# Correspondance entre le cours et A02

**Groupe 9 :**

- Yacine Diagne
- Papa Abdou Calloga
- Yaye Khadidiatou Diop
- Aby Ndiaye
- Alioune Sall

# A02 : Défaillances cryptographiques

- Nature données
- Force algorithme
- Fonctions de chiffrement
- Fonctions de hachage

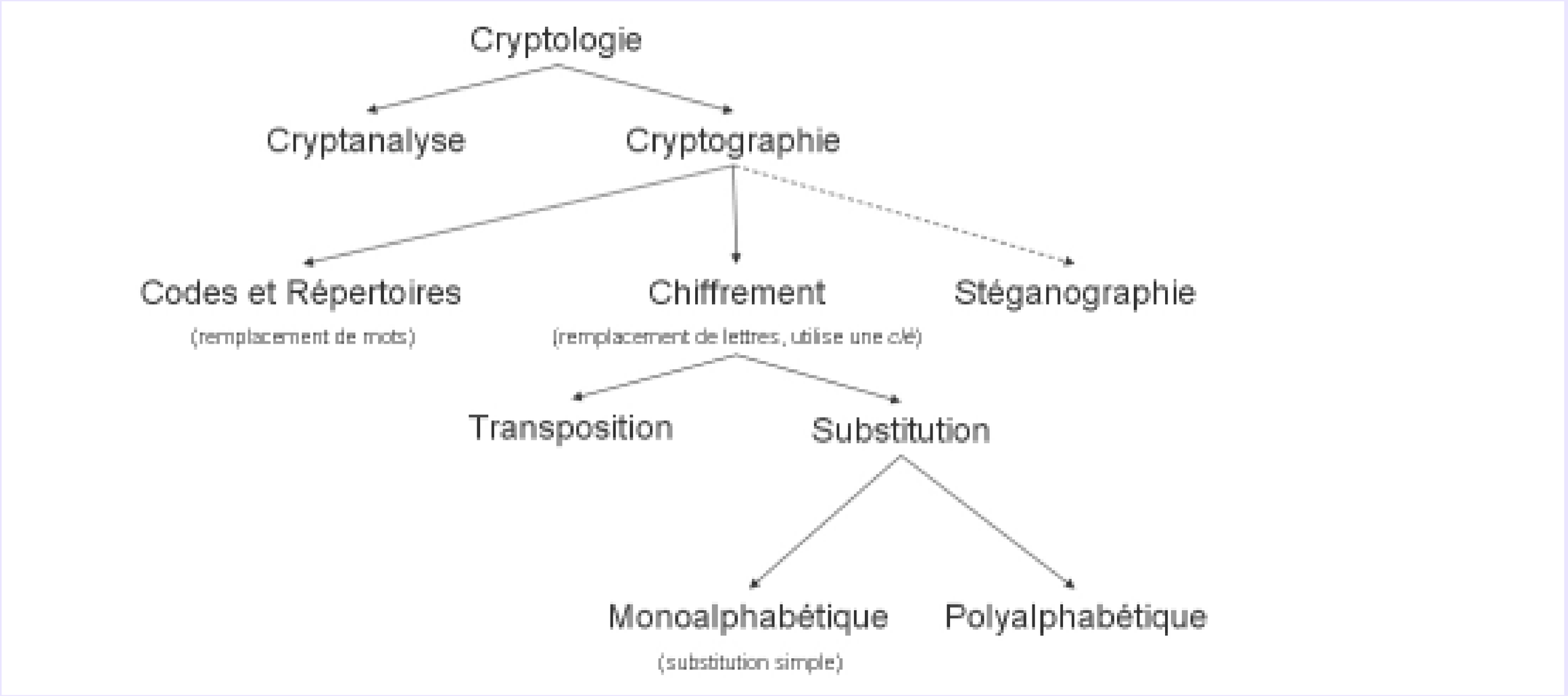
# PLAN

1. Cryptographie classique
2. Cryptographie à clé secrète
3. Cryptographie à clé publique
4. Fonctions de hachage


# Cryptographie Classique

# Définition

- Ensemble des techniques mises en œuvre pour brouiller la signification d'un message qui est matériellement visible
- En cryptographie classique, le chiffrement est symétrique, émetteur du message en clair et récepteur ont besoin initialement de partager un même secret, la « clé »




# Branches de la cryptologie

# Chiffrement par substitution : Exemple du chiffrement de César

## Comment fonctionne-t-il ?

- Technique de chiffrement ancienne
- Il consiste à décaler les lettres de l'aphabet d'un nombre de positions constant vers la droite ou la gauche

