms to be noticed only when their uncontrolled replication consumes system resources, slowing or halting other tasks. **A computer worm infection spreads without user interaction.**
- **Trojan**: a Trojan horse is a program that appears harmless, but is, in fact, malicious. Unexpected changes to computer settings and unusual activity, even when the computer should be idle, are strong indications that a Trojan is residing on a computer. A Trojan horse may also be referred to as a Trojan horse virus, but that is technically incorrect. Unlike a computer virus, **a Trojan horse is not able to replicate itself, nor can it propagate without an end user's assistance.**

Most known viruses/ warms

- **ILOVEYOU** : Attached (.txt) file to emails, consequences: Laptop speed reducing and virus spread to all your contacts,
- **PETYA** : Ransomware, encrypt your data. Company doesn't have access to database,
- **HeartBleed**: your password are not confidential anymore,
- **Freak**: based on a weakness in TLS, it was able to access your bank accounts,
- **Stuxnet**: called the nuclear warm. Hacked the Iranian nuclear site in 2010 and stopped the uranium centrifuges,
- Etc.

Cyber Attacks

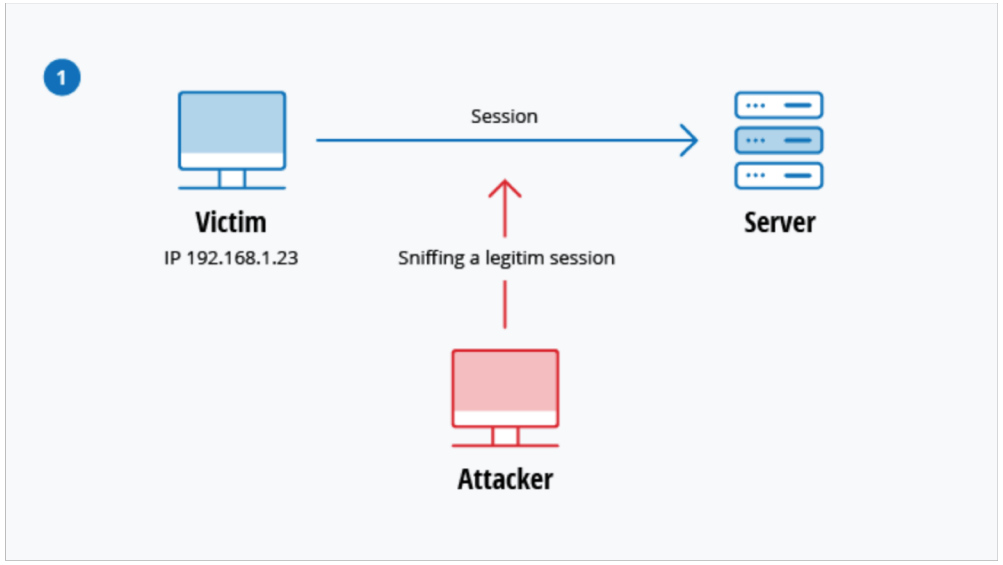
Denial-of-Service (DoS)

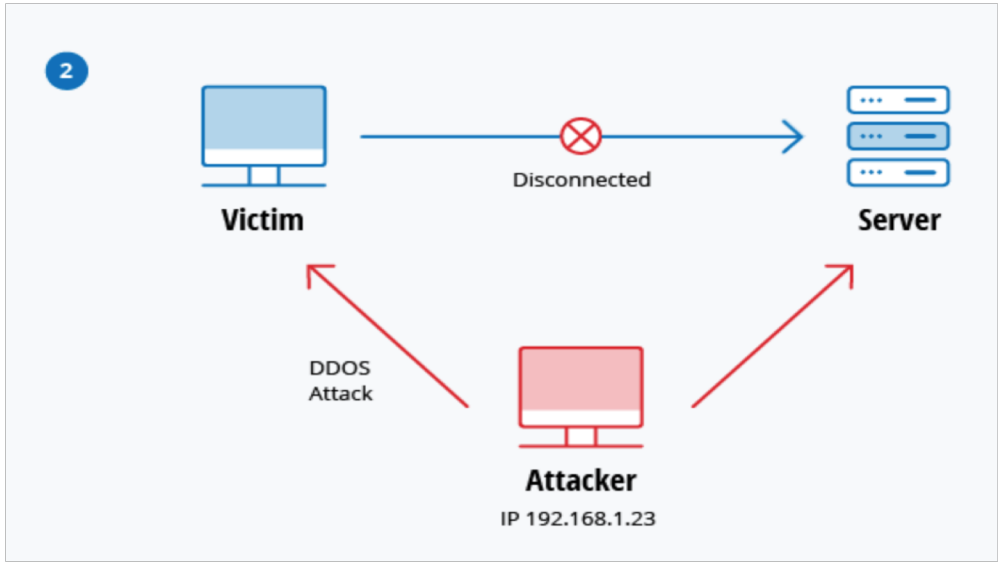
- Imagine you're sitting in traffic on a one-lane country road, with cars backed up as far as the eye can see. Normally this road never sees more than a car or two, but a county fair and a major sporting event have ended around the same time, and this road is the only way for visitors to leave town. The road can't handle the massive amount of traffic, and as a result it gets so backed up that pretty much no one can leave.
- That's essentially what happens to a website during a denial-of-service (DoS) attack. If you flood a website with more traffic than it was built to handle, you'll overload the website's server and it'll be nigh-impossible for the website to serve up its content to visitors who are trying to access it.
- This can happen for innocuous reasons of course, say if a massive news story breaks and a newspaper's website gets overloaded with traffic from people trying to find out more. But often, this kind of traffic overload is malicious, as an attacker floods a website with an overwhelming amount of traffic to essentially shut it down for all users.
- In some instances, these DoS attacks are performed by many computers at the same time. This scenario of attack is known as a Distributed Denial-of-Service Attack (DDoS). This type of attack can be even more difficult to overcome due to the attacker appearing from many different IP addresses around the world simultaneously, making determining the source of the attack even more difficult for network administrators. Different types of DOX attacks:
    - **TCP SYN flood attack**
    - **Teardrop attack**
    - **Smurf attack**
    - **Ping of Death**
    - **Botnets**

Cyber Attacks

Session Hijacking and Man-in-the-Middle Attacks

- When you're on the internet, your computer has a lot of small back-and-forth transactions with servers around the world letting them know who you are and requesting specific websites or services. In return, if everything goes as it should, the web servers should respond to your request by giving you the information you're accessing. This process, or session, happens whether you are simply browsing or when you are logging into a website with your username and password.
- The session between your computer and the remote web server is given a unique session ID, which should stay private between the two parties; however, an attacker can hijack the session by capturing the session ID and posing as the computer making a request, allowing them to log in as an unsuspecting user and gain access to unauthorized information on the web server. There are a number of methods an attacker can use to steal the session ID, such as a cross-site scripting attack used to hijack session IDs.
- An attacker can also opt to hijack the session to insert themselves between the requesting computer and the remote server, pretending to be the other party in the session. This allows them to intercept information in both directions and is commonly called a man-in-the-middle attack.





Cyber Attacks
Phishing, SQL Injection

- **Phishing**
    - An attacker may send you an email that appears to be from someone you trust, like your boss or a company you do business with. The email will seem legitimate, and it will have some urgency to it (e.g. fraudulent activity has been detected on your account). In the email, there will be an attachment to open or a link to click. Upon opening the malicious attachment, you'll thereby install malware in your computer. If you click the link, it may send you to a legitimate-looking website that asks for you to log in to access an important file—except the website is actually a trap used to capture your credentials when you try to log in
- **SQL Injection**
    - SQL stands for structured query language; it's a programming language used to communicate with databases. Many of the servers that store critical data for websites and services use SQL to manage the data in their databases. A SQL injection attack specifically targets this kind of server, using malicious code to get the server to divulge information it normally wouldn't. This is especially problematic if the server stores private customer information from the website, such as credit card numbers, usernames and passwords (credentials), or other personally identifiable information, which are tempting and lucrative targets for an attacker.
    - An SQL injection attack works by exploiting any one of the known SQL vulnerabilities that allow the SQL server to run malicious code. For example, if a SQL server is vulnerable to an injection attack, it may be possible for an attacker to go to a website's search box and type in code that would force the site's SQL server to dump all of its stored usernames and passwords for the site.

Cyber Attacks

Drive-By

- Drive-by download attacks are a common method of spreading malware. H**ackers look for insecure websites and plant a malicious script into HTTP or PHP code on one of the pages**. This script might **install malware directly onto the computer of someone who visits the site, or it might re-direct the victim to a site controlled by the hackers**. Drive-by downloads can happen when visiting a website or viewing an email message or a pop-up window. Unlike many other types of cyber security attacks, a **drive-by doesn't rely on a user to do anything to actively enable the attack** — you don't have to click a download button or open a malicious email attachment to become infected. A drive-by download can take advantage of an app, operating system or web browser that contains security flaws due to unsuccessful updates or lack of updates.
- To protect yourself from drive-by attacks, you need to keep your browsers and operating systems up to date and avoid websites that might contain malicious code. Stick to the sites you normally use — although keep in mind that even these sites can be hacked. Don't keep too many unnecessary programs and apps on your device. The more plug-ins you have, the more vulnerabilities there are that can be exploited by drive-by attacks.

