Network Architecture and Security

ECAM STRASBOURG-EUROPE 2018-2019

LECTURER: ROMAIN ORHAND (ROMAIN.ORHAND@ECAM-STRASBOURG.EU)

Let's start with a riddle

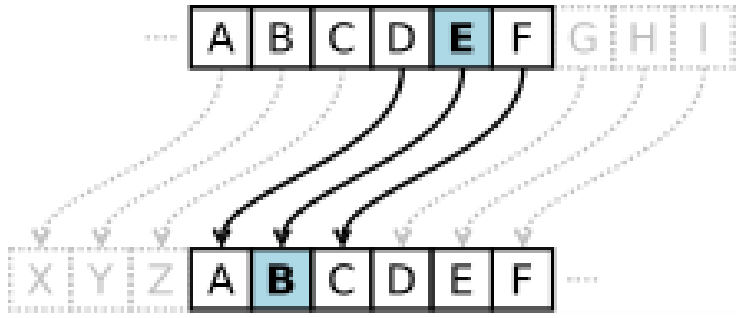
Are you able to guess what’s behind the following words ?

RSNOD ROZKS XRKBY VN

Security and Cryptography

Caesar's Code

It is a type of **substitution cipher** in which each letter in the plaintext is replaced by a letter **some fixed number of positions down or up** the alphabet.



Caesar's Code

According the previous example RSNOD ROZKS XRKBY VN

The shift is **about 10** and so, you should have decrypt it by

"Hide the pain Harold"

Symmetric encryption

All is about a **key** which is shared by few people and an algorithm (function)

Asymmetric encryption

Two goals :

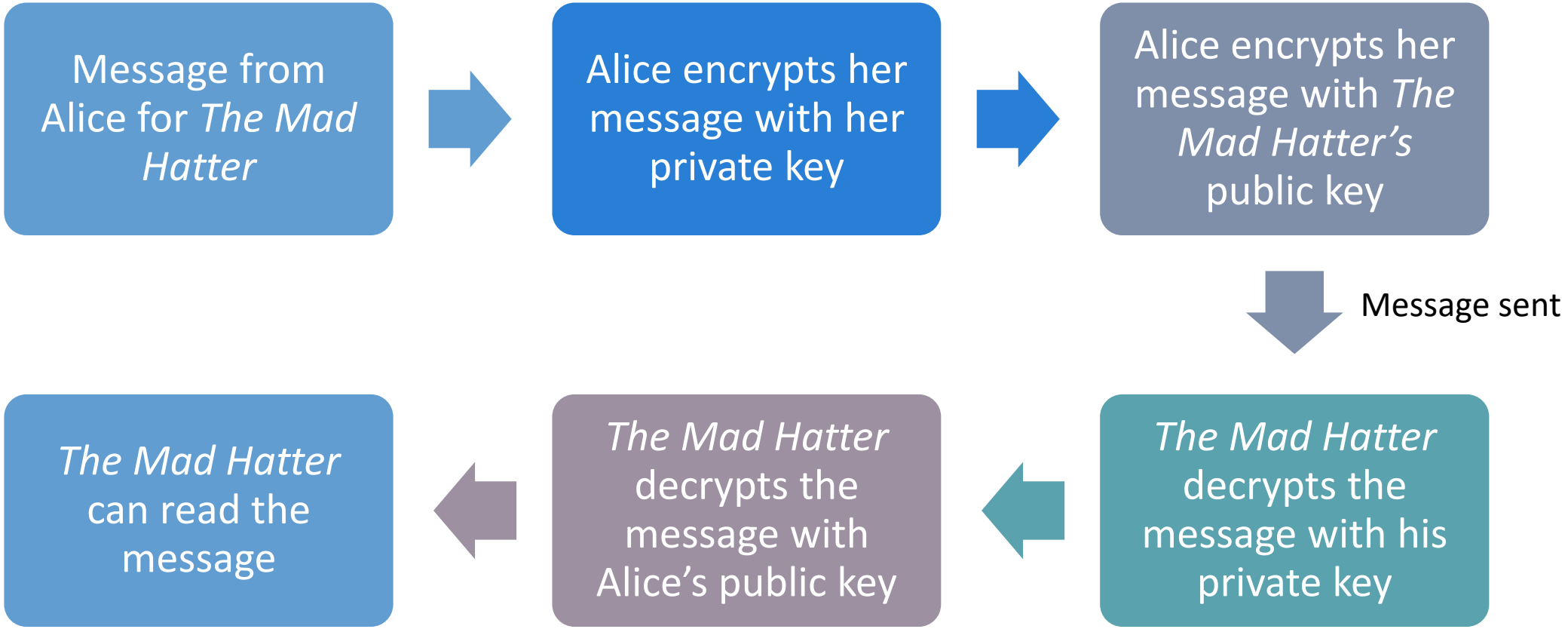
- Ensure the authenticity of the sender
- Crypt and decrypt the messages sent

Asymmetric encryption

We need :

- A **private key** which is also called the decryption key ;
- A **public key** which is also called the encryption key;
- A **one-way function** with a **secret breach**.

