# A06:2021 Composants vulnérables et obsolètes

Groupe 4:
Marieme BOUSSO
Aissata NDIAYE
Sokhna Oumou WADE
Serigne Fallou NDIAYE
Moustapha Adrien MBOUMBA

# Plan de la présentation

## Introduction

Intégrité

Fonction de hachage

Cryptographie

## Conclusion

# Introduction

Les composants vulnérables sont un problème connu pour lequel nous avons du mal à tester et à évaluer les risques. C'est-à -dire un composant qui présente des failles niveau sécurité qui exposent le logiciel à des attaques qui peuvent mener à une modification de nos données ou qui rendent le système défaillant.

Il se peut aussi que les composants soient obsolètes en d'autres termes que la version de ses composants ait expiré. De ce fait, cela peut mener à des dysfonctionnements du système et ouvrir la porte à des attaques extérieures vu que les failles ne sont plus prises en charge.

# 01
# INTEGRITE

# INTEGRITE

- **CVE-2017-5638**


Une vulnérabilité d'exécution à distance, qui permet l'exécution de code arbitraire sur le serveur, a été responsable d'importantes violations .

**10.0 CRITIQUE**

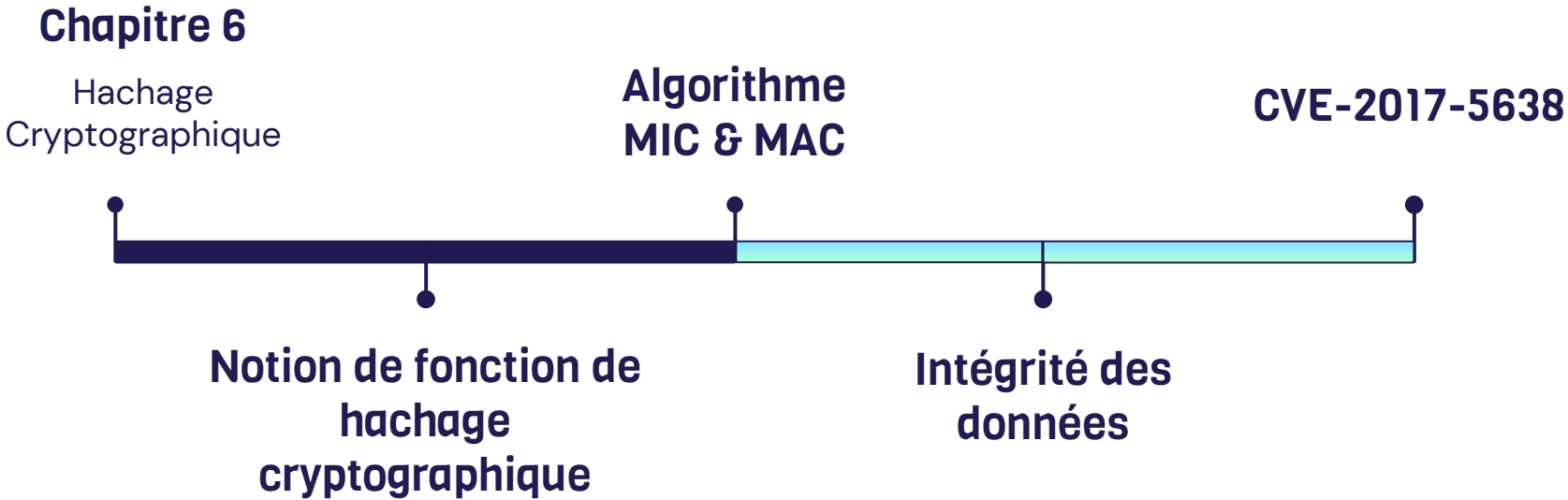
# INTEGRITE

- **Matching avec le cours**

# 02
# FONCTION DE HACHAGE

# FONCTION DE HACHAGE

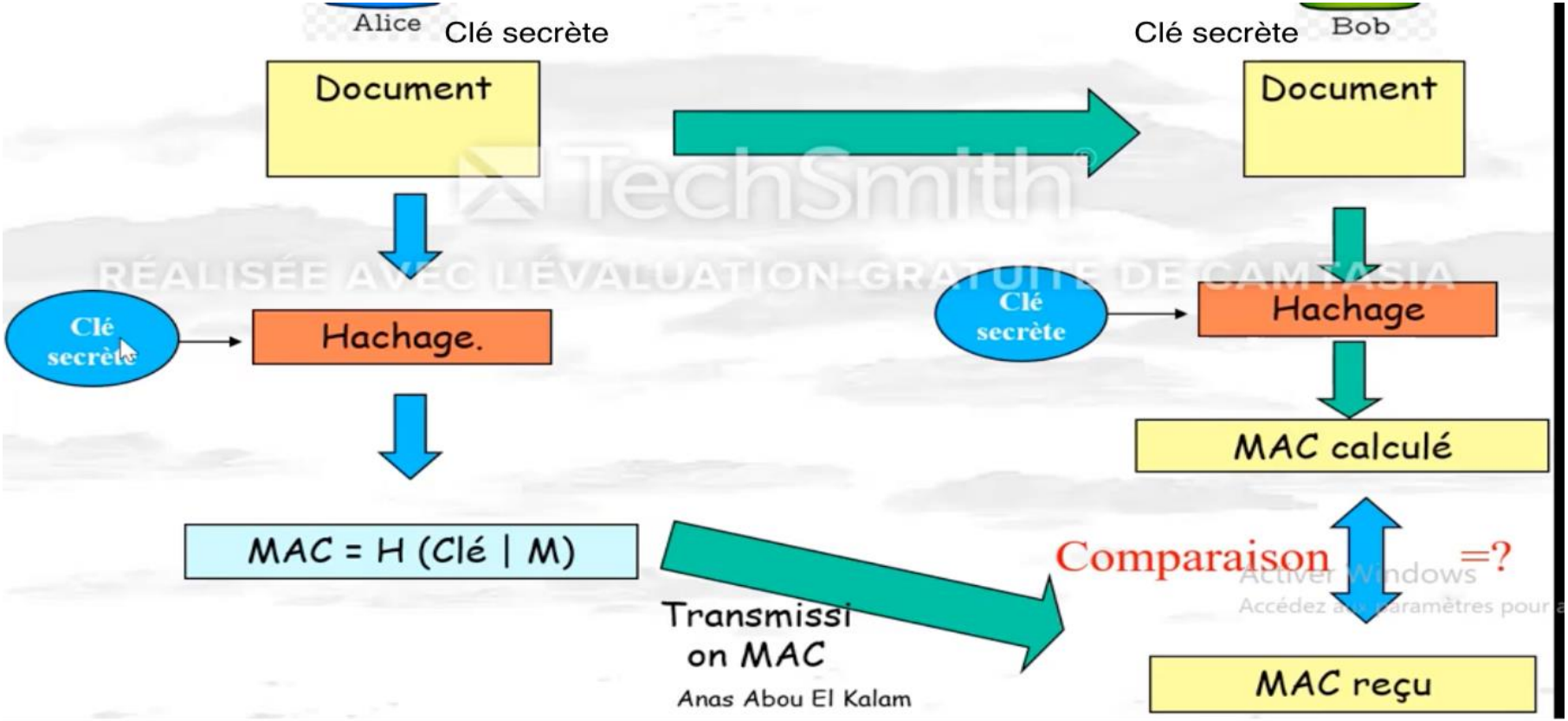
