
Ecole Supérieure Polytechnique
Laboratoire d'Informatique,
de Télécommunications et Applications
LITA

# Introduction générale à la Cryptologie

**Pr Gervais MENDY**
**gervais.mendy@esp.sn**

Département Génie Informatique, École Supérieure Polytechnique ESP-UCAD

March 13, 2024

# Plan

# Définitions

Cryptologie, cryptographie, cryptanalyse

- La cryptologie est la discipline qui regroupe la cryptographie et la cryptanalyse.

# Définitions

Cryptologie, cryptographie, cryptanalyse

- La cryptologie est la discipline qui regroupe la cryptographie et la cryptanalyse.
- La cryptographie peut être définie comme un art et une science permettant de concevoir des techniques pour garder le secret des messages transmis. Elle est pratiquée par des cryptographes.

# Définitions

Cryptologie, cryptographie, cryptanalyse

- La cryptologie est la discipline qui regroupe la cryptographie et la cryptanalyse.
- La cryptographie peut être définie comme un art et une science permettant de concevoir des techniques pour garder le secret des messages transmis. Elle est pratiquée par des cryptographes.
- La cryptanalyse, pratiquée par des cryptanalystes ; constitue l'ensemble des techniques qui permettent de trouver des failles dans les systèmes cryptographiques.

# Objectif de la cryptographie

**But fondamental**

L'objectif fondamental de la cryptographie est de permettre l'échange d'informations de manière sécurisée entre deux entités (personnes) à travers un canal peu sûr pouvant être espionné par un intrus.

# Histoire de la cryptographie

premiers éléments recensés cryptographiques

- Les Hiéroglyphes. Vers 1900 av. J.C., le scribe de Khnumhotep retraçait la vie de son maître dans sa tombe en utilisant un certain nombre de symboles inhabituels pour masquer le sens des inscriptions avec les hiéroglyphes qu'il dessinait.

# Histoire de la cryptographie

premiers éléments recensés cryptographiques

- Les Hiéroglyphes. Vers 1900 av. J.C., le scribe de Khnumhotep retraçait la vie de son maître dans sa tombe en utilisant un certain nombre de symboles inhabituels pour masquer le sens des inscriptions avec les hiéroglyphes qu'il dessinait.
- La scytale. Vers 500 av. J.-C., les Spartiates ont développé un dispositif appelé Scytale, qui a été utilisé pour envoyer et recevoir des messages secrets. Le dispositif est un cylindre dans lequel une bande étroite de parchemin était enroulée.

# Histoire de la cryptographie

premiers éléments recensés cryptographiques

- Les Hiéroglyphes. Vers 1900 av. J.C., le scribe de Khnumhotep retraçait la vie de son maître dans sa tombe en utilisant un certain nombre de symboles inhabituels pour masquer le sens des inscriptions avec les hiéroglyphes qu'il dessinait.
- La scytale. Vers 500 av. J.-C., les Spartiates ont développé un dispositif appelé Scytale, qui a été utilisé pour envoyer et recevoir des messages secrets. Le dispositif est un cylindre dans lequel une bande étroite de parchemin était enroulée.
- Méthode romaine. La méthode romaine la plus ancienne de cryptographie, connue sous le nom de chiffrement de César, est la première utilisation militaire enregistrée, il y a 2000 ans.

# Évolution de la cryptographie

Chiffrement d'Alberti-Vigenère

- Au milieu des années 1400, Alberti inventa un système de chiffrement basé sur un dispositif mécanique à disques coulissants qui permettait de nombreuses méthodes de substitution. C'est le concept de base d'un chiffrement poly alphabétique.

# Évolution de la cryptographie

Chiffrement d'Alberti-Vigenère

- Au milieu des années 1400, Alberti inventa un système de chiffrement basé sur un dispositif mécanique à disques coulissants qui permettait de nombreuses méthodes de substitution. C'est le concept de base d'un chiffrement poly alphabétique.
- Dans les années 1500, De Vigenère, créa un chiffrement qui fonctionne exactement comme celui de César, sauf qu'il change la clé tout au long du processus de cryptage. Le chiffrement de Vigenère utilise une grille de lettres qui donnent la méthode de substitution. Cette grille est appelée Carré de Vigenère ou Table de Vigenère.

# Évolution de la cryptographie

Le cylindre chiffrant de Jefferson

- À la fin des années 1700, Jefferson inventa un système de chiffrement très similaire au chiffrement de Vigenère, avec une sécurité plus élevée.