Asymmetric encryption



A example of use of asymmetric encryption : HTTPS

Remember : HTTP is an application protocol for distributed, collaborative, hypermedia information systems.

HTTPS is an extension of HTTP for **secure** communication.

A example of use of asymmetric encryption : HTTPS

You can protect yourselves from :

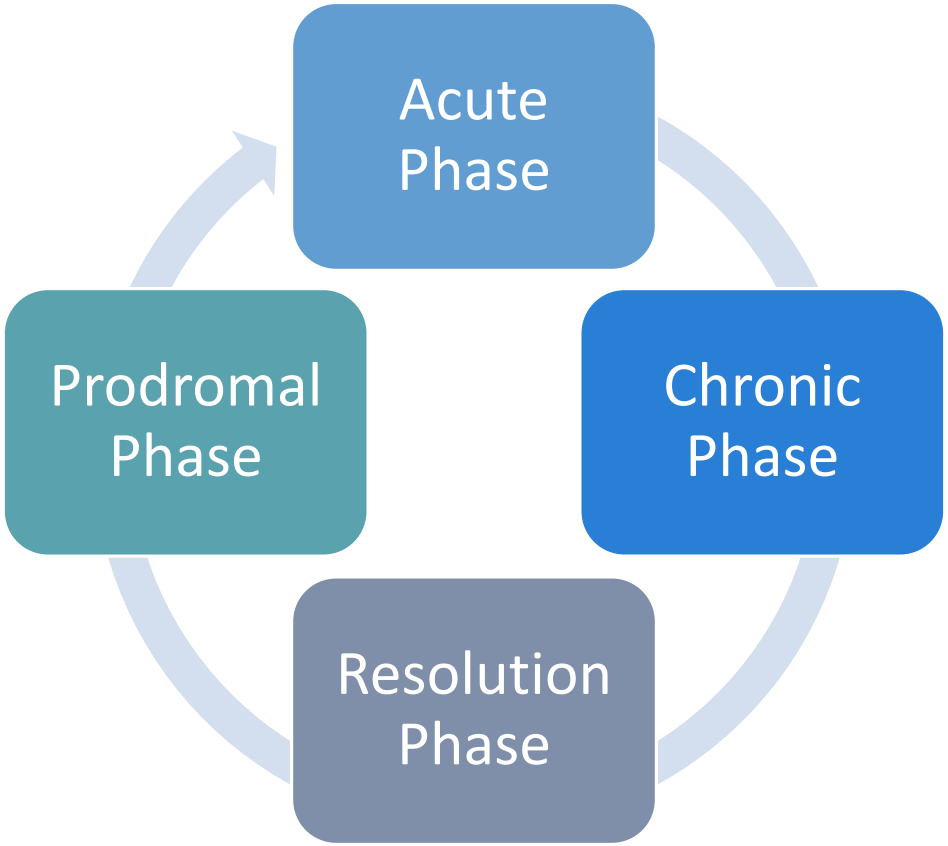
- **Eavesdropping** ;
- **Man-in-the-middle attack** thanks to *ARP Spoofing* or *DNS poisoning* for example.

Some methodology

Let’s say that you’re attacked or you have detected something abnormal.

What would you do ?

The phase of crisis management



Let’s see an example

It’s the morning, the sun is shinning.

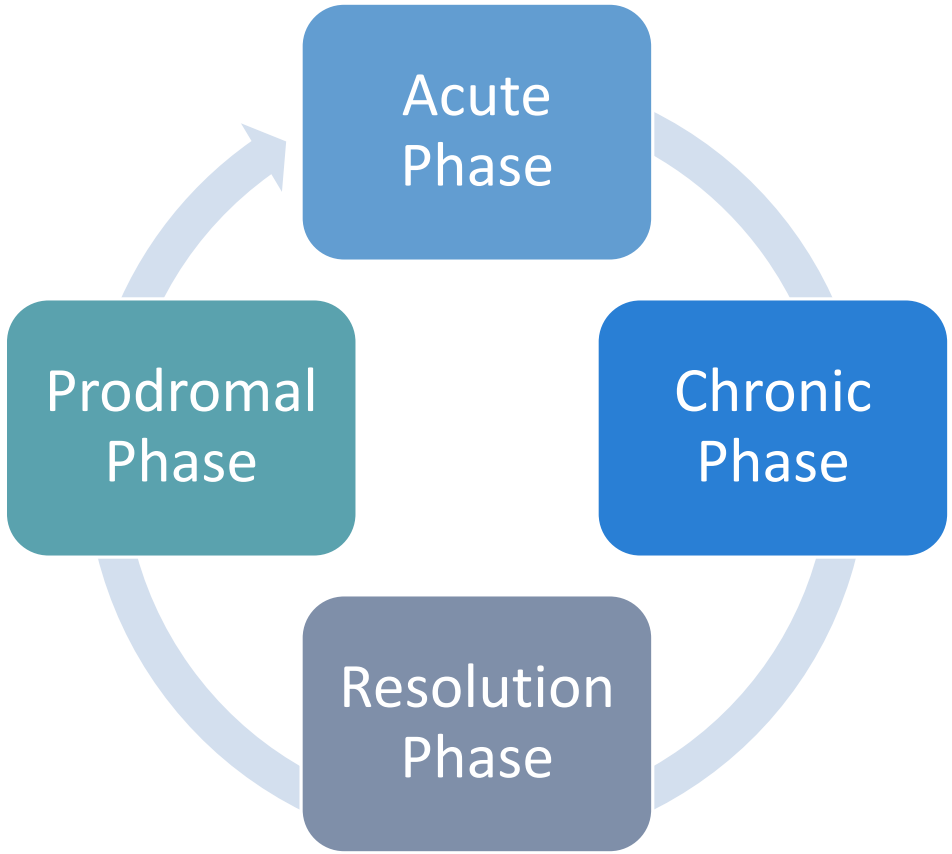
You want to read your emails.

