Cryptanalyse

Objectifs de la cryptanalyse

Attaquer un cryptosystème, cassable(vulnérable). Cryptosystème vulnérable :

- Décrypter des messages sans connaître la clé.
- Chiffrer des messages sans connaître la clé
- Trouver la clé

Niveaux d'Attaques

Les niveaux d'attaques en cryptographie se définissent par les informations disponibles pour l'attaquant et les méthodes utilisées pour casser un système.

Objectif principal :

Découvrir la clé secrète, déchiffrer un message ou compromettre le système de sécurité.

Types d'attaques principales :

- Attaques sur le texte chiffré.
- Attaques sur le texte clair connu.
- Attaques sur le texte clair choisi.
- Attaques sur le texte chiffré choisi.

Attaque par Texte Chiffré Seul (Ciphertext Only Attack - COA)

Description :

- L'attaquant dispose uniquement d'un ou plusieurs textes chiffrés.
- Il tente d'extraire des informations ou de déduire la clé.

Techniques possibles :

- Analyse de fréquence (pour les chiffrements simples).
- Essais systématiques (force brute).

Attaque par Texte Clair Connu (Known Plaintext Attack - KPA)

Description :

- L'attaquant dispose d'un texte chiffré et de son équivalent en clair.
- Il utilise ces informations pour déduire la clé ou le mécanisme de chiffrement.

Techniques possibles :

- Analyse des patterns (répétitions dans le texte clair et le texte chiffré).
- Utilisation de modèles linguistiques.

Attaque par Texte Clair Choisi (Chosen Plaintext Attack - CPA)

Description :

- L'attaquant choisit un texte clair spécifique et obtient son équivalent chiffré.
- Cela lui permet d'étudier le fonctionnement du chiffrement.

Techniques possibles :

- Envoi de textes clairs identiques ou similaires pour analyser les résultats.
- Exploitation des relations entre les textes clairs et chiffrés.

Attaque par le texte Chiffré Choisi (Chosen Ciphertext Attack - CCA)

Description :

- L'attaquant choisit un texte chiffré et obtient son équivalent en clair.
- Utilisé pour tester les faiblesses des algorithmes et des implémentations.

Techniques possibles :

- Exploitation des failles dans le déchiffrement ou le padding (ex : attaque par Oracle Padding).

Attaque par Force Brute

Principe :

- Essayer toutes les combinaisons possibles de clés ou de mots de passe jusqu'à trouver la bonne.
- Fonctionne pour des systèmes utilisant des clés courtes ou faibles.

Algorithme :

1. Générer une clé candidate.
2. Chiffrer ou déchiffrer le message avec cette clé.
3. Comparer le résultat avec un texte attendu.
4. Répéter jusqu'à ce que la clé correcte soit trouvée.

Attaque par Analyse de Fréquence

Principe :

- Exploiter la fréquence des lettres dans une langue donnée pour déduire les substitutions dans un texte chiffré.
- Applicable aux chiffrements mono-alphabétiques comme César ou Polybe.

Algorithme :

1. Calculer la fréquence de chaque lettre dans le texte chiffré.
2. Comparer ces fréquences avec les fréquences typiques de la langue.
3. Faire correspondre les lettres en fonction des probabilités.

Analyse Différentielle

Principe :

- Étudier l'effet des différences dans les textes clairs sur les différences dans les textes chiffrés.
- Exploite la propagation des différences à travers les étapes de chiffrement pour déduire des informations sur la clé.

Algorithme :

1. Choisir des paires de textes clairs avec une différence spécifique.
2. Observer les différences dans les textes chiffrés correspondants.
3. Analyser les corrélations pour identifier des failles dans le chiffrement.

Analyse Linéaire

Principe :

- Approximations linéaires des relations entre les bits du texte clair, du texte chiffré et de la clé.
- Exploite des corrélations statistiques faibles dans le chiffrement.

Algorithme :

1. Formuler une approximation linéaire reliant le texte clair, le texte chiffré et la clé.
2. Tester cette relation sur un grand nombre de textes clairs et chiffrés.
3. Identifier des biais statistiques pour déduire des parties de la clé.

Principe de Kerckhoffs

Principe de Kerckhoffs

Définition :

Le principe de Kerckhoffs, proposé en 1883, énonce qu'un système cryptographique doit rester sécurisé, même si tout, sauf la clé, est connu par l'attaquant.