# Évolution de la cryptographie

Le cylindre chiffrant de Jefferson

- À la fin des années 1700, Jefferson inventa un système de chiffrement très similaire au chiffrement de Vigenère, avec une sécurité plus élevée.
- Son invention était constituée de 26 roues avec l'alphabet dispersé aléatoirement sur chaque roue. Les roues étaient numérotées et commandées avec un ordre spécifié.

# Évolution de la cryptographie

Le cylindre chiffrant de Jefferson

- À la fin des années 1700, Jefferson inventa un système de chiffrement très similaire au chiffrement de Vigenère, avec une sécurité plus élevée.
- Son invention était constituée de 26 roues avec l'alphabet dispersé aléatoirement sur chaque roue. Les roues étaient numérotées et commandées avec un ordre spécifié.
- Cet ordre est la clé de l'algorithme de chiffrement.

# Évolution de la cryptographie

Au 19 ème siècle

Ce n'est qu'après le 19 ème siècle que la cryptographie a évolué, des approches ad hoc du cryptage vers une sophistication de l'art et de la science de la sécurité de l'information.

# Évolution de la cryptographie

Première guerre mondiale

- À la fin de la Première Guerre mondiale, Arthur Scherbius inventa l'**Enigma**, une machine mécanique et électromécanique qui a été utilisée pour le cryptage et le décryptage des messages secrets.

# Évolution de la cryptographie

Première guerre mondiale

- À la fin de la Première Guerre mondiale, Arthur Scherbius inventa l'**Enigma**, une machine mécanique et électromécanique qui a été utilisée pour le cryptage et le décryptage des messages secrets.
- Les Japonais développèrent pendant cette période une machine de cryptage appelée **Purple**.

# Évolution de la cryptographie

Première guerre mondiale

- À la fin de la Première Guerre mondiale, Arthur Scherbius inventa l'**Enigma**, une machine mécanique et électromécanique qui a été utilisée pour le cryptage et le décryptage des messages secrets.
- Les Japonais développèrent pendant cette période une machine de cryptage appelée **Purple**.
- Plus tard les américains construisirent une machine pour déchiffrer le Purple.

# Évolution de la cryptographie

Deuxième guerre mondiale

- Pendant la période de la Seconde Guerre mondiale, la cryptographie et la cryptanalyse deviennent excessivement mathématiques.

# Évolution de la cryptographie

Deuxième guerre mondiale

- Pendant la période de la Seconde Guerre mondiale, la cryptographie et la cryptanalyse deviennent excessivement mathématiques.
- Les progrès réalisés dans ce domaine ont permis aux organisations gouvernementales, aux unités militaires et à certaines corporations d'adopter les applications de la cryptographie.

# Évolution de la cryptographie

Deuxième guerre mondiale

- Pendant la période de la Seconde Guerre mondiale, la cryptographie et la cryptanalyse deviennent excessivement mathématiques.
- Les progrès réalisés dans ce domaine ont permis aux organisations gouvernementales, aux unités militaires et à certaines corporations d'adopter les applications de la cryptographie.
- Aujourd'hui, l'arrivée des ordinateurs et de l'Internet a rendu la cryptographie accessible au grand public.

# Cryptographie moderne

## Cryptographie moderne

La cryptographie moderne est la pierre angulaire de la sécurité des ordinateurs et des communications. Elle s'appuie sur différents concepts de mathématiques tels que:

- la théorie des nombres,

# Cryptographie moderne

## Cryptographie moderne

La cryptographie moderne est la pierre angulaire de la sécurité des ordinateurs et des communications. Elle s'appuie sur différents concepts de mathématiques tels que:

- la théorie des nombres,
- la théorie de la complexité

# Cryptographie moderne

## Cryptographie moderne

La cryptographie moderne est la pierre angulaire de la sécurité des ordinateurs et des communications. Elle s'appuie sur différents concepts de mathématiques tels que:

- la théorie des nombres,
- la théorie de la complexité
- et la théorie des probabilités.

# Caractéristiques de la cryptographie moderne

classique vs moderne

Il existe trois caractéristiques principales qui séparent la cryptographie moderne de l'approche classique.

- **classique**: elle manipule les caractères traditionnels, c'est-à-dire les lettres et les chiffres directement.
  **moderne**: elle opère sur des séquences de bits.

