Complexité et Cryptographie Master :Ingénierie de Développement Logiciel et Décisionnel

Pr. Fatima-Ezzahra Ziani

Faculté des Sciences - Université Mohammed V- Rabat

Année Universitaire : 2024-2025

Pourquoi Étudier la Complexité et Cryptographie ?

1. La Cryptographie est Au Cœur de Notre Société Numérique

- Les communications en ligne (messages, appels, transactions) reposent sur des protocoles cryptographiques pour protéger la confidentialité et l'intégrité.
- Des services de tous les jours, comme la banque en ligne, le e-commerce, et les réseaux sociaux, utilisent la cryptographie pour garantir des échanges sécurisés.

Motivations

2. Menaces Croissantes et Besoin de Sécurité

- Les cyberattaques, telles que les piratages, les violations de données et les ransomwares, rendent indispensable la sécurisation des informations.
- Avec des milliards de dollars perdus chaque année en raison de cybercrimes, il est crucial de renforcer les systèmes de sécurité.

Objectif du cours

Objectif du Cours

Comprendre les bases de la cryptographie, maîtriser les algorithmes, et apprendre à sécuriser des systèmes d'information contre les menaces modernes.

Cryptographie

Cryptographie

Science et art d'écrire des messages de manière à les rendre illisibles pour toute personne autre que le destinataire prévu.

Cryptanalyse

Discipline qui consiste à casser ou déchiffrer les systèmes cryptographiques
⇒Analyser et découvrir les moyens de casser un chiffrement sans connaître les clés secrètes.