Cyber Attacks

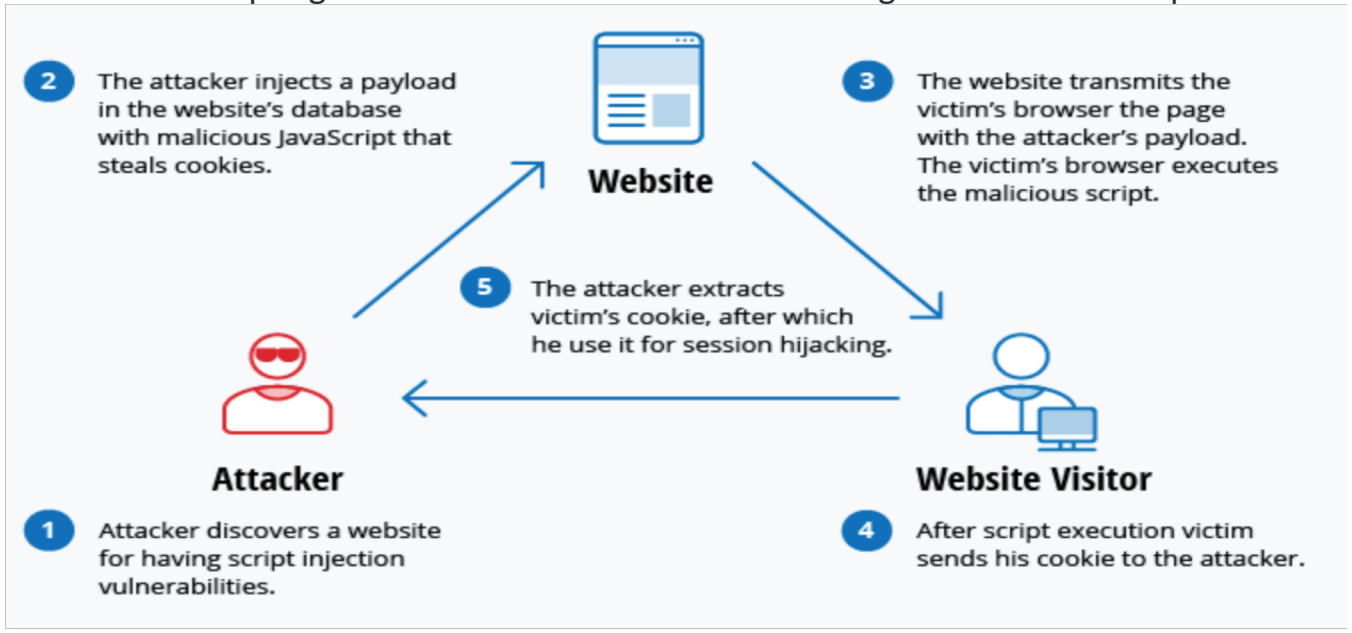
Credential Reuse & Password attacks

- Users today have so many logins and passwords to remember that it's tempting to reuse credentials here or there to make life a little easier. Even though security best practices universally recommend that you have unique passwords for all your applications and websites, many people still reuse their passwords—a fact attackers rely on.
- Once attackers have a collection of usernames and passwords from a breached website or service (easily acquired on any number of black market websites on the internet), they know that if they use these same credentials on other websites there's a chance they'll be able to log in. No matter how tempting it may be to reuse credentials for your email, bank account, and your favorite sports forum, it's possible that one day the forum will get hacked, giving an attacker easy access to your email and bank account. When it comes to credentials, variety is essential. Password managers are available and can be helpful when it comes to managing the various credentials you use.
- Because passwords are the most commonly used mechanism to authenticate users to an information system, obtaining passwords is a common and effective attack approach. Access to a person's password can be obtained by looking around the person's desk, ''sniffing'' the connection to the network to acquire unencrypted passwords, using social engineering, gaining access to a password database or outright guessing. The last approach can be done in either a random or systematic manner:
- **Brute-force** password guessing means using a random approach by trying different passwords and hoping that one work Some logic can be applied by trying passwords related to the person's name, job title, hobbies or similar items.
- In a **dictionary attack,** a dictionary of common passwords is used to attempt to gain access to a user's computer and network. One approach is to copy an encrypted file that contains the passwords, apply the same encryption to a dictionary of commonly used passwords, and compare the results.
- In order to protect yourself from dictionary or brute-force attacks, you need to **implement an account lockout policy that will lock the account after a few invalid password attempts**.

Cyber Attacks

Cross-Site Scripting (XSS)

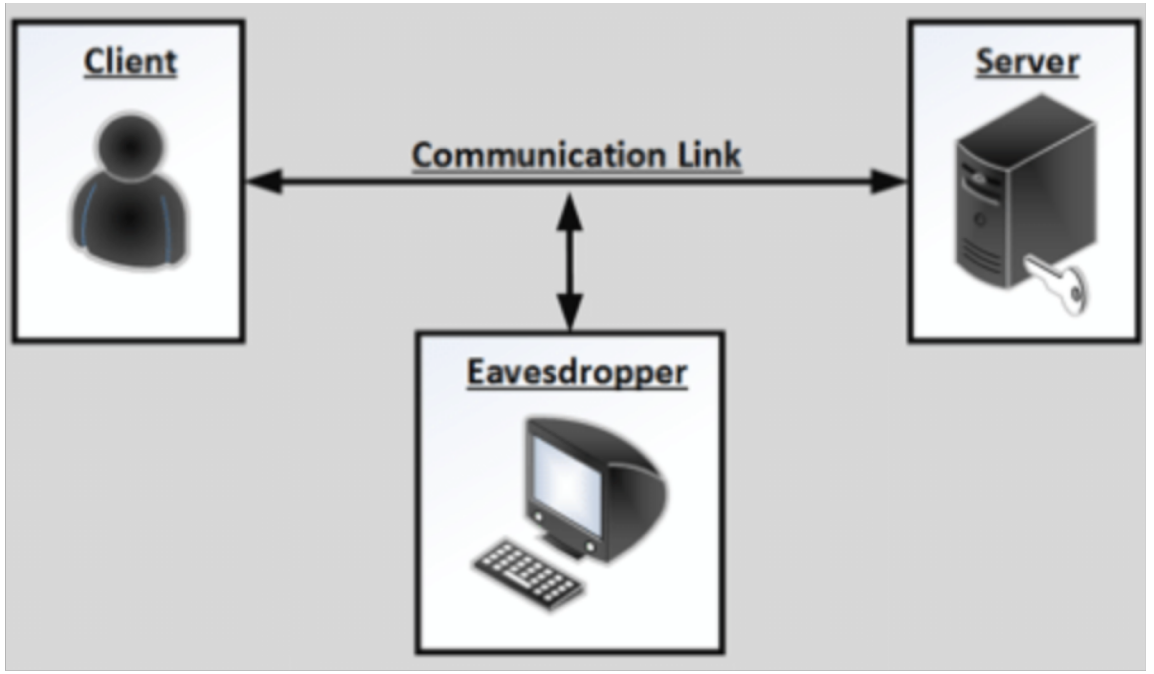
- In an SQL injection attack, an attacker goes after a vulnerable website to target its stored data, such as user credentials or sensitive financial data. But if the attacker would rather directly target a website's users, they may opt for a cross-site scripting attack. Similar to an SQL injection attack, this attack also involves injecting malicious code into a website, but in this case the website itself is not being attacked. Instead, the malicious code the attacker has injected only runs in the user's browser when they visit the attacked website, and it goes after the visitor directly, not the website.
- One of the most common ways an attacker can deploy a cross-site scripting attack is by injecting malicious code into a comment or a script that could automatically run. For example, they could embed a link to a malicious JavaScript in a comment on a blog.
- Cross-site scripting attacks can significantly damage a website’s reputation by placing the users' information at risk without any indication that anything malicious even occurred. Any sensitive information a user sends to the site—such as their credentials, credit card information, or other private data—can be hijacked via cross-site scripting without the website owners realizing there was even a problem in the first place.