# Caractéristiques de la cryptographie moderne

classique vs moderne

- **classique**: Elle repose principalement sur la *sécurité par l'obscurité*. Les techniques employées pour le codage sont gardées secrètes et seules les parties impliquées dans la communication le savent.
  **moderne**: Elle s'appuie sur des algorithmes mathématiques connus publiquement pour coder l'information. Le secret est obtenu par une clé secrète qui est utilisée comme graine pour les algorithmes. La difficulté de calcul des algorithmes, l'absence de clé secrète, etc, rendent impossible l'obtention de l'information originale par un attaquant même s'il connaît l'algorithme utilisé pour le codage.

# Caractéristiques de la cryptographie moderne

classique vs moderne

- **classique**: Elle nécessite l'ensemble du cryptosystème pour communiquer en toute confiance.
  **moderne**: La cryptographie moderne exige que les parties intéressées par la communication sécurisée possèdent uniquement la clé secrète.

# Les services de sécurité

Les services fondamentaux

Le but premier de l'utilisation de la cryptographie est de garantir les quatre services fondamentaux de la sécurité des informations :

- la confidentialité,

# Les services de sécurité

Les services fondamentaux

Le but premier de l'utilisation de la cryptographie est de garantir les quatre services fondamentaux de la sécurité des informations :

- la confidentialité,
- l'intégrité des données,

# Les services de sécurité

Les services fondamentaux

Le but premier de l'utilisation de la cryptographie est de garantir les quatre services fondamentaux de la sécurité des informations :

- la confidentialité,
- l'intégrité des données,
- l'authentification

# Les services de sécurité

Les services fondamentaux

Le but premier de l'utilisation de la cryptographie est de garantir les quatre services fondamentaux de la sécurité des informations :

- la confidentialité,
- l'intégrité des données,
- l'authentification
- et la non-répudiation.

# Les services de sécurité

La confidentialité

- C'est un service de sécurité qui préserve l'information d'une personne non autorisée. On parle parfois de vie privée ou de secret.

# Les services de sécurité

La confidentialité

- C'est un service de sécurité qui préserve l'information d'une personne non autorisée. On parle parfois de vie privée ou de secret.
- La confidentialité peut être obtenue grâce à de nombreux moyens allant de la sécurisation physique à l'utilisation d'algorithmes mathématiques pour le cryptage des données.

# Les services de sécurité

L'intégrité des données

- C'est le service de sécurité qui s'occupe d'identifier toute altération des données.

# Les services de sécurité

L'intégrité des données

- C'est le service de sécurité qui s'occupe d'identifier toute altération des données.
- Le destinataire d'un message doit pouvoir vérifier que celui-ci n'a pas été modifié en chemin.

# Les services de sécurité

L'intégrité des données

- C'est le service de sécurité qui s'occupe d'identifier toute altération des données.
- Le destinataire d'un message doit pouvoir vérifier que celui-ci n'a pas été modifié en chemin.
- Un intrus ne doit pas être capable de faire passer un faux message pour un légitime.

# Les services de sécurité

L'authentification

- L'authentification fournit l'identification de l'auteur.

# Les services de sécurité

L'authentification

- L'authentification fournit l'identification de l'auteur.
- Il confirme au destinataire que les données reçues ont été envoyées par un expéditeur identifié et vérifié.

# Les services de sécurité

L'authentification

- L'authentification fournit l'identification de l'auteur.
- Il confirme au destinataire que les données reçues ont été envoyées par un expéditeur identifié et vérifié.
- Un intrus ne doit pas être capable de se faire passer pour quelqu'un d'autre.

# Les services de sécurité

L'authentification

Le service d'authentification comporte deux variantes:

- L'authentification de message identifie l'auteur du message sans aucun routeur ou système qui envoie le message.

# Les services de sécurité

L'authentification

Le service d'authentification comporte deux variantes:

- L'authentification de message identifie l'auteur du message sans aucun routeur ou système qui envoie le message.
- L'authentification d'entité est l'assurance que la donnée a été reçue d'une entité spécifique, par exemple un site Web particulier.

# Les services de sécurité

La non-répudiation ou le non-désaveu

- C'est un service de sécurité qui garantit qu'une entité ne peut pas refuser la propriété d'un engagement antérieur ou d'une action.

# Les services de sécurité

La non-répudiation ou le non-désaveu

- C'est un service de sécurité qui garantit qu'une entité ne peut pas refuser la propriété d'un engagement antérieur ou d'une action.
- La non-répudiation est une propriété qui est la plus souhaitable dans les situations où il y a des possibilités de conflit sur l'échange de données.