Terminologie

Cryptologie

Cryptologie = Cryptographie + Cryptanalyse

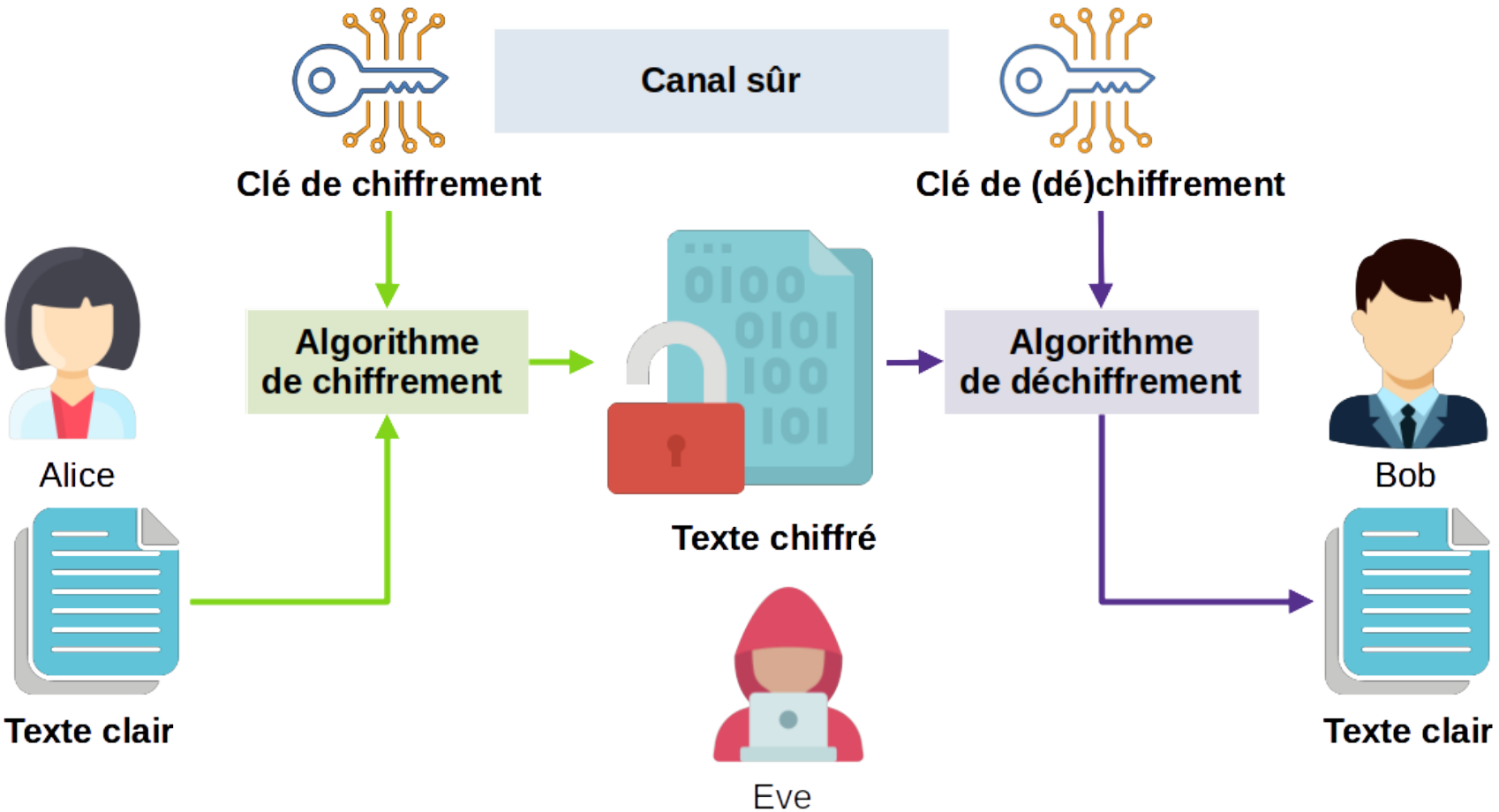
Clé

Information secrète utilisée pour crypter le message puis plus tard pour le décrypter.

Cryptosystème

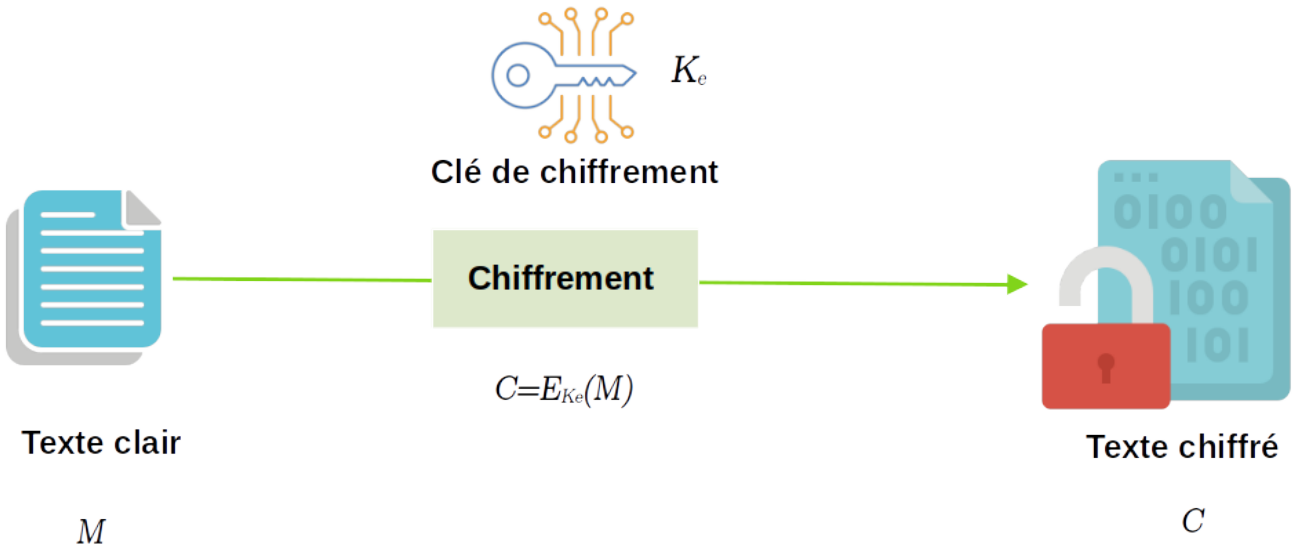
Ensemble d'algorithmes et de clés, formant un système permettant de chiffrer et déchiffrer des informations pour assurer leur sécurité.