Cyber Attacks

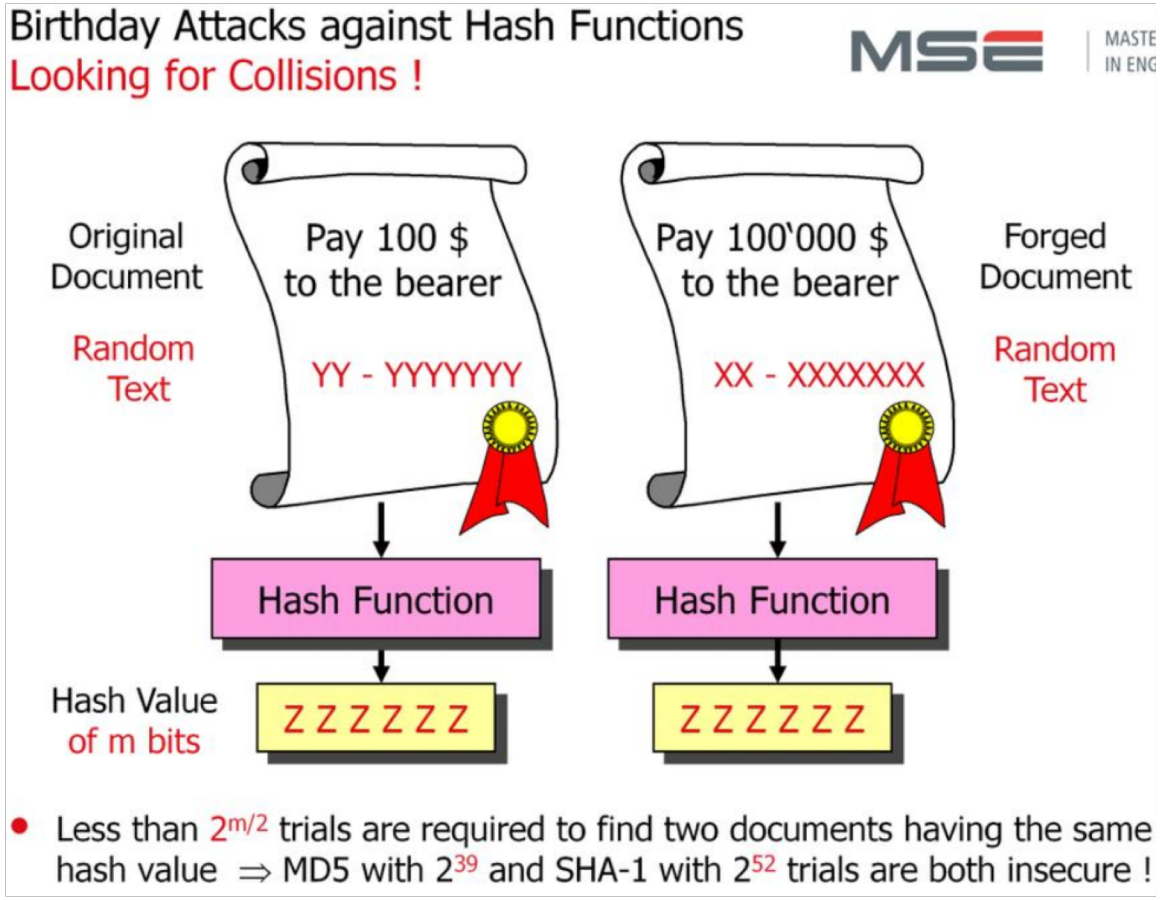
Eavesdropping

- Eavesdropping attacks occur through the interception of network traffic. By eavesdropping, an attacker can obtain passwords, credit card numbers and other confidential information that a user might be sending over the network. Eavesdropping can be passive or active:
  - **Passive eavesdropping** — A hacker detects the information by listening to the message transmission in the network.
  - **Active eavesdropping** — A hacker actively grabs the information by disguising himself as friendly unit and by sending queries to transmitters. This is called probing, scanning or tampering.
- Detecting passive eavesdropping attacks is often more important than spotting active ones, since active attacks requires the attacker to gain knowledge of the friendly units by conducting passive eavesdropping before.
- **Data encryption is the best countermeasure for eavesdropping.**



Cyber Attacks
Birthday

- Birthday attacks are made against hash algorithms that are used to verify the integrity of a message, software or digital signature. A message processed by a hash function produces a message digest (MD) of fixed length, independent of the length of the input message; this MD uniquely characterizes the message. The birthday attack refers to the probability of finding two random messages that generate the same MD when processed by a hash function. If an attacker calculates same MD for his message as the user has, he can safely replace the user's message with his, and the receiver will not be able to detect the replacement even if he compares MDs.



Cyber Attacks

Malware

Unwanted software that is installed in your system without your consent. It can attach itself to legitimate code and propagate; it can lurk in useful applications or replicate itself across the Internet. Here are some of the most common types of malware:

- **Macro Viruses**
- **File infectors**
- **System or boot record infectors**
- **Polymorphic viruses**
- **Stealth viruses**
- **Trojans**
- **Logic bomb**
- **Worms**
- **Droppers**
- **Ransomware**

Takeaway Notes

Measures to mitigate threats vary, but security basics stay the same:

- Keep your systems and anti-virus databases up to date,
- Train your employees,
- Configure your firewall to whitelist only the specific ports and hosts you need,
- Keep your passwords strong,
- Use a least-privilege model in your IT environment,
- Make regular backups,
- And, continuously audit your IT systems for suspicious activity.

Small group Exercise

Simulation of a corporate security attack

- As a CISO you learned that some hackers have encrypted you customer data base and you don’t have access to the system anymore. They want you to pay a ransom of 2M€ to give back the Key. The situation is critical, the case is public and you have to take a quick decision in 24h.

Small group Exercise

Simulation of a corporate security attack

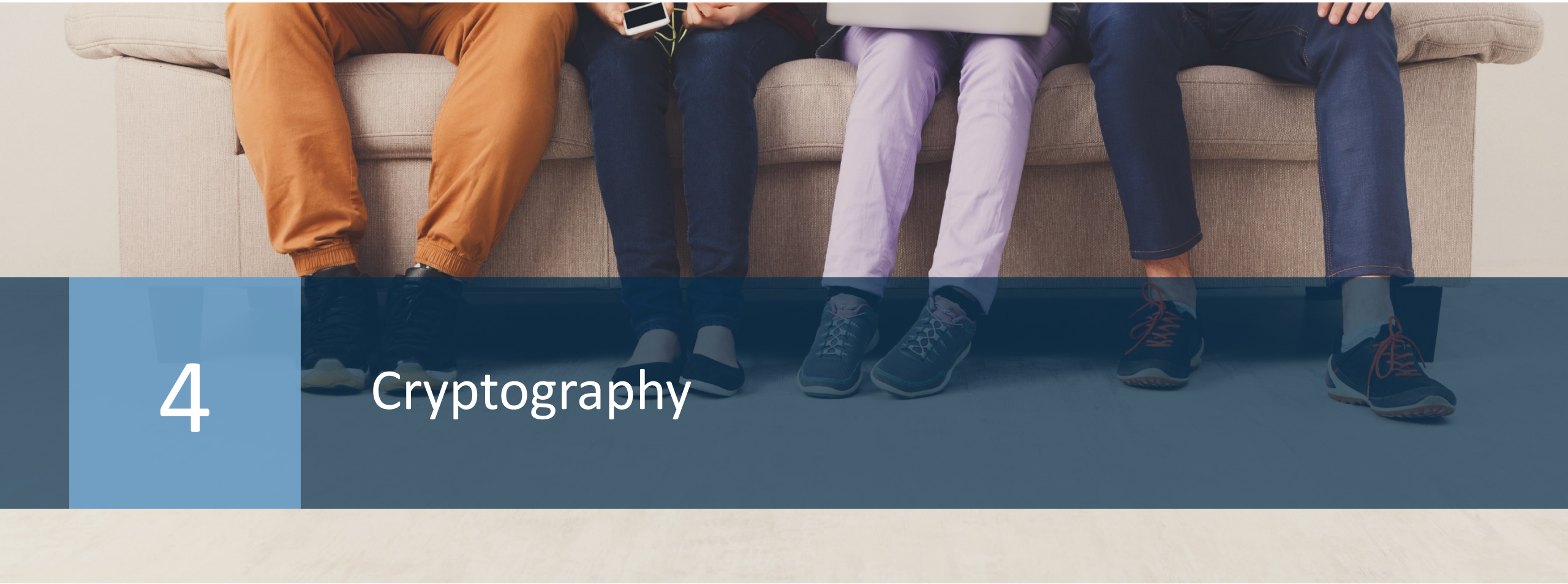
Put yourselves in a group of 4 people and assess the following questions:

- Who’s in charge of the investigation?
- Who’s part of the incident response team?
- What document do you use to guide you?
- What role does every group provide? IT, HR, Legal, Financer, communication , etc. ?
- Do you ask for outside support?
- Do you pay the ransom or not, why?

Man in the Middle attack- Video

There are a few dos and don’ts when it comes to ransomware.

- **Do not pay the ransom.** It only encourages and funds these attackers. Even if the ransom is paid, there is no guarantee that you will be able to regain access to your files.
- **Restore any impacted files from a known good backup**. Restoration of your files from a backup is the fastest way to regain access to your data.
- **Do not provide personal information** when answering an email, unsolicited phone call, text message or instant message. Phishers will try to trick employees into installing malware, or gain intelligence for attacks by claiming to be from IT. Be sure to contact your IT department if you or your coworkers receive suspicious calls.
- **Use reputable antivirus software and a firewall**. Maintaining a strong firewall and keeping your security software up to date are critical. It’s important to use antivirus software from a reputable company because of all the fake software out there.
- **Do employ content scanning and filtering on your mail servers**. Inbound e-mails should be scanned for known threats and should block any attachment types that could pose a threat.
- **Do make sure that all systems and software are up-to-date with relevant patches**. Exploit kits hosted on compromised websites are commonly used to spread malware. Regular patching of vulnerable software is necessary to help prevent infection.
- If traveling, alert your IT department beforehand, especially if you’re going to be using public wireless Internet. Make sure you use a **trustworthy Virtual Private Network (VPN) when accessing public Wi-Fi like Norton Secure VPN.**



4 Cryptography

Security of Information Systems

Cryptography

Cryptography
Definition

Cryptography is the science of using mathematics to encrypt and decrypt data.

Phil Zimmermann

Cryptography is the art and science of keeping messages secure.

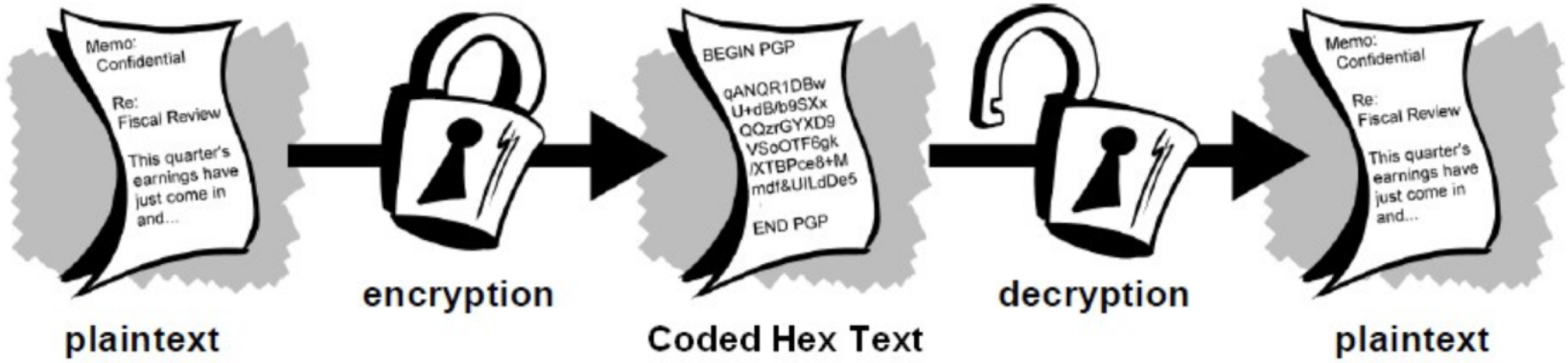
Bruce Schneier

The art and science of concealing the messages to introduce secrecy in information security is recognized as cryptography.