# Primitives cryptographiques

Primitives cryptographiques

Les primitives cryptographiques ne sont rien d'autre que les outils et techniques de la cryptographie qui peuvent être sélectivement utilisés pour fournir un ensemble de services de sécurité souhaités :

- Chiffrement

Les primitives cryptographiques sont intimement liées et elles sont souvent combinées pour obtenir un ensemble de services de sécurité souhaités à partir d'un cryptosystème.

# Primitives cryptographiques

Primitives cryptographiques

Les primitives cryptographiques ne sont rien d'autre que les outils et techniques de la cryptographie qui peuvent être sélectivement utilisés pour fournir un ensemble de services de sécurité souhaités :

- Chiffrement
- Fonctions de hachage

Les primitives cryptographiques sont intimement liées et elles sont souvent combinées pour obtenir un ensemble de services de sécurité souhaités à partir d'un cryptosystème.

# Primitives cryptographiques

Primitives cryptographiques

Les primitives cryptographiques ne sont rien d'autre que les outils et techniques de la cryptographie qui peuvent être sélectivement utilisés pour fournir un ensemble de services de sécurité souhaités :

- Chiffrement
- Fonctions de hachage
- Codes d'Authentification des Messages (MAC)

Les primitives cryptographiques sont intimement liées et elles sont souvent combinées pour obtenir un ensemble de services de sécurité souhaités à partir d'un cryptosystème.

# Primitives cryptographiques

Primitives cryptographiques

Les primitives cryptographiques ne sont rien d'autre que les outils et techniques de la cryptographie qui peuvent être sélectivement utilisés pour fournir un ensemble de services de sécurité souhaités :

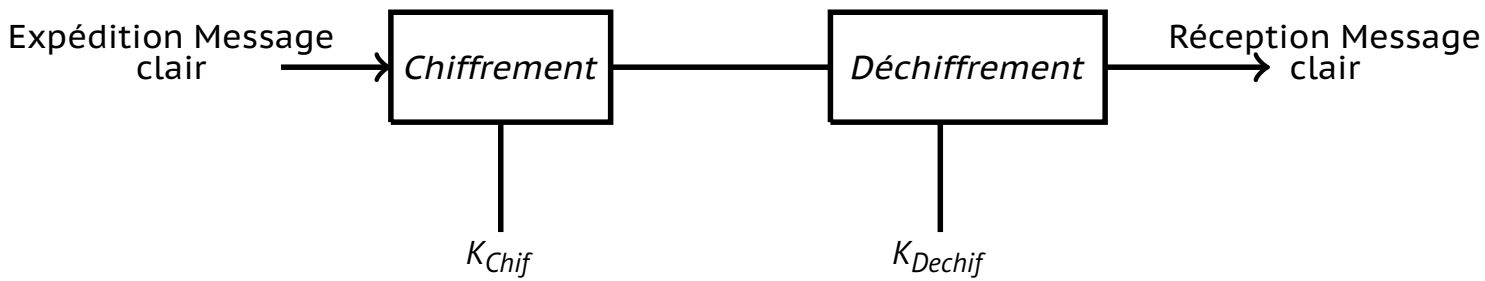
- Chiffrement
- Fonctions de hachage
- Codes d'Authentification des Messages (MAC)
- Signatures numériques

Les primitives cryptographiques sont intimement liées et elles sont souvent combinées pour obtenir un ensemble de services de sécurité souhaités à partir d'un cryptosystème.

# Cryptosystème

Définition

Un cryptosystème est une implémentation de techniques cryptographiques et de leur infrastructure d'accompagnement pour fournir des services de sécurité de l'information. Un cryptosystème est également appelé **système de chiffrement**.
Le modèle de base est représenté dans l'illustration de la figure suivante



# Les composantes d'un cryptosystème

Définitions

- **Texte en clair**. Ce sont les données à protéger pendant la transmission.

# Les composantes d'un cryptosystème

Définitions

- **Texte en clair**. Ce sont les données à protéger pendant la transmission.
- **Chiffrement**. C'est un processus de transformation d'un message de manière à le rendre incompréhensible. Le résultat de ce processus de chiffrement est appelé **texte chiffré** ou encore **cryptogramme**.

# Les composantes d'un cryptosystème

Définitions

- **Texte en clair**. Ce sont les données à protéger pendant la transmission.
- **Chiffrement**. C'est un processus de transformation d'un message de manière à le rendre incompréhensible. Le résultat de ce processus de chiffrement est appelé **texte chiffré** ou encore **cryptogramme**.
- **Texte chiffré**. C'est la version brouillée du texte en clair produit par le chiffrement. Le texte chiffré n'est pas protégé. Il circule sur le canal public et il peut être intercepté ou compromis par quiconque qui a accès au canal de communication.