Principe de la cryptographie



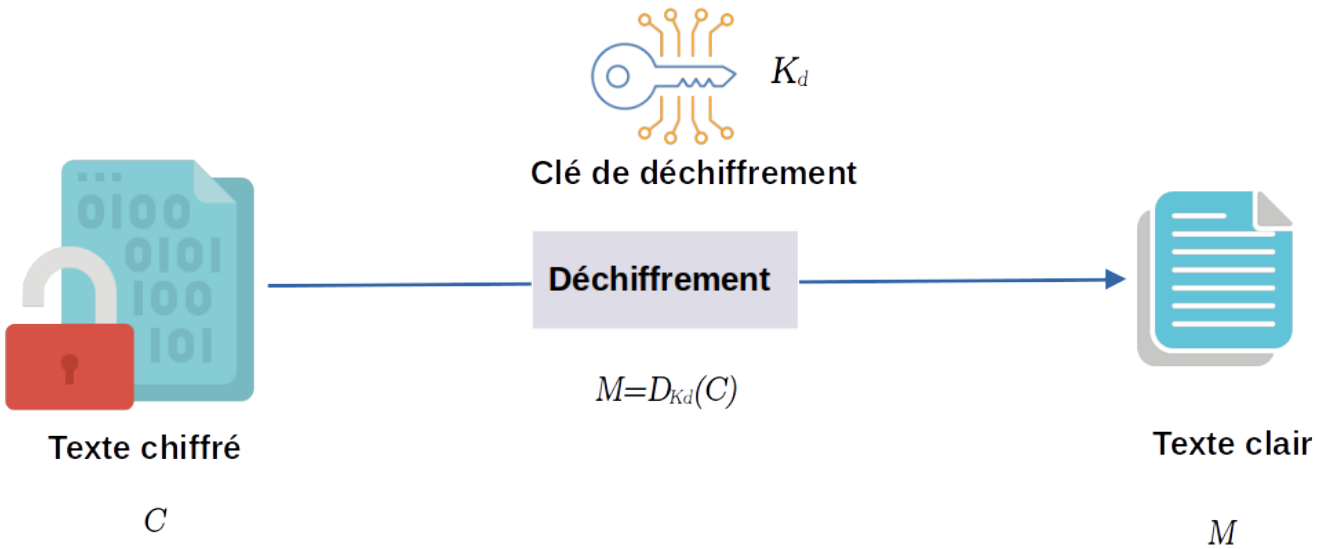
Chiffrement

Processus de conversion de données (texte en clair) en une forme illisible (texte chiffré) à l'aide d'un algorithme et d'une clé.