Cryptography
Terminologies

A message is **plaintext** (sometimes called **cleartext**). The process of disguising a message in such a way as to hide its substance is **encryption**. An encrypted message is **ciphertext**. The process of turning ciphertext back into plaintext is **decryption**.

A **cipher** (or **cypher**) is an algorithm for performing encryption or decryption—a series of well-defined steps that can be followed as a procedure.



Cryptography
Terminologies

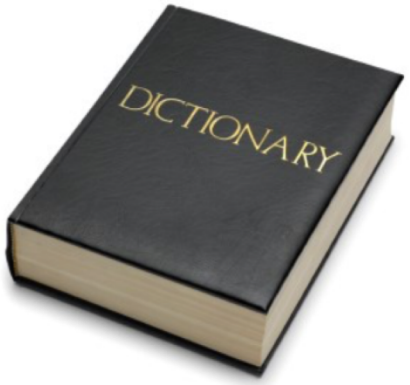
A **cryptosystem** is an implementation of cryptographic techniques and their accompanying infrastructure to provide information security services. A cryptosystem is also referred to as a cipher system. The various components of a basic cryptosystem are as follows −

- Plaintext
- Encryption Algorithm
- Ciphertext
- Decryption Algorithm
- Encryption Key
- Decryption Key

Cryptography
Terminologies

While **cryptography** is the science of securing data, **cryptanalysis** is the science of analyzing and breaking secure communication. Classical cryptanalysis involves an interesting combination of analytical reasoning, application of mathematical tools, pattern finding, patience, determination, and luck. **Cryptanalysts** are also called attackers.

Cryptology embraces both cryptography and cryptanalysis.



Cryptography
History

As civilizations evolved, human beings got organized in tribes, groups, and kingdoms.

This led to the emergence of ideas such as power, battles, supremacy, and politics.

These ideas further fueled the natural need of people to communicate secretly with selective recipient which in turn ensured the continuous evolution of cryptography as well.

The roots of cryptography are found in Roman and Egyptian civilizations.

Cryptography
History

Hieroglyph

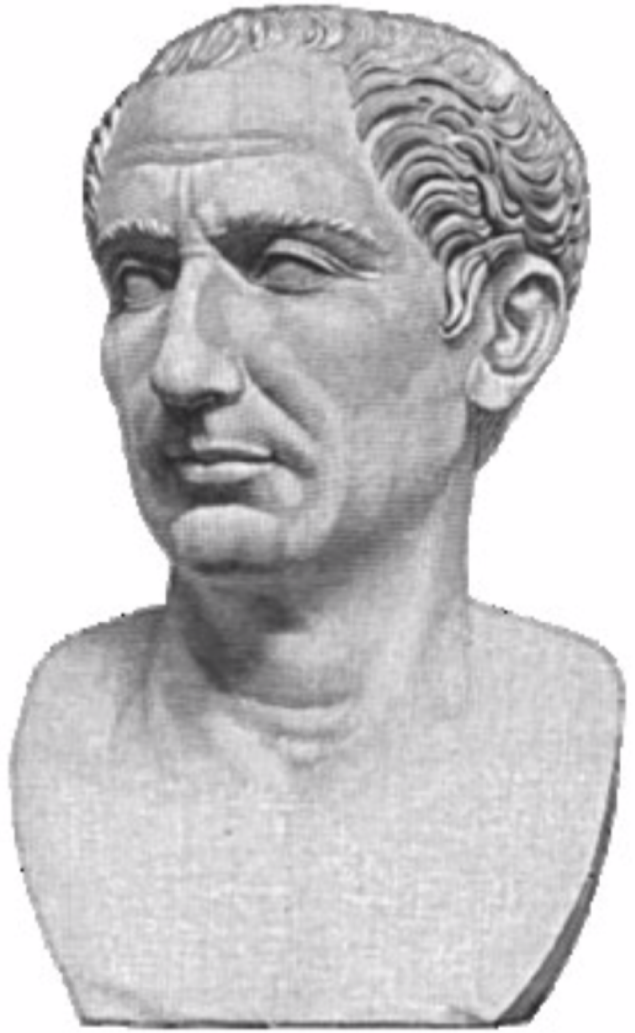
The first known evidence of cryptography can be traced to the use of ‘hieroglyph’. Some 4000 years ago, the Egyptians used to communicate by messages written in hieroglyph.

Cryptography
History

Caesar Shift Cipher

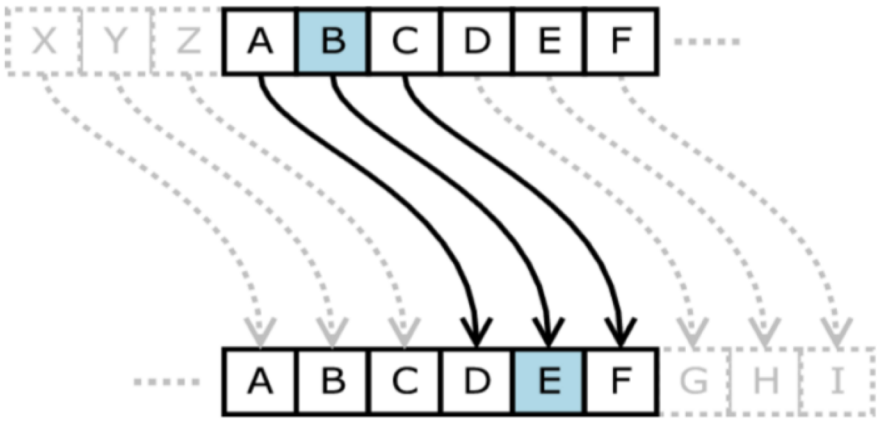
Caesar Shift Cipher, relies on shifting the letters of a message by an agreed number (three was a common choice), the recipient of this message would then shift the letters back by the same number and obtain the original message.

The Caesar cipher is named after Julius Caesar , who used it with a shift of three to protect messages of military significance.