## Comment le casser ?

- Attaque par force brute
- Analyse de fréquences

# Chiffrement par transposition

## Fonctionnement

C’est un système de chiffrement qui consiste à bouleverser l’ordre des données à chiffrer (de façon à les rendre incompréhensibles) sans pour autant remplacer les lettres du message par d’autres
lettres ou symboles

## Le casser ?

Analyse de fréquences des lettres du texte

# Les CWEs impliqués

01 CWE-757 : sélection d'un algorithme moins sécurisé pendant la négociation ("rétrogradation d'algorithme")

02 CWE-327 : Utilisation d'un algorithme cryptographique défectueux ou risqué ?


# Cryptograhie à clé secréte

Permet à la fois de chiffrer et de déchiffrer des messages, à l'aide d'un même mot clé.

Wikipedia-Cryptographie Symétrique

“

Des algorithmes utilisés, soit par défaut, soit dans le code source existant, sont faibles ou désuets.

OWASP-A02-Déscription

Certains des algorithmes à clef symétrique sont cassables et donc leur utilisation introduit une vulnérabilité certaine dans nos systèmes.

Ex :
Un des algorithmes de chiffrement symétrique, réputé pour sa vulnérabilité aux attaques est celui de César

- Cryptographie symétrique d'emblée moins sécurisés, dû au fait que la clé secrète est à transmettre.

- Si les clefs générées sont faibles (DES), ou réutilisés (comme dans le mode ECB du cryptage par bloc), cela introduit une vulnérabilité.

> Des clefs de chiffrement faibles sont générées ou utilisées

OWASP-A02-Déscription

> Les vecteurs d'initialisation sont ignorés, réutilisés ou générés avec une sécurité insuffisante pour le mode d'opération cryptographique

OWASP-A02-Déscription

Mode CBC du chiffrement par bloc:

Des blocs de texte chiffrés identiques sont obtenus lorsque le même texte en clair est chiffré sous la même clé et le vecteur v

Ce vecteur d’initialisation n’a pas besoin d'être chiffré, mais ne doit pas être utilisé avec la même clé.

Remplissage :

Consiste à faire en sorte que la taille des données soit compatible avec les algorithmes utilisés

Utilisé dans la cryptographie symétrique:

- Par blocs
- Par flots

> Des méthodes cryptographiques de remplissage dépréciées, comme PKCS 1 v1.5 sont utilisées

OWASP-A02-Déscription

> Les clés ne sont pas générées de façon cryptographiquement aléatoire et stockées en mémoire sous la forme de tableau d'octets

OWASP-A02-Déscription

Par exemple pour le chiffrement DES, des doutes ont été émis sur la sécurité:

Ces doutes se fondent sur des spéculations sur:

- la longueur de la clef (56bits);
- le nombre d'itérations;
- et le schema de conception des tables-S.

# Des CWEs impliqués

01 CWE-329 Génération d'un vecteur d'initialisation prévisible avec le mode CBC

02 CWE-335 : Utilisation incorrecte des graines dans le générateur de nombres pseudo-aléatoires (PRNG)

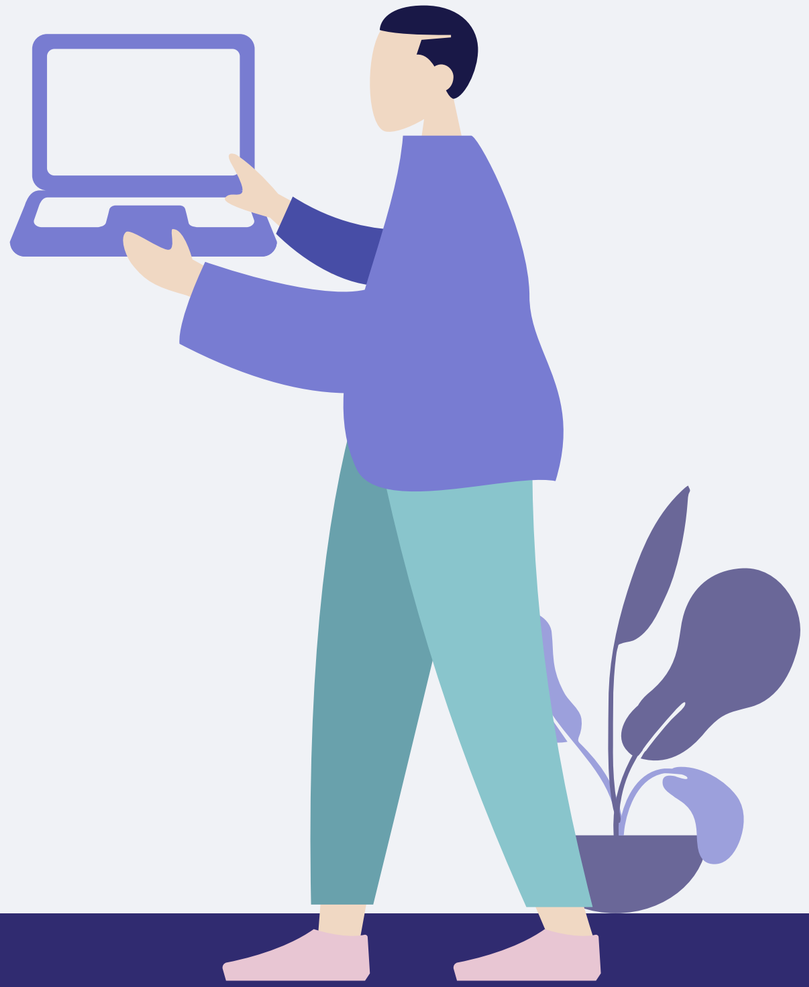
03 CWE-324 : Utilisation d'une clé après sa date d'expiration