But your connection is abnormally slow.

So you decide to check the server status.

And you find a process that executes with high CPU load.

After further investigations, this process is a spyware …

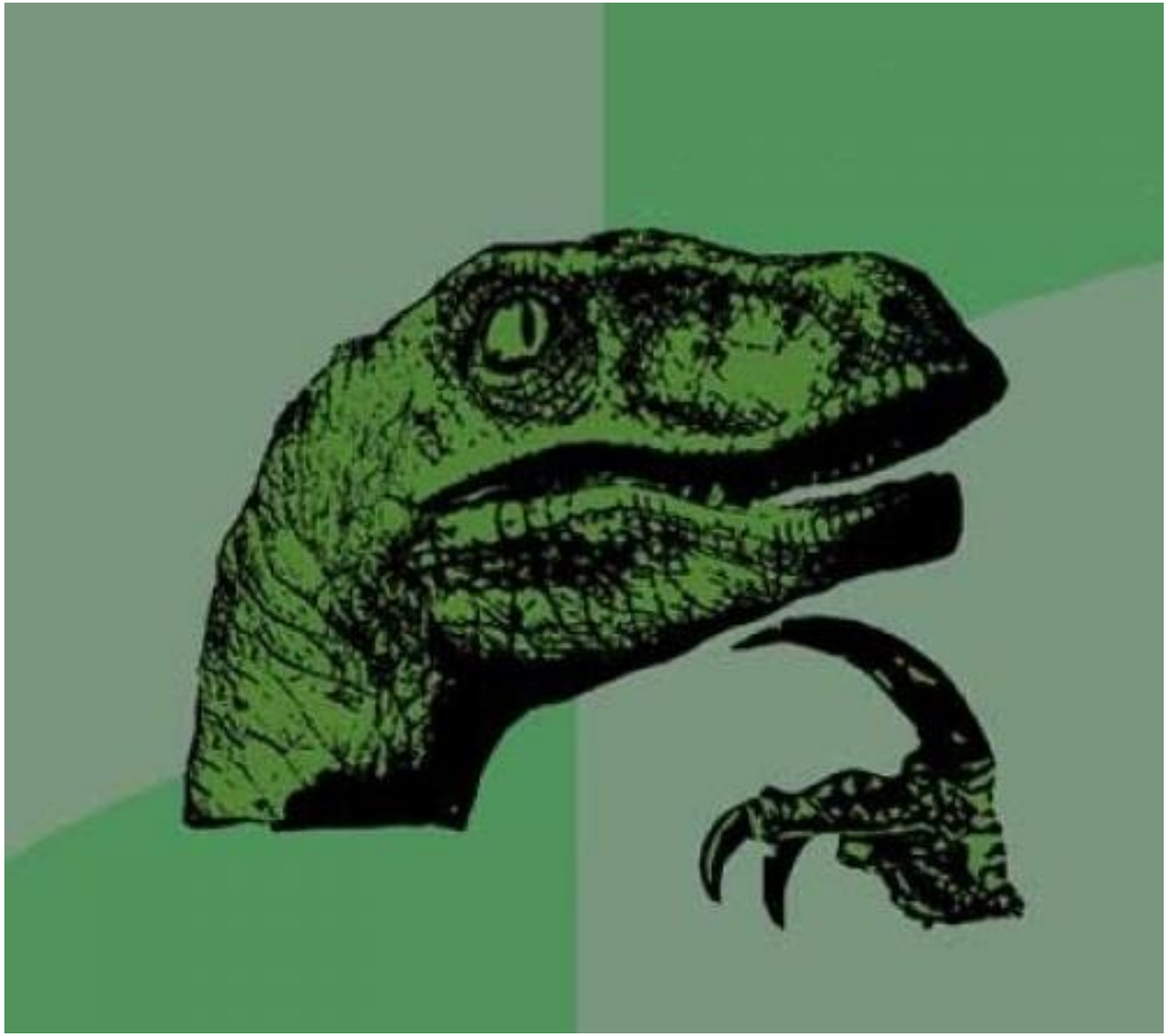


Let’s see another example

https://www.numerama.com/tech/423855-facebook-une-grosse-faille-de-securite-a-touche-50-millions-de-comptes.html

You have some minutes to read the article …

and give me the details of the resolution of this crisis =)



Any questions ?