Déchiffrement

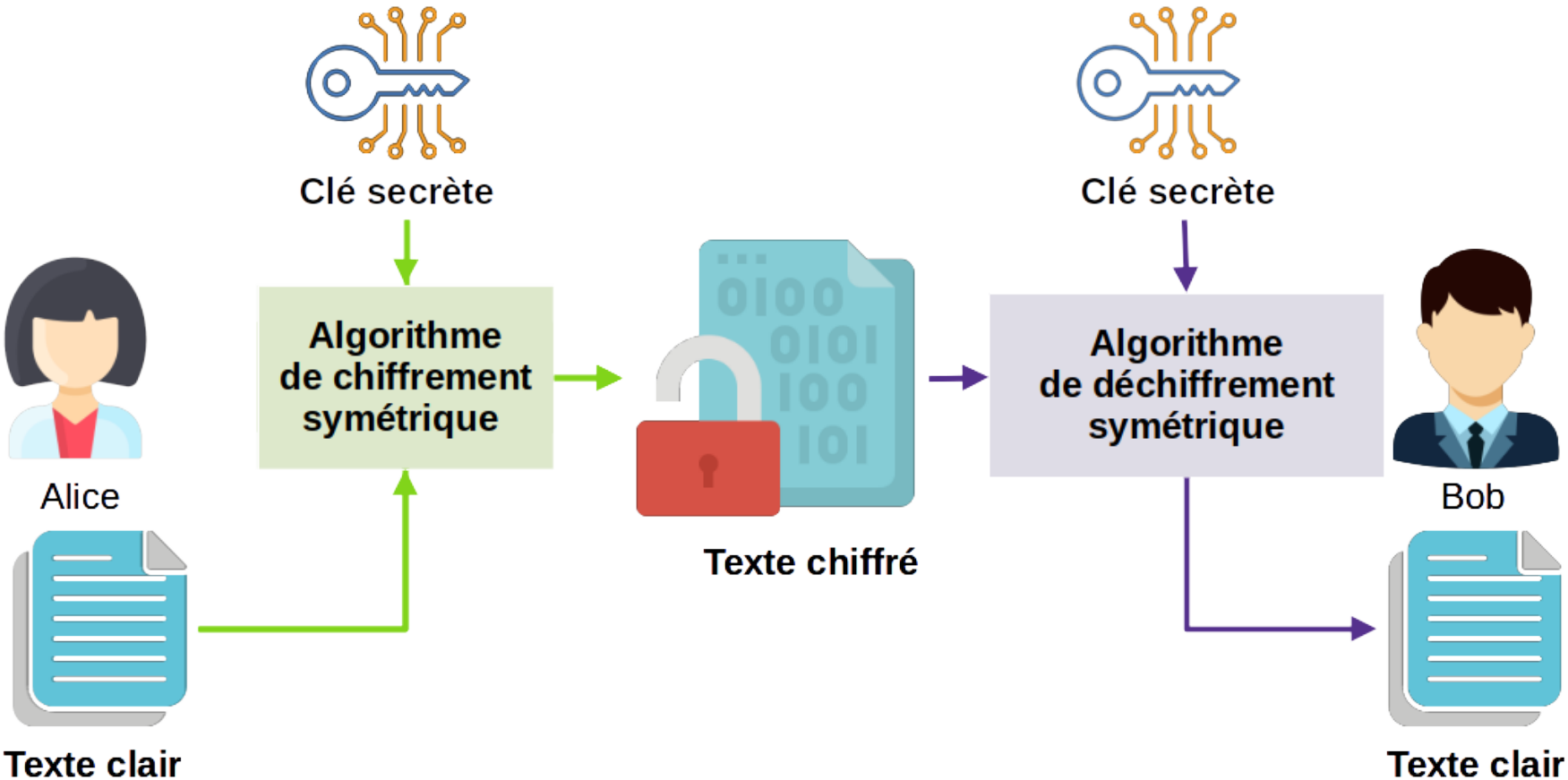
Processus inverse du chiffrement, visant à reconvertir le texte chiffré en texte en clair, généralement à l'aide de la clé de déchiffrement.