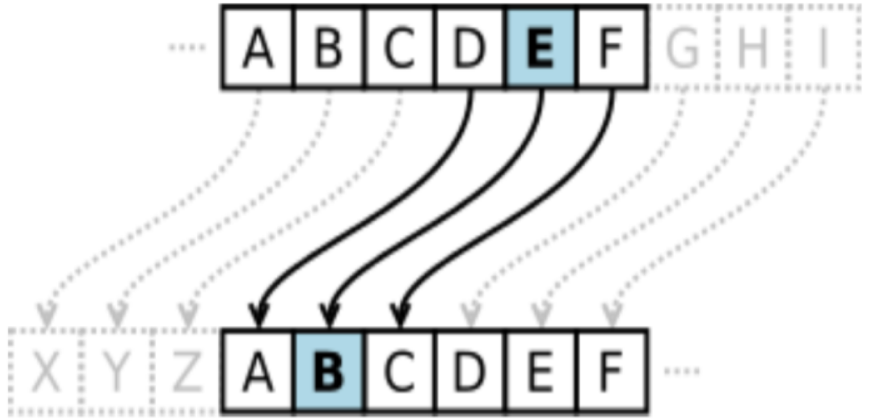


Cryptography
History

Caesar Shift Cipher



Encryption



Decryption

PLAINTEXT : internet society ghana chapter

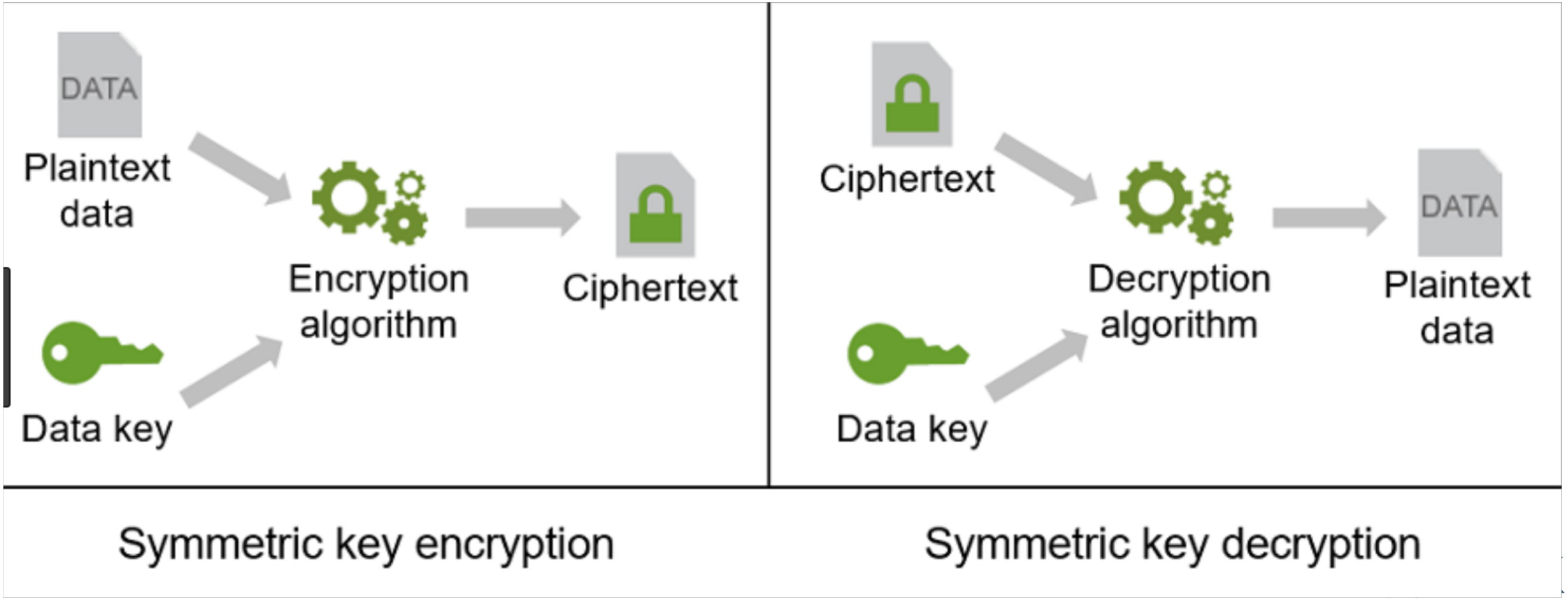
CYPHERTEXT : lqwhuqhw vrflhwb jkdqd fkdswhu

Symmetric Key Cryptography

- Also known as Secret Key Cryptography or Conventional Cryptography, Symmetric Key Cryptography is an encryption system in which the sender and receiver of a message share a single, common key that is used to encrypt and decrypt the message.
- The Algorithm use is also known as a secret key algorithm or sometimes called a symmetric algorithm
- A key is a piece of information (a parameter) that determines the functional output of a cryptographic algorithm or cipher.

Symmetric Key Cryptography

The key for encrypting and decrypting the file had to be known to all the recipients. Else, the message could not be decrypted by conventional means.



Symmetric Key Cryptography - Examples

Data Encryption Standard (DES)

- The Data Encryption Standard was published in 1977 by the US National Bureau of Standards.
  DES uses a 56 bit key and maps a 64 bit input block of plaintext onto a 64 bit output block of ciphertext.
  56 bits is a rather small key for today's computing power.

Triple DES

- Triple DES was the answer to many of the shortcomings of DES. Since it is based on the DES algorithm, it is very easy to modify existing software to use Triple DES. It also has the advantage of proven reliability and a longer key length that eliminates many of the shortcut attacks that can be used to reduce the amount of time it takes to break DES.

Symmetric Key Cryptography - Examples

Advanced Encryption Standard (AES) (RFC3602)

- Advanced Encryption Standard (AES) is an encryption standard adopted by the U.S. government. The standard comprises three block ciphers, AES-128, AES-192 and AES-256, adopted from a larger collection originally published as Rijndael.
- Each AES cipher has a 128-bit block size, with key sizes of 128, 192 and 256 bits, respectively. The AES ciphers have been analyzed extensively and are now used worldwide, as was the case with its predecessor, the Data Encryption Standard (DES).
- Other examples:

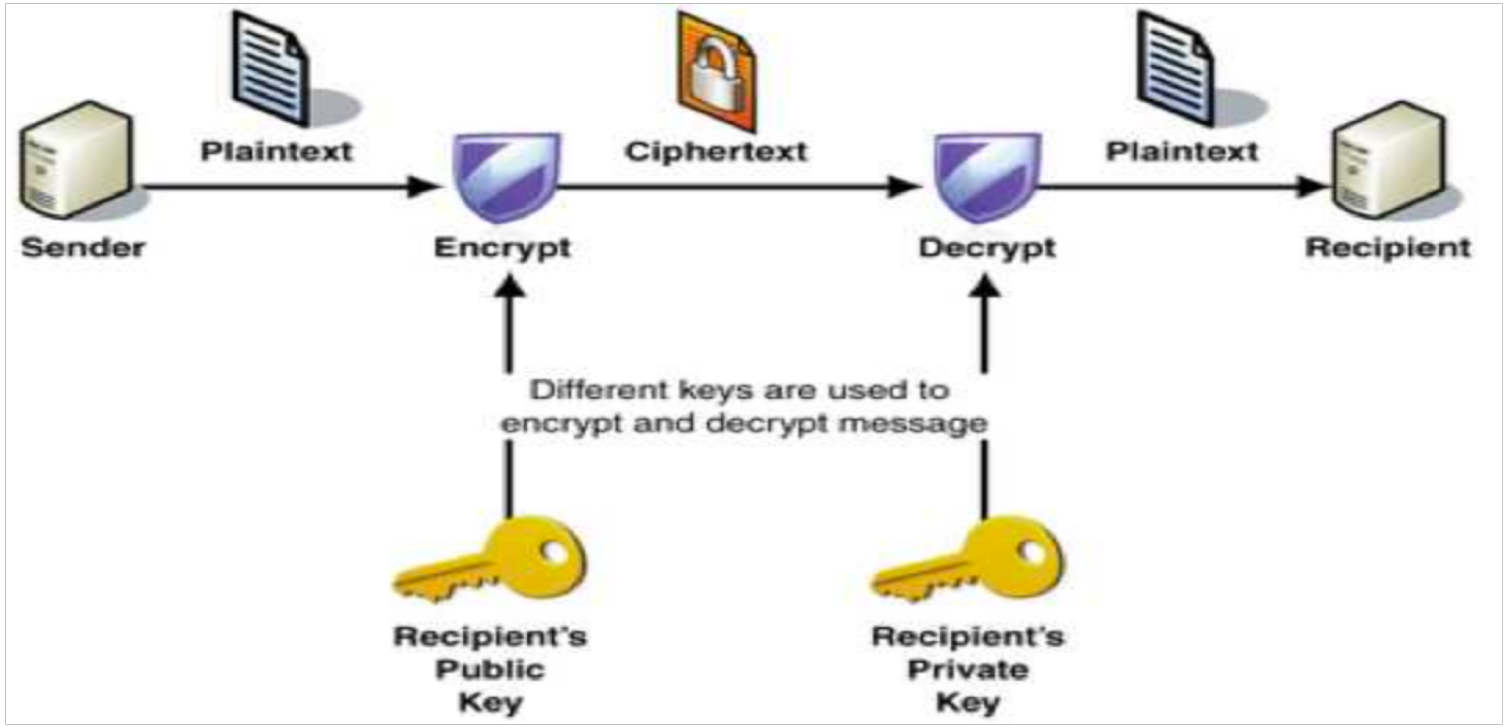
Lucifer	-	Madryga
FEAL	-	REDOC
LOKI	-	GOST
CAST	-	Blowfish
Safer	-	Crab
RC5	-	

Limitation of Symmetric Key Cryptography ` Key Management

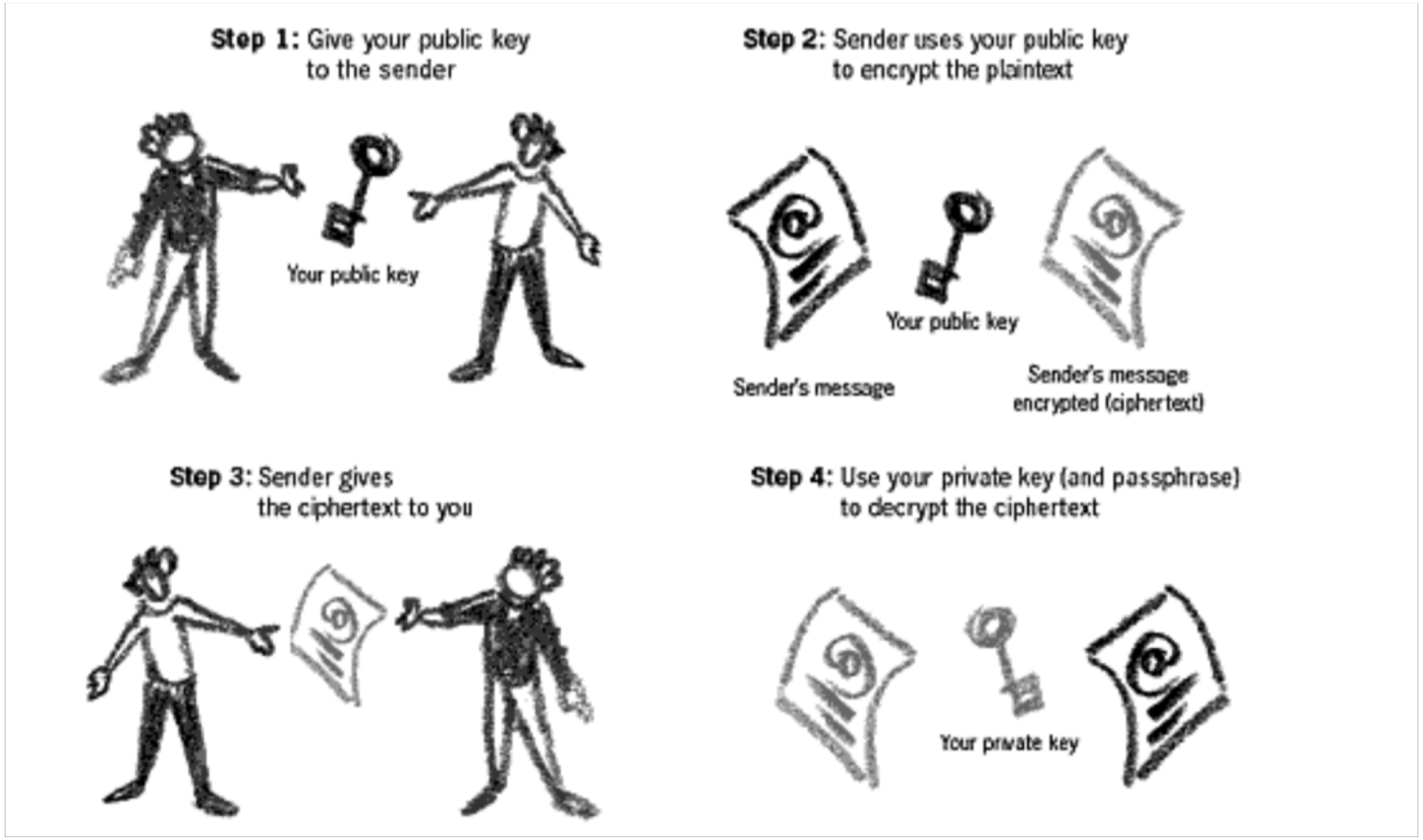
- Symmetric-key systems are simpler and faster; their main drawback is that the two parties must somehow exchange the key in a secure way and keep it secure after that.
- Key Management caused nightmare for the parties using the symmetric key cryptography. They were worried about how to get the keys safely and securely across to all users so that the decryption of the message would be possible. This gave the chance for third parties to intercept the keys in transit to decode the top-secret messages. Thus, if the key was compromised, the entire coding system was compromised and a “Secret” would no longer remain a “Secret”.
- **This is why the “Public Key Cryptography” came into existence.**