- **MATCHING AVEC LE COURS**

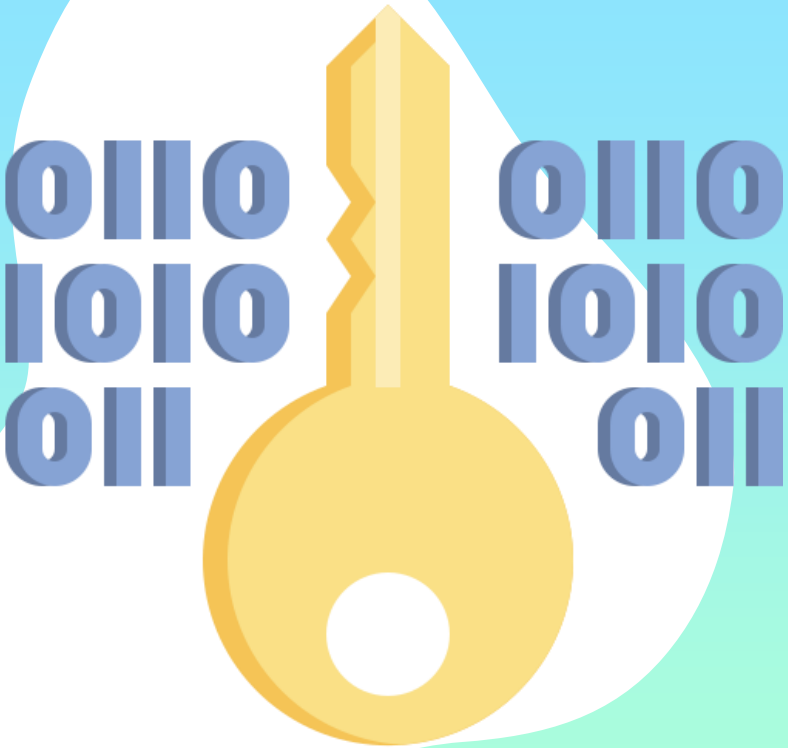


# FONCTION DE HACHAGE

- Une fonction de hachage cryptographique est un type de mécanisme de sécurité qui transforme un message de taille arbitraire en un message de taille fixe, appelé un condensé.
- **H(M) = h**
- Elle n’a pas de réciproque et doit être sans collision(**M1≠M2⇒H(M1)≠H(M2)**)

# Algorithme MAC



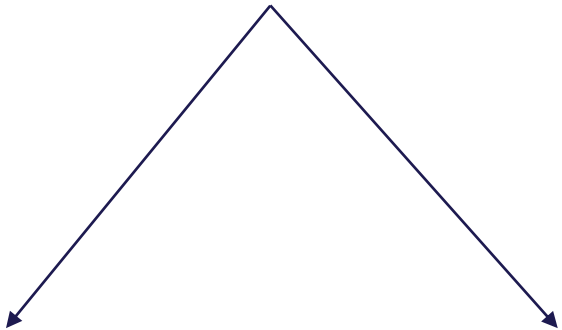


# 03
# CHIFFREMENT ASYMETRIQUE

# CHIFFREMENT ASYMETRIQUE

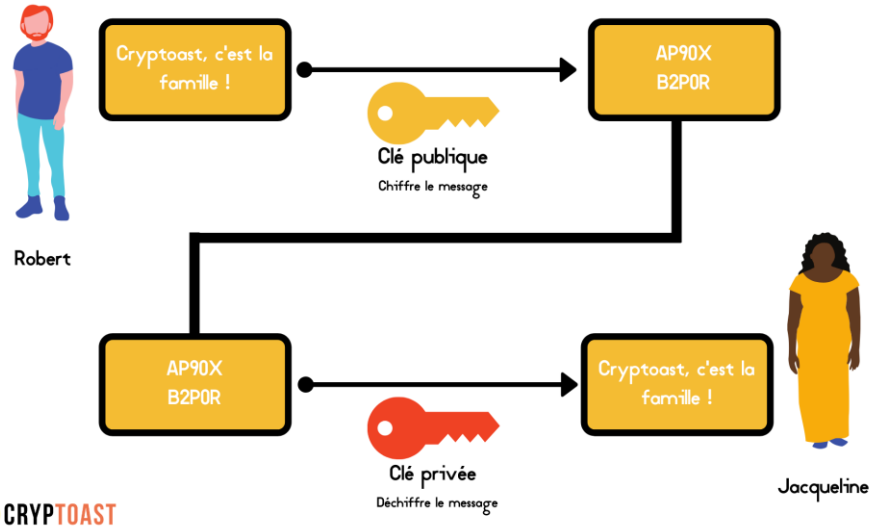
## DEFINITION

Méthode de chiffrement avec l'utilisation de 2 clés :