# Les composantes d'un cryptosystème

Définitions

- **Texte en clair**. Ce sont les données à protéger pendant la transmission.
- **Chiffrement**. C'est un processus de transformation d'un message de manière à le rendre incompréhensible. Le résultat de ce processus de chiffrement est appelé **texte chiffré** ou encore **cryptogramme**.
- **Texte chiffré**. C'est la version brouillée du texte en clair produit par le chiffrement. Le texte chiffré n'est pas protégé. Il circule sur le canal public et il peut être intercepté ou compromis par quiconque qui a accès au canal de communication.
- **Déchiffrement**. C'est le processus de reconstruction du texte en clair à partir du texte chiffré.

# Les composantes d'un cryptosystème

Définitions

- **algorithme cryptographique**. C'est une fonction mathématique utilisée pour le chiffrement et le déchiffrement.

# Les composantes d'un cryptosystème

Définitions

- **algorithme cryptographique**. C'est une fonction mathématique utilisée pour le chiffrement et le déchiffrement.
- **Clé de chiffrement**. C'est une valeur qui est connue de l'expéditeur. L'expéditeur entre la clé de chiffrement dans l'algorithme de chiffrement avec le texte en clair afin de calculer le texte chiffré.

# Les composantes d'un cryptosystème

Définitions

- **algorithme cryptographique**. C'est une fonction mathématique utilisée pour le chiffrement et le déchiffrement.
- **Clé de chiffrement**. C'est une valeur qui est connue de l'expéditeur. L'expéditeur entre la clé de chiffrement dans l'algorithme de chiffrement avec le texte en clair afin de calculer le texte chiffré.
- **Clé de déchiffrement**. C'est une valeur qui est connue du récepteur. La clé de décryptage est liée à la clé de chiffrement, mais n'est pas toujours identique à celle-ci. Le récepteur saisit la clé de décryptage dans l'algorithme de décryptage avec le texte chiffré pour calculer le texte en clair.

# Les composantes d'un cryptosystème

Définitions

Pour un cryptosystème donné, un ensemble de toutes les clés possibles de déchiffrement est appelée un **espace des clefs**.
Un intercepteur (attaquant) est une entité non autorisée qui tente de déterminer le texte en clair. Il peut voir le texte chiffré et peut connaître l'algorithme de déchiffrement. Cependant, il ne doit jamais connaître la clé de déchiffrement.

# Les types fondamentaux

Deux types

- le chiffrement symétrique

# Les types fondamentaux

Deux types

- le chiffrement symétrique
- le chiffrement asymétrique

# Le chiffrement symétrique

La cryptographie symétrique

- Le processus de chiffrement où les mêmes clés sont utilisées pour crypter et déchiffrer les informations, est connu sous le nom chiffrement symétrique.

# Le chiffrement symétrique

La cryptographie symétrique

- Le processus de chiffrement où les mêmes clés sont utilisées pour crypter et déchiffrer les informations, est connu sous le nom chiffrement symétrique.
- L'étude des cryptosystèmes symétriques est appelée cryptographie symétrique.

# Le chiffrement symétrique

La cryptographie symétrique

- Le processus de chiffrement où les mêmes clés sont utilisées pour crypter et déchiffrer les informations, est connu sous le nom chiffrement symétrique.
- L'étude des cryptosystèmes symétriques est appelée cryptographie symétrique.
- Les cryptosystèmes symétriques sont aussi parfois appelés cryptosystèmes à clés secrètes.

# Le chiffrement symétrique

Les caractéristiques du chiffrement symétrique

Les principales caractéristiques du cryptosystème basé sur le chiffrement symétrique sont:

- Le processus de chiffrement où les mêmes clés sont utilisées pour crypter et déchiffrer les informations, est connu sous le nom chiffrement symétrique.

# Le chiffrement symétrique

Les caractéristiques du chiffrement symétrique

Les principales caractéristiques du cryptosystème basé sur le chiffrement symétrique sont:

- Le processus de chiffrement où les mêmes clés sont utilisées pour crypter et déchiffrer les informations, est connu sous le nom chiffrement symétrique.
- Il est recommandé de changer régulièrement les clés pour éviter toute attaque du système.