# Cryptographie à cle publique

**Partage clé publique:**
On chiffre avec la clé publique et on déchiffre avec la clé prive qu'on garde

## Algorithmes asymétriques

- **RSA**
- **DSA**



# RSA?

## Algorithme

1. Générer aléatoirement de grands nombres premiers p et q
2. Calculer $n = pq$ et $\varphi = (p - 1)(q - 1)$
3. Choisir un entier aléatoire e, $1 < e < \varphi$ tel que $\text{pgcd}(e, \varphi) = 1$
4. Utiliser l'algorithme d'Euclide étendu pour calculer l'unique entier d, $1 < d < \varphi$ tel que $ed \equiv 1 \pmod{\varphi}$
5. La clef publique est (n, e) et la clef privée est d

# Cryptographie à cle publique

## Attaques

- Attaques par brute force
- Attaques mathématiques

# les CWEs Touchés

- CWE-780: Use of RSA Algorithm without OAEP
- CWE-338: Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG)
- CWE-327: Use of a Broken or Risky Cryptographic Algorithm
- CWE-325: Missing Cryptographic Step
- CWE-321: Use of Hard-coded Cryptographic Key

# Fonction de Hachage Cryptographique

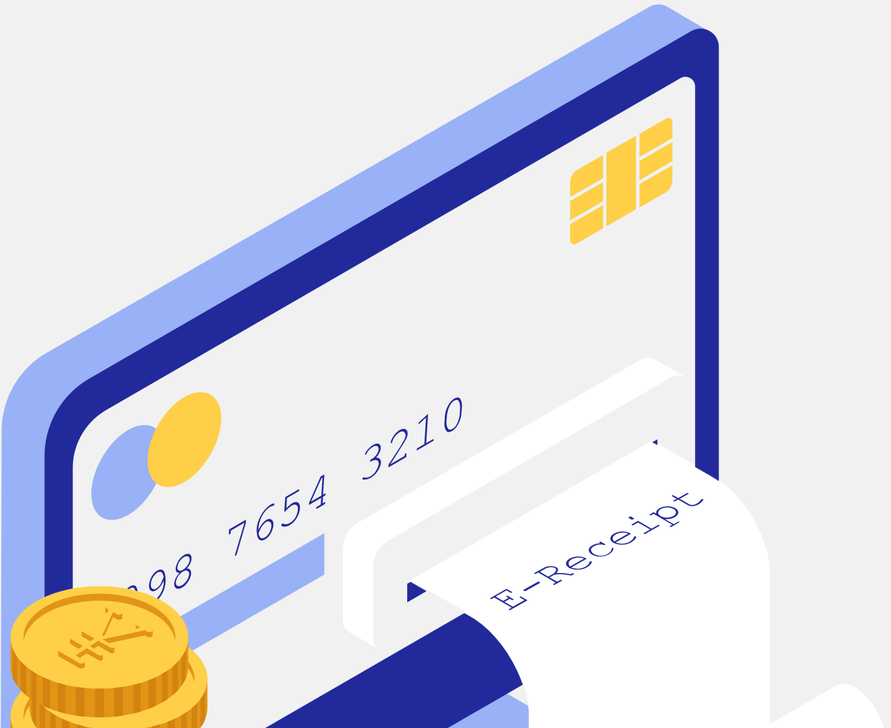
**"Est-ce que des fonctions de hachage dépréciées telles que MD5 ou SHA1 sont utilisées ou est-ce que des fonctions de hachage non cryptographiques sont utilisées là où des fonctions de hachage cryptographiques sont nécessaires ?"**

Cette défaillance peut etre liée en effet à l'utilisation d'une fonction de hachage non cryptographique dans une situation où il fallait utliser une fonction de hachage cryptograpique

# Notion de fonctions de hachage

Une fonction de hashage est une fonction qui prend en entree une donnee initiale pour calculer une sortie appelee empreinte numerique permettant d’identifier rapidement la donnee initiale.