Asymmetric Key Cryptography

- Asymmetric cryptography , also known as Public-key cryptography, refers to a cryptographic algorithm which requires two separate keys, one of which is private and one of which is public. The public key is used to encrypt the message and the private one is used to decrypt the message.



Asymmetric Key Cryptography



Asymmetric Key Cryptography

- Public Key Cryptography is a very advanced form of cryptography.
- Officially, it was invented by Whitfield Diffie and Martin Hellman in 1975.
- The basic technique of public key cryptography was first discovered in 1973 by the British Clifford Cocks of Communications-Electronics Security Group (CESG) of (Government Communications Headquarters - GCHQ) but this was a secret until 1997.

Asymmetric Key Cryptography - Examples

Digital Signature Standard (DSS)

- Digital Signature Standard (DSS) is the digital signature algorithm (DSA) developed by the U.S. National Security Agency (NSA) to generate a digital signature for the authentication of electronic documents. DSS was put forth by the National Institute of Standards and Technology (NIST) in 1994, and has become the United States government standard for authentication of electronic documents. DSS is specified in Federal Information Processing Standard (FIPS) 186.

Algorithm - RSA

- RSA (Rivest, Shamir and Adleman who first publicly described it in 1977) is an algorithm for public-key cryptography. It is the first algorithm known to be suitable for signing as well as encryption, and one of the first great advances in public key cryptography.
- RSA is widely used in electronic commerce protocols, and is believed to be secure given sufficiently long keys and the use of up-to-date implementations.

Asymmetric Key Cryptography - Examples

RSA Cryptanalysis

- Rivest, Shamir, and Adelman placed a challenge in Martin Gardner's column in Scientific American (journal) in which the readers were invited to crack.
- C=114,381,625,757,888,867,669,235,779,976,146,612,010,218,296,721,242,362,562,561,842,935,706,935 ,245,733,897,830,597,123,563,958,705,058,989,075,147,599,290,026,879,543,541
- This was solved in April 26, 1994, cracked by an international effort via the internet with the use of 1600 workstations, mainframes, and supercomputers attacked the number for eight months before finding its Public key and its private key.
  Encryption key = **9007**
  - **The message "first solver wins one hundred dollars".**
- In 2009, Benjamin Moody factored an RSA-512 bit key in 73 days using only public software. Of course, the RSA algorithm is safe, as it would be incredibly difficult to gather up such international participation to commit malicious acts. In practice, RSA keys are typically 1024 to 4096 bits long. Some experts believe that 1024-bit keys may become breakable in the near future or may already be breakable by a sufficiently well-funded attacker,

Asymmetric Key Cryptography - Examples

ElGamal

- ElGamal is a public key method that is used in both encryption and digital signing.
- The encryption algorithm is similar in nature to the Diffie-Hellman key agreement protocol It is used in many applications and uses discrete logarithms.
- ElGamal encryption is used in the free GNU Privacy Guard software

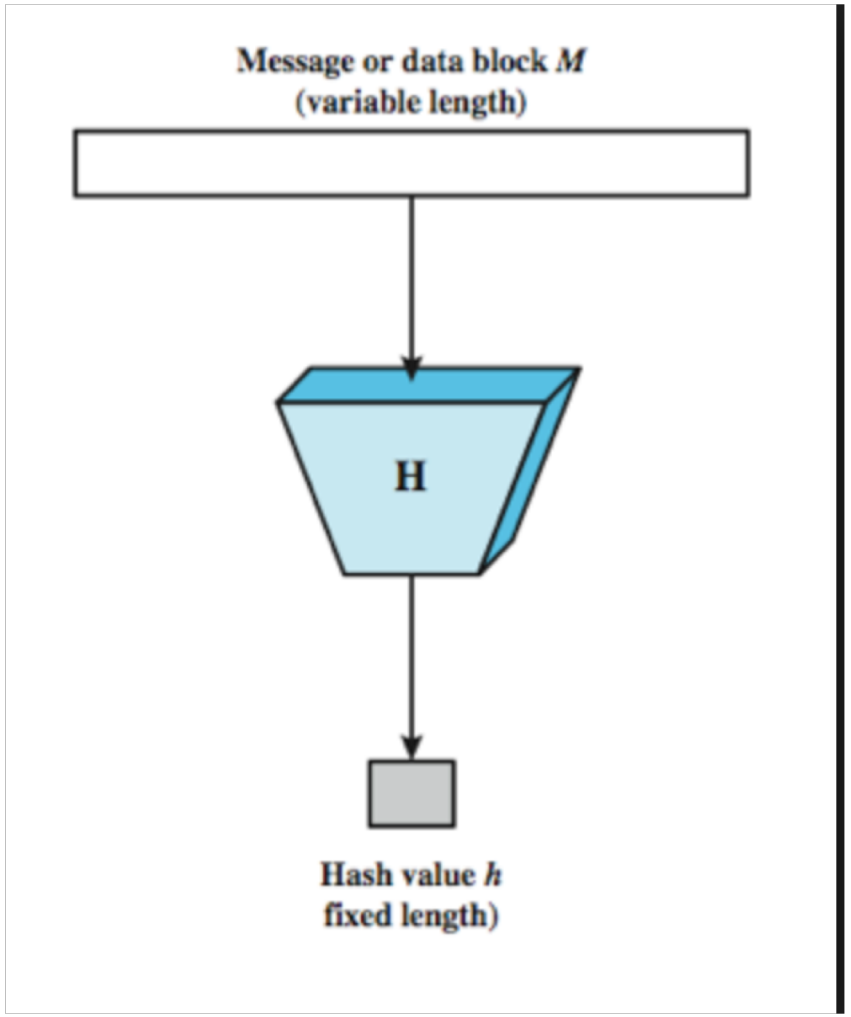
Public Key VS Symmetric Key

Symmetric key	Public key
Two parties MUST trust each other	Two parties DO NOT need to trust each other
Both share same key (or one key is computable from the other)	Two separate keys: a public and a private key
Typically faster	Typically slower
Examples: DES, IDEA, RC5, CAST, AES, ...	Examples: RSA, ElGamal Encryption, ECC...

Hash Functions

What is Hash Function

- A cryptographic hash function is a hash function that takes an arbitrary block of data and returns a fixed-size bit string, the cryptographic hash value, such that any (accidental or intentional) change to the data will (with very high probability) change the hash value. The data to be encoded are often called the message, and the hash value is sometimes called the message digest or simply digest.