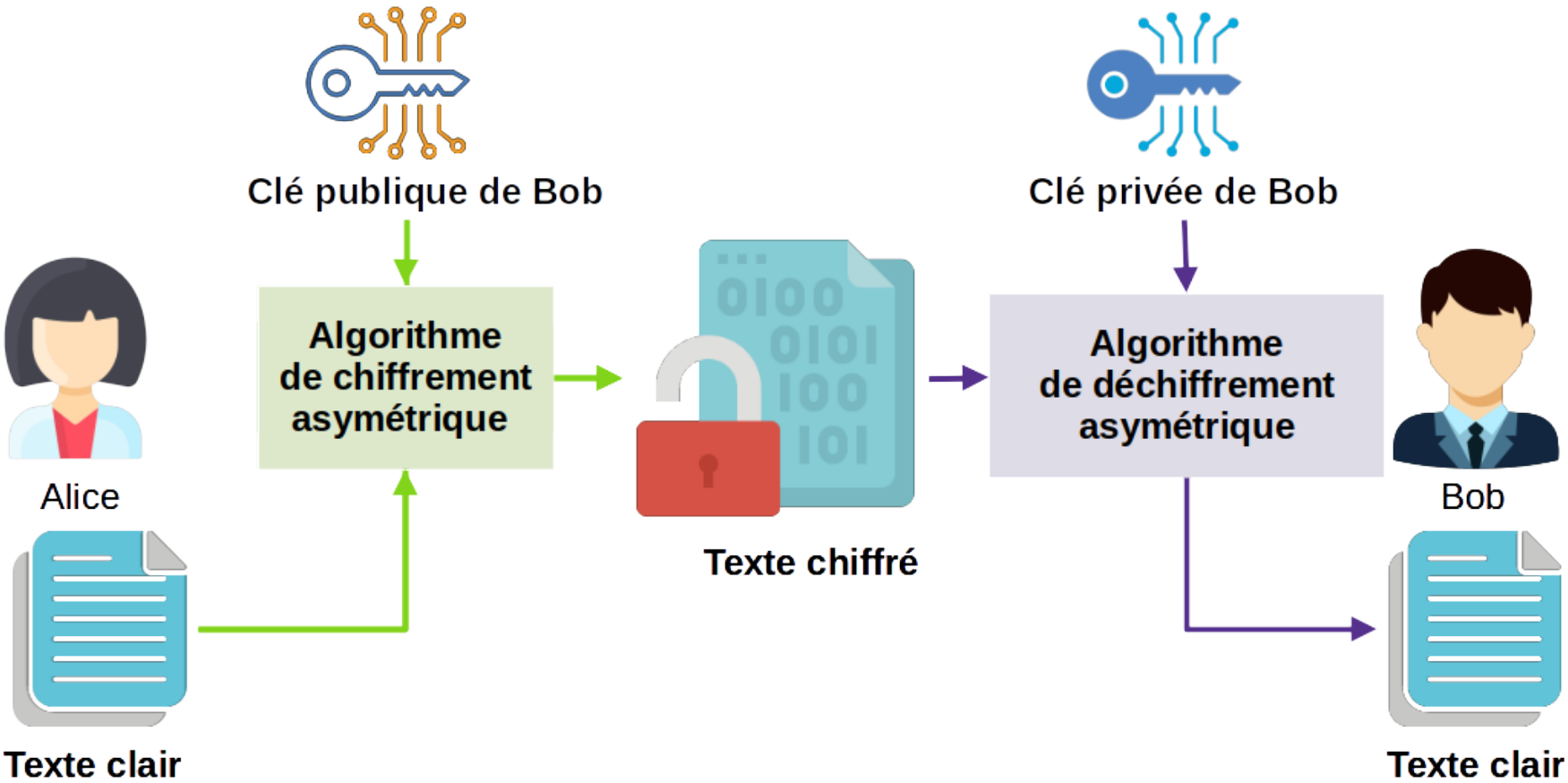
Le type de relation qui unit les clés K_e et K_d permet de définir deux grandes catégories de systèmes cryptographiques

- Les systèmes à clefs secrètes / symétriques : (DES, AES, IDEA, Blowfish, ...) La même clé est utilisée pour chiffrer et déchiffrer.
- Les systèmes à clefs publiques / asymétriques : (RSA, El-Gamal, un cryptosystème elliptique ...) La clé de chiffrement est différente de la clé de déchiffrement.

Cryptographie symétrique



Cryptographie asymétrique



Principes de Base de la Cryptographie Moderne

Confidentialité :

Assurer que seuls les destinataires autorisés peuvent accéder aux informations.

⇒ Alice veut être certaine qu'une personne non-autorisée (Ève) ne peut pas prendre connaissance des messages qu'elle envoie.
⇒ Bob veut être certain que personne d'autre que lui (et Alice bien sûr) n'a accès au contenu du message.

Exemple de Confidentialité : Application Bancaire

Exemple : Application Bancaire Mobile

- Connexion sécurisée : Les données échangées entre l'application et le serveur sont chiffrées avec le protocole TLS . Cela empêche quiconque d'intercepter et de lire ces informations sensibles sur un réseau non sécurisé.
- Chiffrement des données de transaction : Les numéros de compte, soldes, et détails de transactions sont chiffrés avant d'être stockés sur les serveurs de la banque. Même en cas de piratage, les données restent protégées.

Résultat

Ces techniques assurent la confidentialité des informations bancaires, protégeant ainsi les données contre les interceptions et les accès non autorisés.