- Une clé publique connue de tous
- Une clé privée rendue sécrète

# CHIFFREMENT ASYMETRIQUE

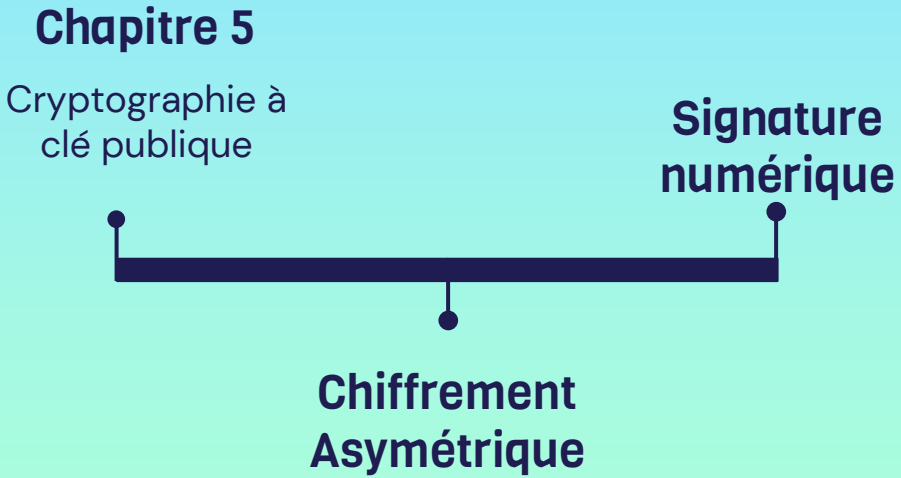



Clé Publique du destinataire pour chiffrer

Clé Privé du receveur pour déchiffrer

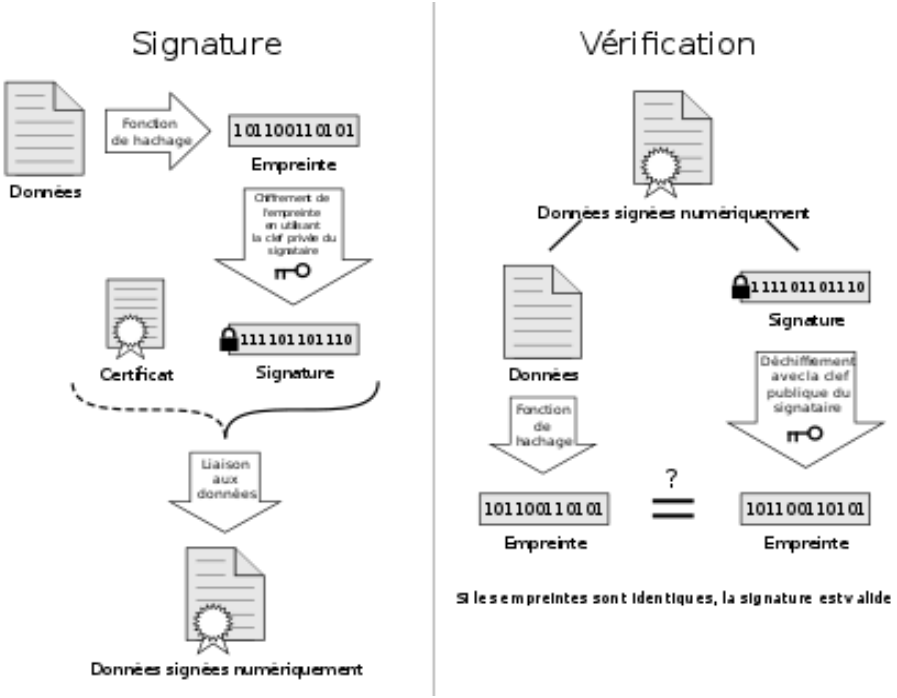
# CHIFFREMENT ASYMETRIQUE

- **MATCHING AVEC LE COURS**



# CHIFFREMENT ASYMETRIQUE

- **Notion de paquets non signés**




Paquets non signés → Risque de logiciels vulnérables ou corrompus

En effet, la signature numérique se base sur le principe de chiffrement asymétrique. Elle utilise la clé privée pour la signature et la clé publique pour le déchiffrement.

# Merci de votre attention