Enjeux :

- La sécurité doit reposer sur le secret de la clé, et non sur l'obscurité de l'algorithme.
- Les systèmes peuvent être audités publiquement pour garantir leur robustesse.
- Le principe favorise la transparence et la confiance dans les systèmes cryptographiques.

Importance du Principe de Kerckhoffs

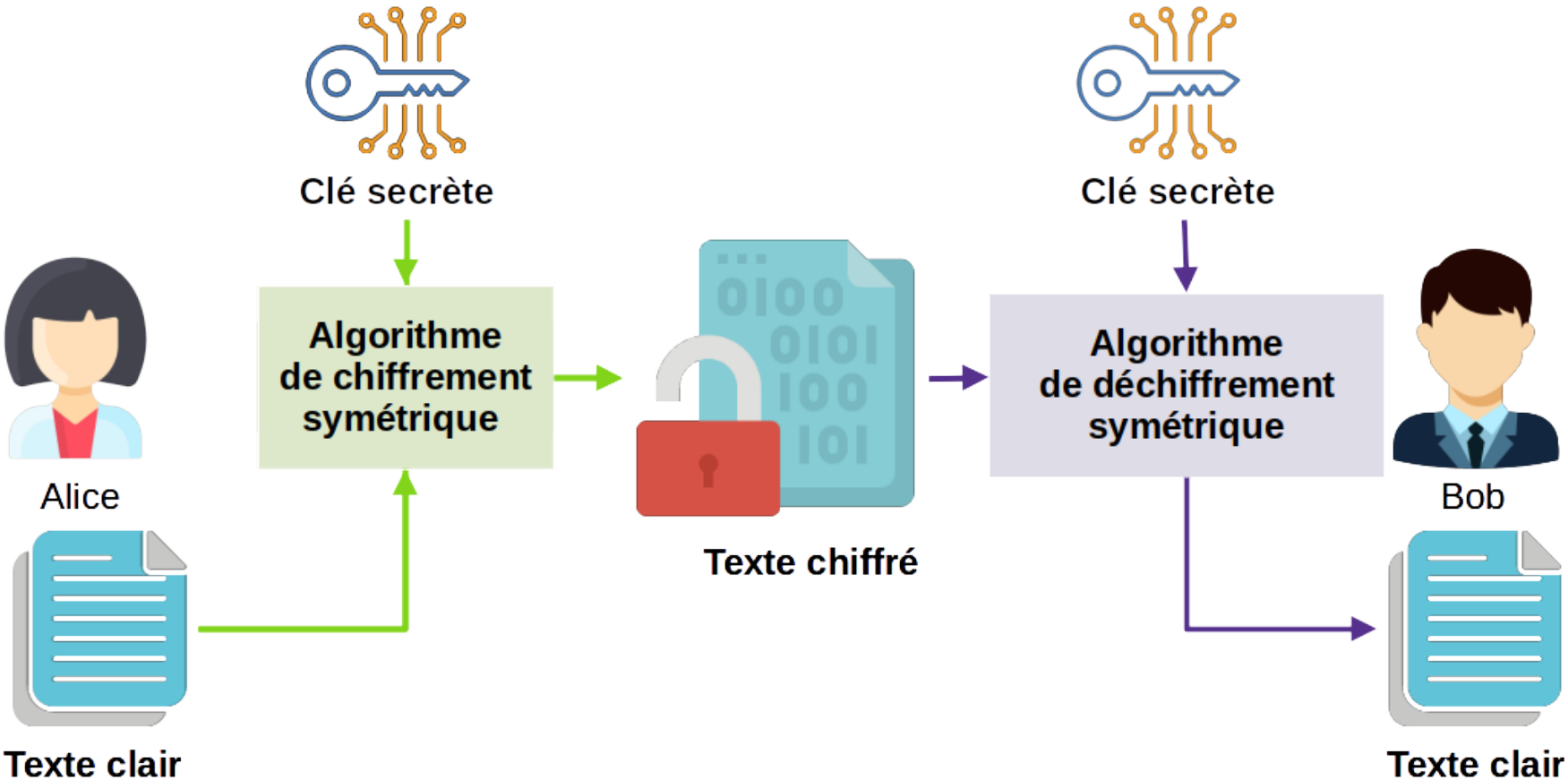
Pourquoi ce principe est-il crucial ?

- **Transparence :** Permet de tester les systèmes publiquement, augmentant leur robustesse.
- **Sécurité durable :** Même si l'algorithme est exposé, la sécurité persiste tant que la clé est protégée.
- **Simplicité de mise à jour :** Changer une clé est beaucoup plus simple que modifier un algorithme.