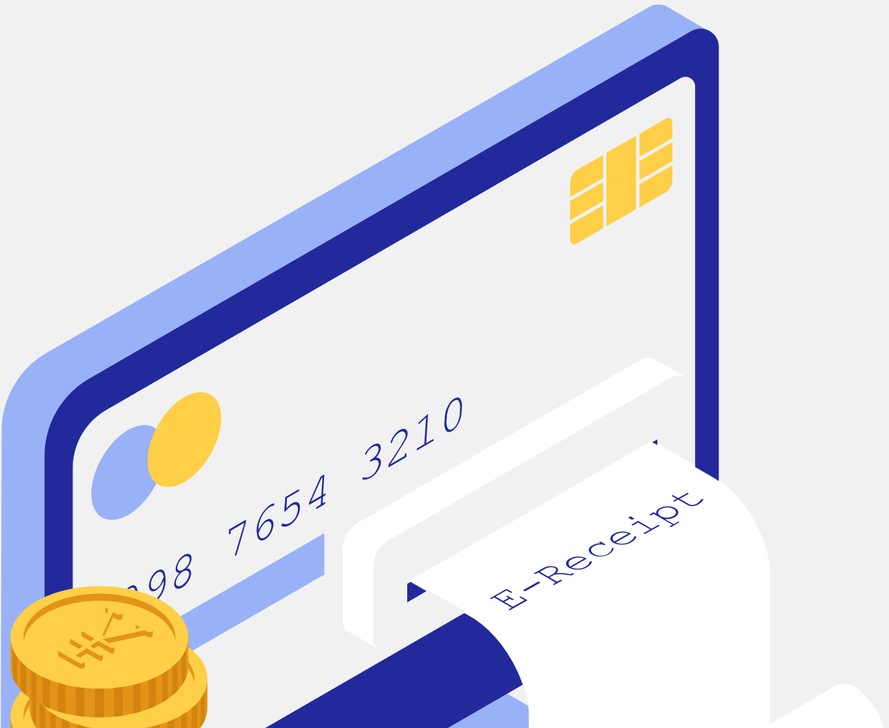
# Notion de fonctions de hachage cryptographique




La différence entre fonctions de hachage et celle cryptographique est que la dernière est à sens unique. C’est à dire à partir de l’image il est difficile de retrouver l’antécédent a partir de la fonction de hachage.

- Résistance à la collision → une fonction de hachage crypto dont le calcul de la preimage est de complexité : O(2^N)

# Notion de fonctions de hachage cryptographique




C’est à dire quand un attaquant dispose l’empreinte numérique la probabilité de retrouver la donnée initiale est de 2^n : la propriété de résistance à la collision

- Application de la fhc: intégrité et authentification des messages
- L’association entre une donnée initiale devrait être de telle sorte qu’une donnée initiale est identifiée de facon unique avec sa valeur de hachage avec une probabilité quasi inexistante de collision (les fonctions de hachages sont non injectives).
- Le systeme de crypto-monaie s’appuie sur des mécanismes de cryptographie simple telle que les hachages cryptotgraphiques et les signatures numériques.

# Classification des fonctions de hachage

Il existe deux types de fonctions de hachages cryptographiques :

- FHC sans clé
- FHC avec clé

Deux propriétés des FHC :

- compression → Entrée de nb bits arbitraire / sortie de n bit fixe
- Facilté de calcul de h(x) a partir de x

Parmi les fonctions de hashages sans clé on distingue deux types :

- OWHF → difficulté de trouver une entrée à partir d'une valeur de hachage pre-specifie.

- CRHF → résistance a la collision cad il est difficile de trouver deux valeurs d'entrée ayant la même valeur de hashage

Fonction de hashages avec clé : Mac

# Les CWEs Impliqués

01 CWE-759 Use of a One-Way Hash without a Salt

02 CWE-760 Use of a One-Way Hash with a Predictable Salt

03 Use of Password Hash With Insufficient Computational Effort

04 CWE-261 Weak Encoding for Password

# CONLUSION

*Que retenir ?*

# Merci de votre attention ! 😇