Hash Functions

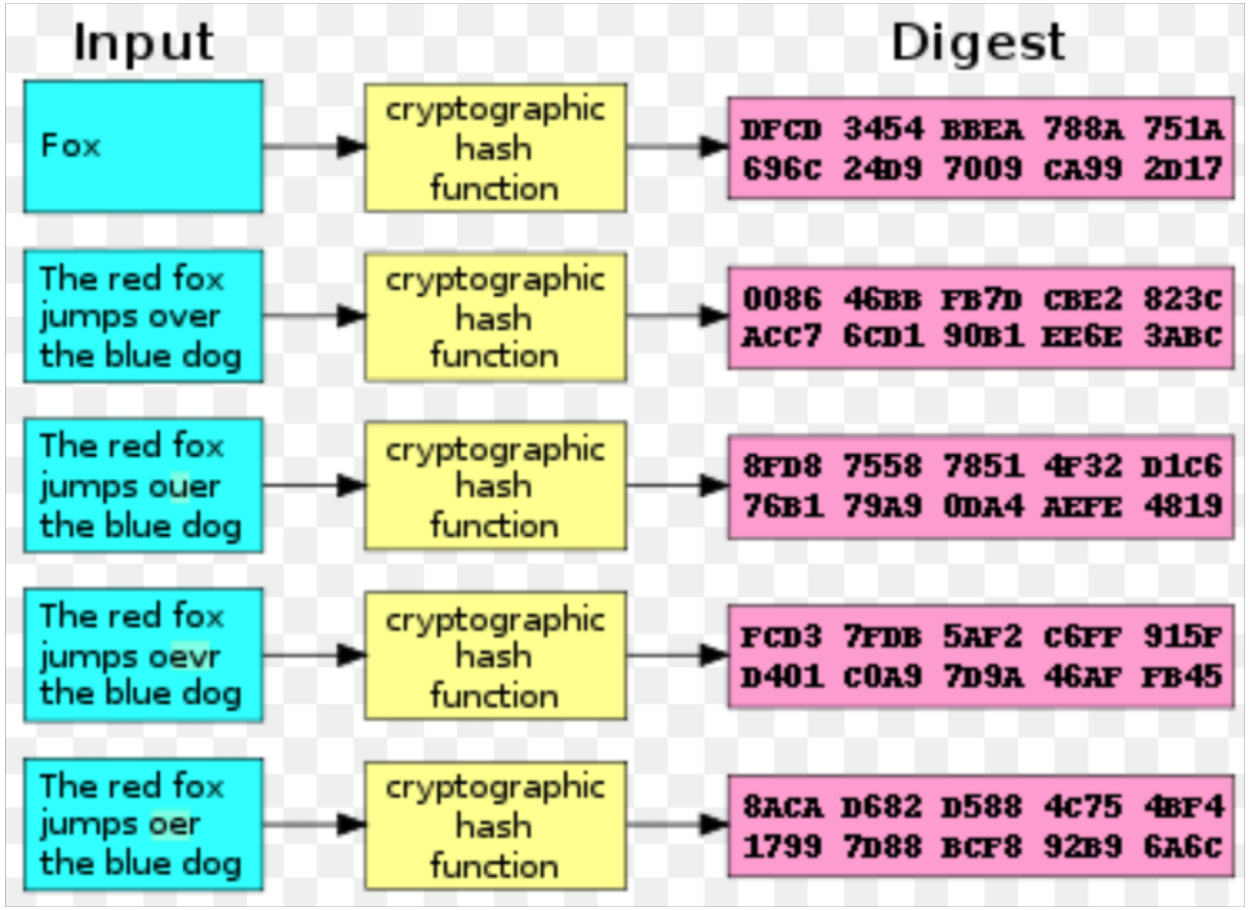
What is Hash Function

The ideal cryptographic hash function has four main properties:

- it is easy to compute the hash value for any given message
- it is infeasible to generate a message that has a given hash
- it is infeasible to modify a message without changing the hash
- it is infeasible to find two different messages with the same hash.

Hash Functions

What is Hash Function



Hash Functions -Examples

Snefru		Ralph Merkle	
N-Hash		Nippon T.T.	
Message Digest	MD2	(RFC 1115)	B. Kaliski
	MD4	(RFC1320)	Ron Rivest
	MD5	(RFC 1321)	Ron Rivest
	MD6		
SHA1			
SHA2			

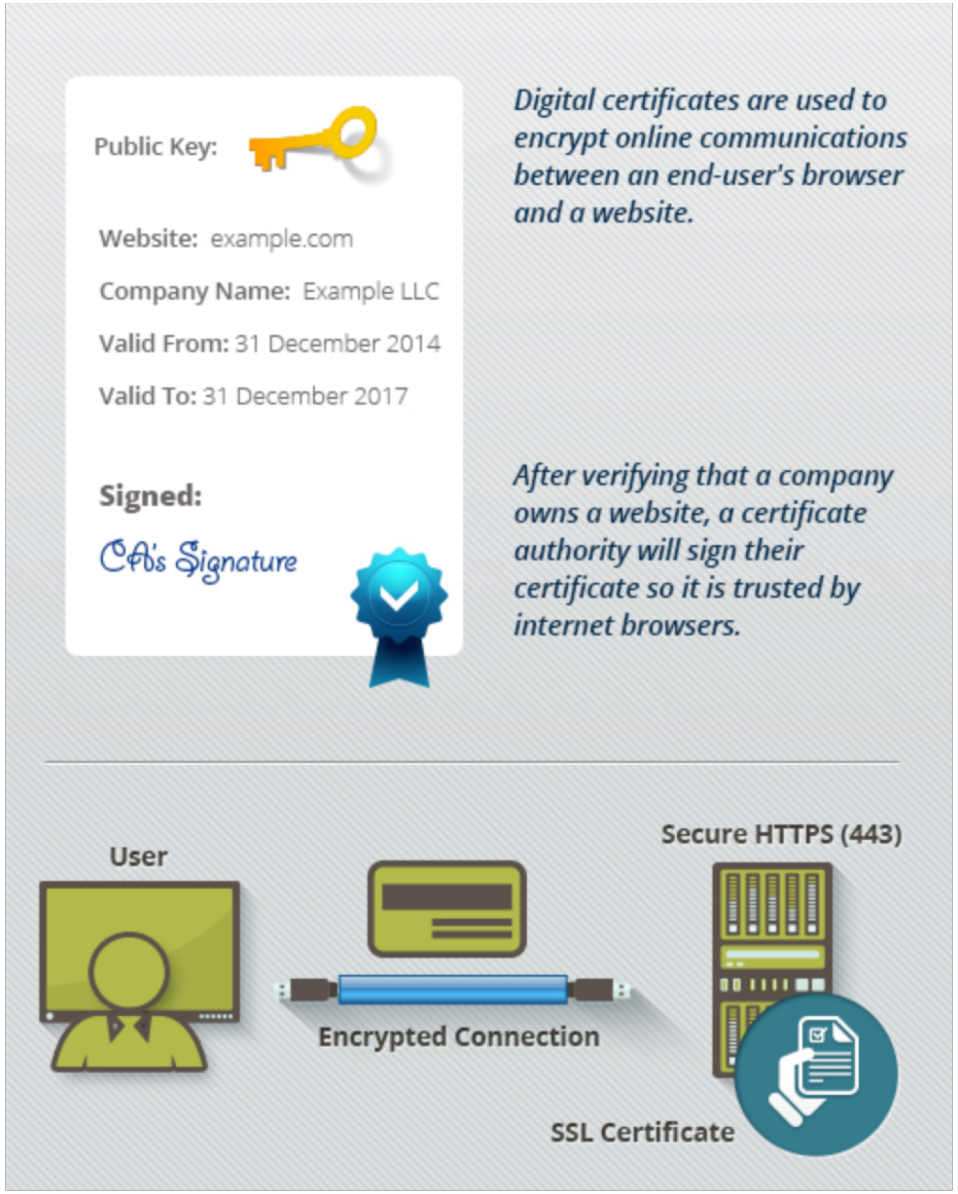
- In March 2005 Xiaoyun Wang and Hongbo Yu of Shandong University in China created a pair of files that share the same MD5 checksum hence prove that there is a collusion when using MD5

Hash Functions -Examples

- The Secure Hash Algorithm (SHA) hash functions are a set of cryptographic hash functions designed by the National Security Agency (NSA) and published by the NIST as a U.S. Federal Information Processing Standard.
- SHA stands for Secure Hash Algorithm.
  Because of the successful attacks on MD5, SHA-0 and theoretical attacks on SHA-1, NIST perceived a need for an alternative, dissimilar cryptographic hash, which became SHA-3.
- In October 2012, the National Institute of Standards and Technology (NIST) choses the **Keccak** algorithm as the new SHA-3 standard.

Digital certificates

- A *digital certificate* is a digital document that *certifies* that a certain public key is owned by a particular user. This document is signed by a third party called the certificate authority (or CA)
- Of course, the certificate is encoded in a digital format. The important thing to remember is that the certificate is signed by a third party (the certificate authority) which does not itself take place in the secure conversation. The signature is actually a digital signature generated with the CA's private key. Therefore, we can verify the integrity of the certificate using the CA's public key.



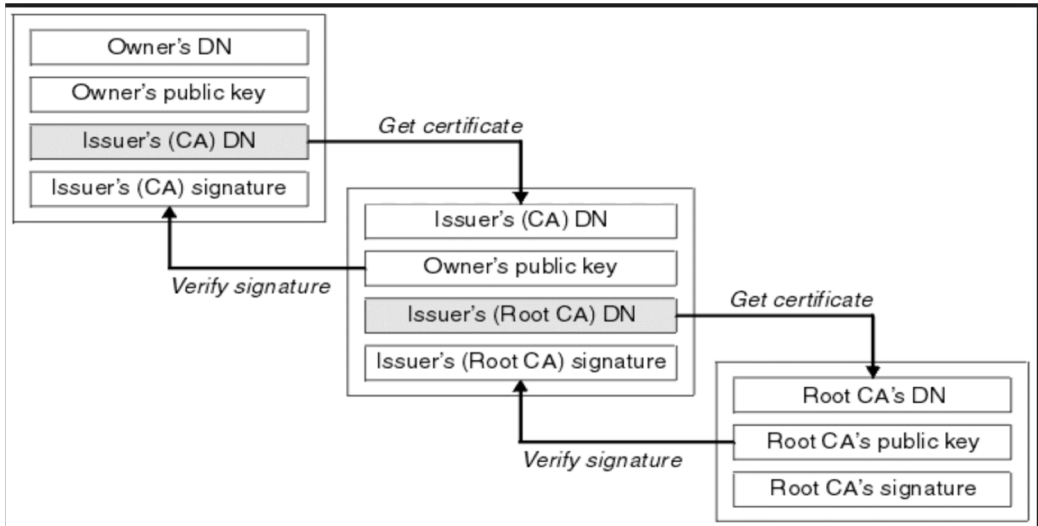
Digital certificates

- *Each digital certificate has its own digital signature, signed (encrypted) by the private key of the certificate authority*
- *Provides message integrity so that an impostor cannot change the name field in the digital certificate to its own*
- *Certificate authorities may revoke digital certificates before the expiration date listed in the digital certificate*
  - *Revoked certificate ID numbers are placed in a certificate revocation list (CRL)*
  - *Verifier must check with the certificate authority to determine if a digital certificate is on the CRL*
- ***Without the CRL check, digital certificates do not support authentication***