Principes de Base de la Cryptographie Moderne

Intégrité :

Empêcher la modification ou altération des données sans détection.

⇒ Alice veut être certaine que ses messages ne seront pas falsifiés par un attaquant malveillant.
⇒ Bon veut être certain que le message n'a pas été falsifié par un attaquant malveillant.

Exemple d'Intégrité des Données

Exemple concret : Vérification de l'intégrité des fichiers

- Lorsqu'un fichier est stocké, une somme de contrôle (par exemple, un hash MD5 ou SHA-256) est calculée et enregistrée.
- Lors de l'accès ultérieur au fichier, la somme de contrôle calculée est comparée à celle initialement enregistrée.
- Si les sommes de contrôle sont identiques, l'intégrité du fichier est confirmée.
- Si les sommes de contrôle diffèrent, cela indique une altération du fichier, qu'il s'agisse d'une corruption ou d'une tentative de manipulation malveillante.

Principes de Base de la Cryptographie Moderne

Authentification :

Vérifier l'identité des parties impliquées dans la communication.

⇒ Bob veut être certain que le message reçu vient bien d'Alice, par exemple qu'un attaquant malveillant (Eve) ne puisse pas se faire passer pour Alice, mascarade ou usurpation d'identité.

Exemple d'Authentification à Deux Facteurs

Exemple concret : Authentification avec mot de passe et code 2FA

- L'utilisateur entre son **mot de passe** sur la page de connexion.
- Une fois le mot de passe validé, un **code temporaire** est généré par une application mobile (ex : Google Authenticator).
- L'utilisateur entre ce code dans l'interface de connexion.
- Si le code correspond à celui généré pour cette période, l'utilisateur est authentifié et obtient l'accès.
- Si le code est incorrect, l'accès est refusé.

Principes de Base de la Cryptographie Moderne

Non-répudiation :

Empêcher une partie de nier avoir envoyé ou reçu un message.

⇒ Alice veut être certaine que le destinataire (Bob) a bien pris connaissance de ses messages et ne pourra pas nier l'avoir reçu.
⇒ Bob veut être certain que l'expéditeur (Alice) ne pourra pas nier avoir envoyé le message.

Exemple concret : Paiement par carte de crédit en ligne

- Lorsqu'un utilisateur effectue un paiement en ligne, il entre ses informations de carte de crédit sur un site sécurisé.
- Le paiement est authentifié via un **code de sécurité** (CVV) et peut être validé par un système d'authentification supplémentaire, comme l'authentification 3D Secure (ex : Verified by Visa ou Mastercard SecureCode).
- Après validation, une **confirmation de paiement** est envoyée au client et au commerçant, contenant des détails comme le montant, l'heure, et un identifiant de transaction unique.

- Cette confirmation sert de preuve irréfutable que le client a bien autorisé le paiement, et elle est horodatée pour garantir la chronologie de l'action.
- Si le client tente de contester plus tard la transaction, la confirmation de paiement et l'authentification par code (CVV) fournissent des preuves de la validité de la transaction.
- Les autorités bancaires et les organismes de sécurité peuvent utiliser ces preuves pour résoudre les conflits de manière transparente.

Histoire de la cryptographie

Antiquité : Premières Techniques de Chiffrement

- **Scytale spartiate (500 av. J.-C** : Dispositif en bâton utilisé pour chiffrer des messages.
- **Chiffre de César (env. 50 av. J.-C.)** : Décalage des lettres pour masquer le message.
- **Méthodes de substitution et de transposition** : Premières bases de la cryptographie.