Exemple contraire :

- Les systèmes qui reposent sur l'obscurité de l'algorithme (ex : chiffrement propriétaire) sont vulnérables si l'algorithme est révélé.
- Exemple : Algorithmes faibles ou obsolètes (DES raccourci ou algorithmes non standard).

Cryptographie symétrique



Cryptographie Symétrique

Cryptographie Classique

Cryptographie Classique

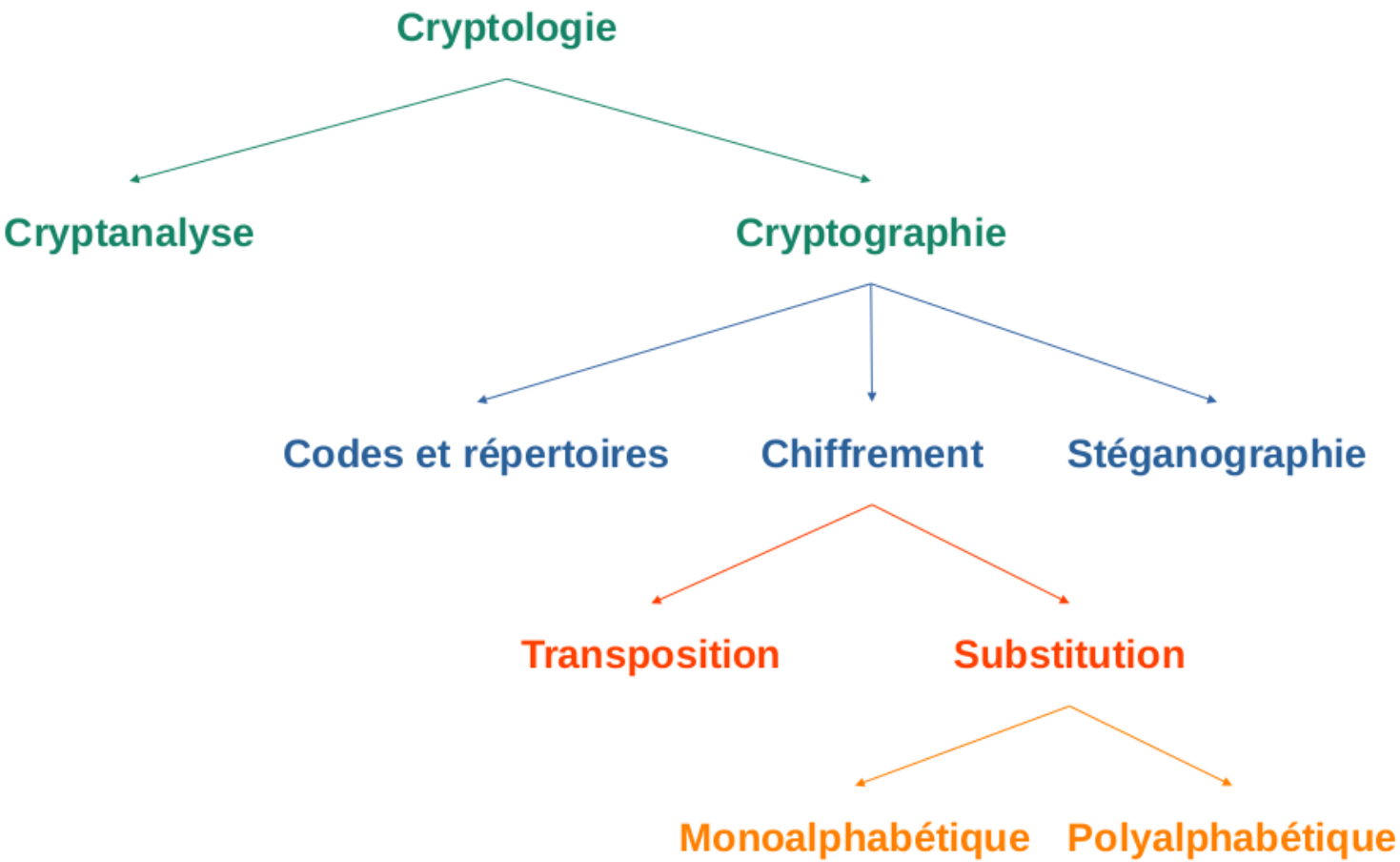
Définition :

- Les chiffrements classiques regroupent les premières techniques cryptographiques.
- Ils visent à protéger les messages en utilisant des méthodes simples de substitution et de transposition.