# Le chiffrement symétrique

Les caractéristiques du chiffrement symétrique

Les principales caractéristiques du cryptosystème basé sur le chiffrement symétrique sont:

- Le processus de chiffrement où les mêmes clés sont utilisées pour crypter et déchiffrer les informations, est connu sous le nom chiffrement symétrique.
- Il est recommandé de changer régulièrement les clés pour éviter toute attaque du système.
- Un mécanisme robuste doit exister pour échanger les clés entre les parties communicantes. Comme les clés doivent être changées régulièrement, ce mécanisme devient coûteux et encombrant.

# Le chiffrement symétrique

Les caractéristiques du chiffrement symétrique (suite)

- Dans un groupe de $n$ personnes, pour permettre la communication bipartite entre deux personnes quelconques, le nombre de clés requises pour le groupe est $n \times (n-1)/2$.

# Le chiffrement symétrique

Les caractéristiques du chiffrement symétrique (suite)

- Dans un groupe de $n$ personnes, pour permettre la communication bipartite entre deux personnes quelconques, le nombre de clés requises pour le groupe est $n \times (n-1)/2$.
- La longueur de la clé (nombre de bits) dans ce chiffrement est plus faible et, par conséquent, le processus de chiffrement-déchiffrement est plus rapide que le chiffrement de clé asymétrique.

# Le chiffrement symétrique

Les caractéristiques du chiffrement symétrique (suite)

- Dans un groupe de $n$ personnes, pour permettre la communication bipartite entre deux personnes quelconques, le nombre de clés requises pour le groupe est $n \times (n-1)/2$.
- La longueur de la clé (nombre de bits) dans ce chiffrement est plus faible et, par conséquent, le processus de chiffrement-déchiffrement est plus rapide que le chiffrement de clé asymétrique.
- La puissance de traitement du système informatique requis pour exécuter l'algorithme symétrique est moindre.

# Le chiffrement symétrique

Défis restrictifs du chiffrement symétrique

- **Établissement de la clé** - Avant toute communication, l'expéditeur et le destinataire doivent convenir d'une clé symétrique secrète. Il exige un mécanisme d'établissement sur place de clé sécurisé.

# Le chiffrement symétrique

Défis restrictifs du chiffrement symétrique

- **Établissement de la clé** - Avant toute communication, l'expéditeur et le destinataire doivent convenir d'une clé symétrique secrète. Il exige un mécanisme d'établissement sur place de clé sécurisé.
- **Problème de confiance** - Étant donné que l'émetteur et le récepteur utilisent la même clé symétrique, il existe une exigence implicite selon laquelle l'émetteur et le récepteur «se font confiance».

# Le chiffrement asymétrique

Définition

Le processus de chiffrement dans lequel différentes clés sont utilisées pour crypter et déchiffrer les informations est connu sous le nom de chiffrement asymétrique. Bien que les clés soient différentes, elles sont mathématiquement liées et, par conséquent, la récupération du texte en clair par décryptage du texte chiffré est possible.

# Le chiffrement asymétrique

Les caractéristiques du chiffrement asymétrique

Les caractéristiques saillantes du chiffrement asymétrique sont:

- Chaque utilisateur de ce système doit posséder une paire de clés différentes, une clé privée et une clé publique. Ces clés sont mathématiquement liées - lorsqu'une clé est utilisée pour le cryptage, l'autre peut déchiffrer le texte chiffré de nouveau au texte en clair original.

# Le chiffrement asymétrique

Les caractéristiques du chiffrement asymétrique

Les caractéristiques saillantes du chiffrement asymétrique sont:

- Chaque utilisateur de ce système doit posséder une paire de clés différentes, une clé privée et une clé publique. Ces clés sont mathématiquement liées - lorsqu'une clé est utilisée pour le cryptage, l'autre peut déchiffrer le texte chiffré de nouveau au texte en clair original.
- Il faut mettre la clé publique dans le dépôt public et la clé privée comme un secret bien gardé, d'où le nom de chiffrement à clé publique.

# Le chiffrement asymétrique

Les caractéristiques du chiffrement asymétrique

Les caractéristiques saillantes du chiffrement asymétrique sont:

- Chaque utilisateur de ce système doit posséder une paire de clés différentes, une clé privée et une clé publique. Ces clés sont mathématiquement liées - lorsqu'une clé est utilisée pour le cryptage, l'autre peut déchiffrer le texte chiffré de nouveau au texte en clair original.
- Il faut mettre la clé publique dans le dépôt public et la clé privée comme un secret bien gardé, d'où le nom de chiffrement à clé publique.
- Bien que les clés publique et privée de l'utilisateur soient liées, il n'est pas possible de les trouver par ordinateur. C'est une force de ce schéma.