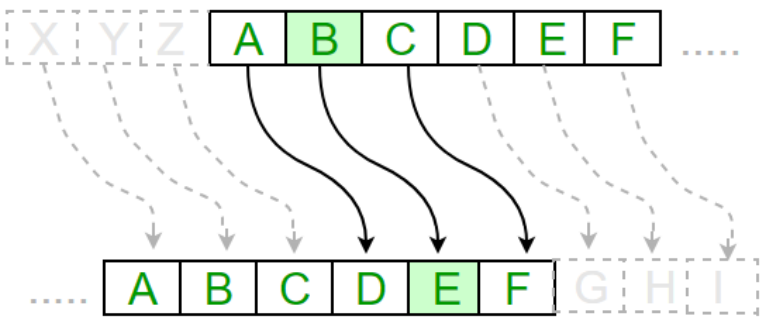


Figure – Illustration du Chiffre de César

Chiffrement de la Scytale

Définition

La scytale est une méthode de chiffrement par transposition utilisée dans la Grèce antique. Elle consiste à enrouler un ruban de cuir autour d'un bâton de diamètre spécifique, appelé scytale, pour écrire un message. Une fois déroulé, le message devient illisible et ne peut être déchiffré qu'en l'enroulant autour d'une scytale de même diamètre.

- Principe : Le message est écrit en lignes successives sur le ruban enroulé. Lorsqu'il est déroulé, les lettres sont mélangées.
- Déchiffrement : Pour retrouver le message, il faut utiliser une scytale de même diamètre et ré-enrouler le ruban.

Exemple

- Message en clair : NOUS ATTAQUONS A MIDI
- Disposition en colonnes (scytale de 4 colonnes) :

N	O	U	S
A	T	T	A
Q	U	O	N
S	A	M	I
D	I	_	_

- Texte chiffré (lecture colonne par colonne) : "NAQSD OTUAI UTOM SANI".

Remarque

La scytale est une méthode de chiffrement simple mais peu sûre, car il suffit d'essayer différents diamètres de bâton pour retrouver le message. Ce chiffrement est vulnérable aux attaques par permutation.

Chiffrement de César

Définition

Le chiffrement de César est une technique de chiffrement par substitution mono-alphabétique, où chaque lettre du texte en clair est décalée d'un nombre fixe de positions dans l'alphabet.

- Principe : Le chiffrement consiste à décaler chaque lettre du texte en clair d'un nombre fixe, appelé clé, dans l'alphabet.
- Formule : Si x est la position d'une lettre dans l'alphabet, le chiffrement de César applique la transformation suivante :

$$E(x) = (x + k) \mod 26$$

où k est le décalage ou la clé.

Chiffrement de César

Exemple (Décalage de 3)

- **Texte en clair** : BONJOUR
- **Chiffrement avec** $k = 3$: Chaque lettre est décalée de 3 positions dans l'alphabet.
- **Texte chiffré** : ERQMRXU

Remarque

Le chiffrement de César est simple à appliquer, mais il est vulnérable aux attaques par analyse fréquentielle, car il conserve les fréquences des lettres du texte en clair.

Moyen Âge et Renaissance : Cryptographie manuelle

- **Chiffre de Vigenère** : Utilisation de plusieurs alphabets pour complexifier le chiffrement.
- **Stéganographie** : Art de dissimuler l'existence d'un message.
- **Systèmes secrets** : Utilisés par les diplomates et militaires pour la communication.

Exemple : Messages cachés dans des images et des illustrations.

Chiffrement de Vigenère

Définition

Le chiffrement de Vigenère est une méthode de chiffrement par substitution polyalphabétique qui utilise un mot-clé pour décaler chaque lettre du texte en clair d'un nombre de positions variable dans l'alphabet. Chaque lettre du mot-clé correspond à un décalage spécifique.

- Principe : Le mot-clé est répété pour correspondre à la longueur du message, puis chaque lettre du texte en clair est décalée selon la valeur de la lettre correspondante dans le mot-clé.
- Formule : Si x est la position d'une lettre du texte en clair et k la position de la lettre correspondante du mot-clé :

$$E(x, k) = (x + k) \mod 26$$

Exemple avec le Mot-Clé "CLE"

- Message en clair : BONJOUR
- Mot-clé : CLECLEC (répétition de "CLE")
- Calcul du texte chiffré :

Texte clair	B	O	N	J	O	U	R
Mot-clé	C	L	E	C	L	E	C
Décalage (clé)	+2	+11	+4	+2	+11	+4	+2
Texte chiffré	D	Z	R	L	Z	Y	T

- Texte chiffré obtenu : "DZRLZYT"

Remarque

Le chiffrement de Vigenère est plus résistant aux attaques par analyse fréquentielle que le chiffre de César, mais reste vulnérable si le mot-clé est court ou si des techniques de cryptanalyse spécifiques, comme la méthode de Kasiski, sont utilisées.