X509 certificate with id

X509v3 extensions:
X509v3 Basic Constraints: critical
CA:TRUE
X509v3 Key Usage: critical
Digital Signature, Non Repudiation, Key Encipherment, Key Agreement, Certificate Sign
Netscape Cert Type:
SSL Client, S/MIME
X509v3 Subject Key Identifier:
45:DC:F9:10:33:C0:45:28:EA:90:6E:83:73:06:6F:51:21:89:13:DD
X509v3 Authority Key Identifier:
keyid:45:DC:F9:10:33:C0:45:28:EA:90:6E:83:73:06:6F:51:21:89:13:DD

X509v3 Subject Alternative Name:
URI:http://bblfish.net/people/henry/card#me
Signature Algorithm: dsaWithSHA1
30:2c:02:14:78:69:1e:4f:7d:37:36:a5:8f:37:30:58:18:5a:
f6:10:e9:13:a4:ec:02:14:03:93:42:3b:c0:d4:33:63:ae:2f:
eb:8c:11:08:1c:aa:93:7d:71:01



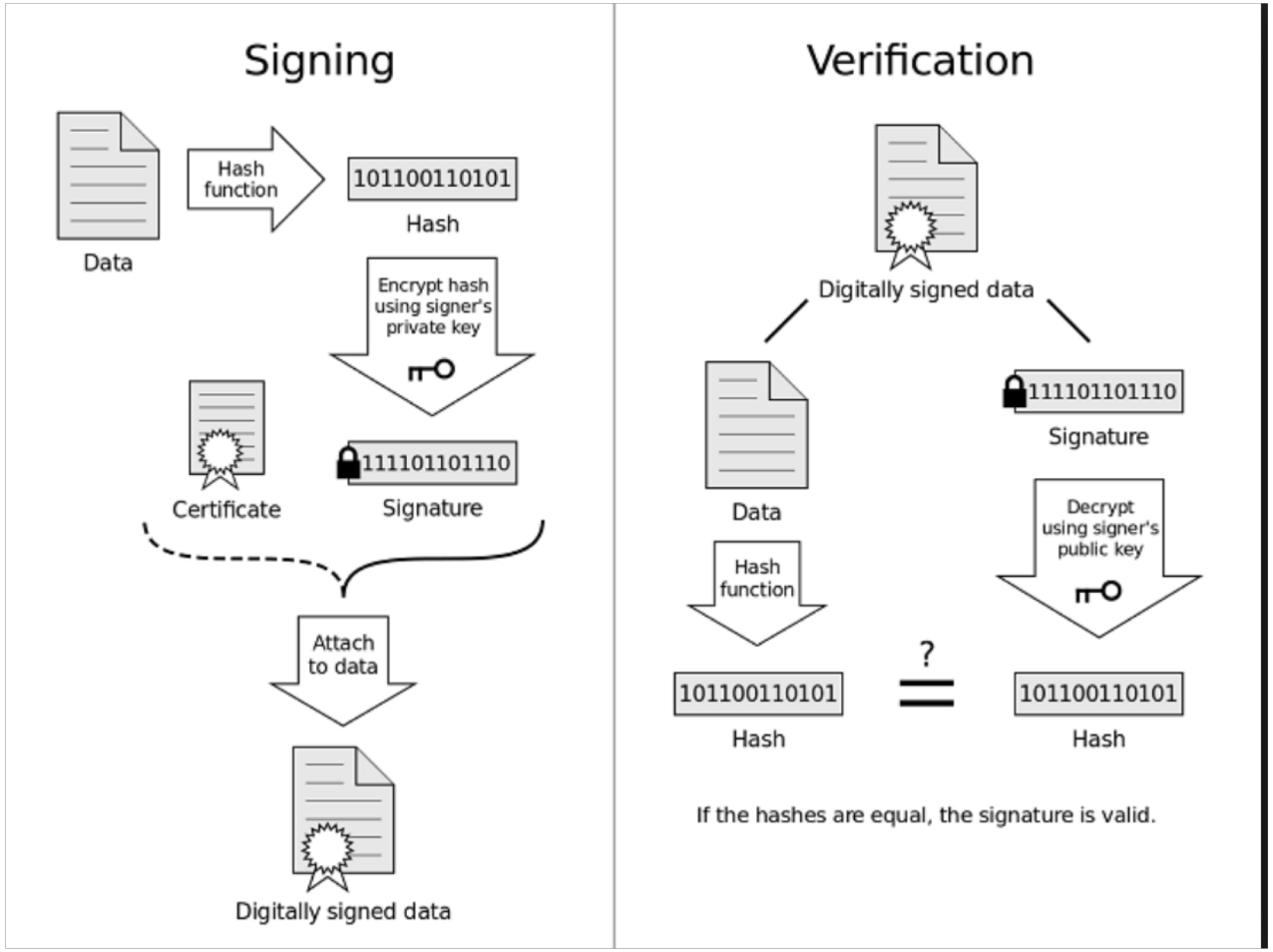
Asymmetric Key Cryptography
Authentication in public-key systems

Having a certificate to prove to everyone else that your public key is really, truly, honestly yours allows us to conquer the third pillar of a secure conversation: authentication. If you digitally sign your message with your private key, and send the receiver a copy of your certificate, he can know for sure that the message was sent by *you* (because only your public key can decrypt the digital signature... and the certificate assures that the public key the receiver uses is yours and no one else's)

Asymmetric Key Cryptography

Digital Integrity

Integrity is guaranteed in public-key systems by using *digital signatures*. A digital signature is a piece of data which is attached to a message and which can be used to find out if the message was tampered with during the conversation (e.g. through the intervention of a malicious user)

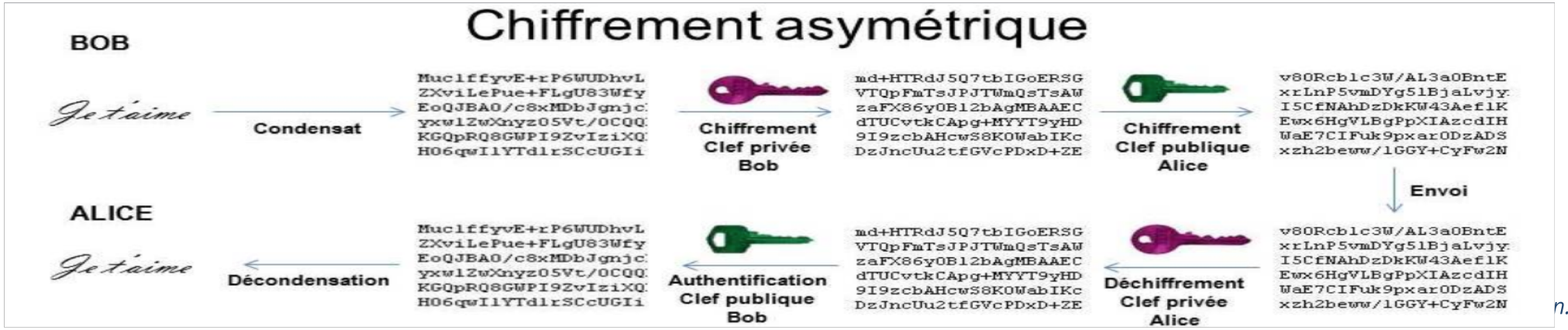


Authentication mechanism – Example 1/2

- A major disadvantage of using asymmetric encryption mechanisms is the fact that the public key is distributed to all people: Bob, Carole and Alice wishing to exchange data confidentially. Therefore, when the person with the private key, Alice, decrypts the encrypted data, he has no way to verify with certainty the source of these data (Bob or Carole): we are talking about **authentication problems**.
- In order to solve this problem, **authentication mechanisms** are used to guarantee the origin of the encrypted information. These mechanisms are also based on asymmetric encryption, the principle of which is as follows: Bob wants to send encrypted data to Alice by guaranteeing that he is the sender.

Authentication mechanism – Example 2/2

- Bob creates a pair of asymmetric keys: he defines a private key and freely distributes his public key (notably to Alice)
- Alice creates a pair of asymmetric keys: she defines a private key and freely diffuses her public key (in particular to Bob)
- Bob makes a condensate of his message "in clear" then encrypts this condensate with his private key
- Bob re-encrypts his already encrypted message with Alice's public key
- Bob sends the encrypted message to Alice
- Alice receives Bob's encrypted message (but a third party, for example Eve, could intercept)
- Alice is able to decrypt the message with her private key. Then she obtains a readable message in the form of condensate. Eve, meanwhile, can not decrypt Bob's intercepted message because she does not know Alice's private key. On the other hand Alice is not sure that the decrypted message (in the form of condensate) is that of Bob
- To read it, Alice will then decipher the condensate (encrypted with Bob's private key) with Bob's public key. By this means, Alice can be certain that Bob is the sender. Otherwise, the message is indecipherable and it may be assumed that a malicious person has attempted to send a message posing as Bob
- This authentication method uses the specificity of asymmetric key pairs: if we encrypt a message using the public key, then we can decipher the message using the private key; the opposite is also possible: **if we encrypt using the private key then we can decrypt using the public key.**



Questions ?