# Le chiffrement asymétrique

Les caractéristiques du chiffrement asymétrique (suite)

- Lorsque l'hôte 1 doit envoyer des données à l'hôte 2, il récupère la clé publique de l'hôte 2, crypte les données et les transmet.

# Le chiffrement asymétrique

Les caractéristiques du chiffrement asymétrique (suite)

- Lorsque l'hôte 1 doit envoyer des données à l'hôte 2, il récupère la clé publique de l'hôte 2, crypte les données et les transmet.
- L'hôte 2 utilise sa clé privée pour extraire le texte en clair.

# Le chiffrement asymétrique

Les caractéristiques du chiffrement asymétrique (suite)

- Lorsque l'hôte 1 doit envoyer des données à l'hôte 2, il récupère la clé publique de l'hôte 2, crypte les données et les transmet.
- L'hôte 2 utilise sa clé privée pour extraire le texte en clair.
- La longueur des clés (nombre de bits) dans ce cryptage est grande et donc, le processus de chiffrement-déchiffrement est plus lent que le chiffrement de clé symétrique.

# Le chiffrement asymétrique

Les caractéristiques du chiffrement asymétrique (suite)

- Lorsque l'hôte 1 doit envoyer des données à l'hôte 2, il récupère la clé publique de l'hôte 2, crypte les données et les transmet.
- L'hôte 2 utilise sa clé privée pour extraire le texte en clair.
- La longueur des clés (nombre de bits) dans ce cryptage est grande et donc, le processus de chiffrement-déchiffrement est plus lent que le chiffrement de clé symétrique.
- La puissance de traitement du système informatique requise pour exécuter l'algorithme asymétrique est plus élevée.

# Le chiffrement asymétrique

Défi du chiffrement asymétrique

- l'utilisateur doit s'assurer que la clé publique qu'il utilise dans les communications avec une personne est vraiment la clé publique de cette personne et qu'elle n'a pas été falsifiée par un tiers malveillant.

[a] Public Key Infrastructure

# Le chiffrement asymétrique

Défi du chiffrement asymétrique

- l'utilisateur doit s'assurer que la clé publique qu'il utilise dans les communications avec une personne est vraiment la clé publique de cette personne et qu'elle n'a pas été falsifiée par un tiers malveillant.
- Ceci est habituellement réalisé par l'intermédiaire d'une Infrastructure à Clé Publique (PKI[a]) constituée par un tiers de confiance. Le tiers gère et atteste en toute sécurité l'authenticité des clés publiques.

[a] Public Key Infrastructure

# Principe de Kerckhoff

Les six principes de Kerckhoff

Les principes de la cryptographie moderne furent posés par Auguste Kerckhoff.

- Le cryptosystème devrait être incassable pratiquement, sauf mathématiquement.

# Principe de Kerckhoff

Les six principes de Kerckhoff

Les principes de la cryptographie moderne furent posés par Auguste Kerckhoff.

- Le cryptosystème devrait être incassable pratiquement, sauf mathématiquement.
- La chute du cryptosystème dans les mains d'un intrus ne doit pas conduire à une compromission du système, et doit empêcher tout inconvénient pour l'utilisateur.

# Principe de Kerckhoff

Les six principes de Kerckhoff

Les principes de la cryptographie moderne furent posés par Auguste Kerckhoff.

- Le cryptosystème devrait être incassable pratiquement, sauf mathématiquement.
- La chute du cryptosystème dans les mains d'un intrus ne doit pas conduire à une compromission du système, et doit empêcher tout inconvénient pour l'utilisateur.
- La clé doit être facilement transmissible, mémorable et changeable.

# Principe de Kerckhoff

Les six principes de Kerckhoff (suite)

- Le texte chiffré doit être transmissible par télégraphe, par un canal non sécurisé.

# Principe de Kerckhoff

Les six principes de Kerckhoff (suite)

- Le texte chiffré doit être transmissible par télégraphe, par un canal non sécurisé.
- Le matériel et les documents de cryptage doivent être portables et exploitables par une seule personne.

# Principe de Kerckhoff

Les six principes de Kerckhoff (suite)

- Le texte chiffré doit être transmissible par télégraphe, par un canal non sécurisé.
- Le matériel et les documents de cryptage doivent être portables et exploitables par une seule personne.
- Enfin, il est nécessaire que le système soit facile à utiliser, ne nécessitant ni souci mental, ni la connaissance d'une longue série de règles à observer.