Caractéristiques :

- Techniques simples, souvent manuelles ou mécaniques.
- Fonctionnent par substitution ou transposition.
- Manipulent les données caractère par caractère (chiffrement par flux).

Cryptographie Classique



Catégories des Chiffrements Classiques

1. Chiffrements par substitution :

- Chaque caractère du texte clair est remplacé par un autre caractère selon une règle définie.
- Exemples :
  - Chiffre de César
  - Chiffre de Vigenère

2. Chiffrements par transposition :

- Les caractères du texte clair sont réorganisés selon un schéma prédéfini.
- Exemples :
  - Scytale spartiate
  - Carré de Polybe

Carré de Polybe (200 av. J.-C.)

Principe :

- Méthode de transposition utilisant une grille pour convertir des lettres en paires de chiffres.
- L'alphabet est placé dans une grille de 5×5, en regroupant I et J dans la même case.

Exemple de grille :

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Carré de Polybe (200 av. J.-C.)

Exemple de chiffrement :

- Texte clair : **BONJOUR**
- Texte chiffré : **12 34 33 24 34 45 42**

	1	2	3	4	5
1	*A*	**B**	*C*	*D*	*E*
2	*F*	*G*	*H*	*I*/**J**	*K*
3	*L*	*M*	**N**	**O**	*P*
4	*Q*	**R**	*S*	*T*	**U**
5	*V*	*W*	*X*	*Y*	*Z*

Chiffrement de Vernam (1917)

Principe :

- Substitution basée sur l'opération XOR (OU exclusif).
- Chaque caractère du texte clair est combiné avec un caractère d'une clé aléatoire de même longueur.

Formule :

$$y = x \oplus k$$

où :

- y : texte chiffré
- x : texte clair
- k : clé (unique et aléatoire)

Chiffrement de Vernam (1917)

Exemple :

- x : 10101011
- k : 11001101
- y : 01100110

Rappel : Calcul modulaire et inverse modulaire

- **Calcul modulaire** : $a \mod m$ représente le reste de la division de a par m.
  Exemple : $17 \mod 5 = 2$ (car $17 = 3 \times 5 + 2$).
- **Inverse modulaire** : Soit a et m tels que $\text{pgcd}(a, m) = 1$.
  L'inverse modulaire $a^{-1} \mod m$ est le nombre b tel que :

$$a \cdot b \equiv 1 \pmod{m}.$$

  Exemple : Pour $a = 3$ et $m = 26$, l'inverse modulaire de 3 est 9 car $3 \cdot 9 \equiv 1 \pmod{26}$.

Le chiffrement affine

- **Formule de chiffrement** :

$$y \equiv (a \cdot x + b) \pmod{n}$$

où :

  - x : la lettre en clair (représentée par un entier),
  - y : la lettre chiffrée,
  - a et b : clés du chiffrement ($\text{pgcd}(a, n) = 1$),
  - n : taille de l'alphabet.

- **Déchiffrement** :

$$x \equiv a^{-1} \cdot (y - b) \pmod{n}.$$

Exemple pratique

Paramètres : $a = 5,\ b = 8,\ n = 26$ (alphabet anglais).

Chiffrement :

- Soit $x = 7$ (représentant la lettre H).
- Calcul : $y \equiv (5 \cdot 7 + 8) \mod 26 = 43 \mod 26 = 17$.
- La lettre chiffrée correspond à $17 \rightarrow R$.

Déchiffrement :

- L'inverse modulaire de $a = 5$ modulo 26 est $a^{-1} = 21$.
- Calcul : $x \equiv 21 \cdot (17 - 8) \mod 26 = 21 \cdot 9 \mod 26 = 189 \mod 26 = 7$.
- La lettre déchiffrée est $7 \rightarrow H$.

Avantages et Limites des Chiffrements Classiques

Avantages :

- Simplicité et facilité d'implémentation.
- Adaptés aux communications non numériques à leur époque.

Limites :

- Vulnérabilité aux attaques modernes comme l'analyse de fréquence.
- Clés souvent courtes et faciles à deviner.
- Inadaptés aux grands volumes de données modernes.

Transition vers la Cryptographie Moderne

Problèmes résolus par les algorithmes modernes :

- Gestion des clés simplifiée avec des clés longues et aléatoires.
- Résistance aux attaques connues grâce à des bases mathématiques solides.
- Adaptation aux volumes de données numériques.

Exemples d'algorithmes modernes :

- Symétriques : AES, DES.
- Asymétriques : RSA, ECC.