Seconde Guerre mondiale : Cryptographie Mécanique

- **Machine Enigma** : Complexité des rotors et câblages pour protéger les messages allemands.
- **Rôle d'Alan Turing** : Décryptage de l'Enigma par les Alliés, moment clé de la guerre.
- **Avancée de la cryptanalyse** : Développement de méthodes avancées pour décrypter.

Figure – Machine Enigma utilisée pendant la Seconde Guerre mondiale

Ère Numérique : Naissance de la Cryptographie Moderne

- **DES (Data Encryption Standard)** : Premier algorithme standard pour le chiffrement symétrique.
- **RSA** : Premier algorithme asymétrique, introduisant la cryptographie à clé publique.
- **Diffie-Hellman** : Introduction des échanges de clés publiques.

Exemple : Utilisation de RSA pour sécuriser les emails et les transactions en ligne.

Cryptographie Avancée : Années 2000 à Aujourd'hui

- **AES (Advanced Encryption Standard)** : Remplace le DES, devenu standard mondial.
- **Cryptographie elliptique** : Algorithmes avec des clés plus petites mais tout aussi sécurisées.

Exemples d'Applications de la Cryptographie

Transactions Bancaires en Ligne

Cryptographie utilisée : SSL/TLS

- Les paiements et les consultations bancaires en ligne sont protégés par le chiffrement des données via SSL/TLS.
- Le protocole assure la confidentialité des informations sensibles, telles que les numéros de carte de crédit.
- Cela empêche l'interception de ces données lors de la transmission.

Messagerie Instantanée Sécurisée

Cryptographie utilisée : Chiffrement de bout en bout (E2E)

- Applications comme WhatsApp ou Signal utilisent le chiffrement de bout en bout.
- Seuls l'expéditeur et le destinataire peuvent lire les messages.
- Même le fournisseur de l'application ne peut pas accéder aux messages échangés.

Certificats SSL/TLS pour Sites Web Sécurisés

Cryptographie utilisée : Chiffrement asymétrique (clé publique/clé privée)

- Les sites web sécurisés utilisent des certificats SSL/TLS pour établir une connexion cryptée avec les utilisateurs.
- Cela garantit la confidentialité des échanges entre le navigateur et le serveur.

Authentification à Deux Facteurs (2FA)

Cryptographie utilisée : Hachage, Codes temporaires (HOTP, TOTP)

- Le 2FA ajoute une couche de sécurité en demandant à l'utilisateur de fournir un code généré par une application ou envoyé par SMS après la saisie de son mot de passe.
- Cela garantit que même si un mot de passe est compromis, l'accès au compte reste sécurisé.

Protection des Fichiers et des Données

Cryptographie utilisée : Chiffrement symétrique (AES), Chiffrement asymétrique (RSA)

- Les fichiers sensibles sont souvent chiffrés pour les protéger contre les accès non autorisés.
- Cela garantit que seul le détenteur de la clé de déchiffrement peut accéder aux données.

Sécurité des Transactions Financières

- **Chiffrement des cartes bancaires** : Protéger les informations de carte de crédit par des méthodes de chiffrement.
- **Protocole 3D Secure** : Authentifie les utilisateurs pour prévenir les fraudes en ligne.
- **Cryptographie dans les portefeuilles numériques** : Utilisée dans les applications de paiement comme Apple Pay et Google Wallet.

Exemple : Chiffrement RSA pour sécuriser les paiements en ligne.

Authentification et Gestion des Identités

- **Mots de passe hachés** : Protection des mots de passe stockés par des fonctions de hachage sécurisées (ex : bcrypt).
- **Authentification multifactorielle (MFA)** : Combine plusieurs méthodes d'authentification pour améliorer la sécurité.
- **Biométrie et signatures numériques** : Utilise des certificats et la biométrie pour authentifier de manière fiable.

Exemple : Hachage de mots de passe pour protéger les bases de données d'utilisateurs.