# Principe de Kerckhoff

Remarque

La deuxième règle est actuellement connue sous le nom de principe de Kerckhoff. Il est appliqué dans pratiquement tous les algorithmes de chiffrement contemporains. Ces algorithmes publics sont considérés comme parfaitement sécurisés. La sécurité du message chiffré dépend uniquement de la sécurité de la clé de chiffrement secrète.

# Attaques sur les cryptosystèmes

## Définition et nature des attaques

Une tentative de cryptanalyse est appelée **attaque**. Les attaques sont généralement catégorisées en fonction de l'action effectuée par l'attaquant. Une attaque, peut donc être:

- **passive**

# Attaques sur les cryptosystèmes

Définition et nature des attaques

Une tentative de cryptanalyse est appelée **attaque**. Les attaques sont généralement catégorisées en fonction de l'action effectuée par l'attaquant. Une attaque, peut donc être:

- **passive**
- ou **active**.

# Attaques passive

Objectif de l'attaque passive

- Le but principal d'une attaque passive est d'obtenir un accès non autorisé à l'information.

# Attaques passive

Objectif de l'attaque passive

- Le but principal d'une attaque passive est d'obtenir un accès non autorisé à l'information.
- Par exemple, des actions telles que l'interception et l'écoute sur le canal de communication peuvent être considérées comme des attaques passives.

# Attaques passive

Objectif de l'attaque passive

- Le but principal d'une attaque passive est d'obtenir un accès non autorisé à l'information.
- Par exemple, des actions telles que l'interception et l'écoute sur le canal de communication peuvent être considérées comme des attaques passives.
- Ces actions sont de nature passive, car elles n'influencent pas l'information ni ne perturbent le canal de communication. Une attaque passive est souvent perçue comme un vol d'information.

# Attaques actives

impact des attaques actives

Une attaque active implique de changer l'information d'une certaine manière en effectuant un processus sur l'information. Par exemple,

- Modification des informations d'une manière non autorisée.

# Attaques actives

impact des attaques actives

Une attaque active implique de changer l'information d'une certaine manière en effectuant un processus sur l'information. Par exemple,

- Modification des informations d'une manière non autorisée.
- Initier la transmission non intentionnelle ou non autorisée d'informations.

# Attaques actives

impact des attaques actives

Une attaque active implique de changer l'information d'une certaine manière en effectuant un processus sur l'information. Par exemple,

- Modification des informations d'une manière non autorisée.
- Initier la transmission non intentionnelle ou non autorisée d'informations.
- Altération des données d'authentification telles que le nom de l'auteur ou l'horodatage associé aux informations.

# Attaques actives

impact des attaques actives

Une attaque active implique de changer l'information d'une certaine manière en effectuant un processus sur l'information. Par exemple,

- Modification des informations d'une manière non autorisée.
- Initier la transmission non intentionnelle ou non autorisée d'informations.
- Altération des données d'authentification telles que le nom de l'auteur ou l'horodatage associé aux informations.
- Suppression non autorisée des données.

# Attaques actives

impact des attaques actives

Une attaque active implique de changer l'information d'une certaine manière en effectuant un processus sur l'information. Par exemple,

- Modification des informations d'une manière non autorisée.
- Initier la transmission non intentionnelle ou non autorisée d'informations.
- Altération des données d'authentification telles que le nom de l'auteur ou l'horodatage associé aux informations.
- Suppression non autorisée des données.
- Refus d'accès à l'information pour les utilisateurs légitimes (déni de service).

# Attaques cryptographiques

Attaquant

- L'intention de base d'un attaquant est de briser un cryptosystème et de trouver le texte en clair à partir du texte chiffré.

# Attaques cryptographiques

Attaquant

- L'intention de base d'un attaquant est de briser un cryptosystème et de trouver le texte en clair à partir du texte chiffré.
- Pour obtenir le texte en clair, l'attaquant n'a besoin que de trouver la clé de déchiffrement secrète, car l'algorithme est déjà dans le domaine public.

# Attaques cryptographiques

Attaquant

- L'intention de base d'un attaquant est de briser un cryptosystème et de trouver le texte en clair à partir du texte chiffré.
- Pour obtenir le texte en clair, l'attaquant n'a besoin que de trouver la clé de déchiffrement secrète, car l'algorithme est déjà dans le domaine public.
- Une fois que l'attaquant est en mesure de déterminer la clé, le système attaqué est considéré comme cassé ou compromis.

# Attaques cryptographiques

Classification des attaques

- **L'attaque à texte chiffré seulement**[a]. Le cryptanalyste dispose du texte chiffré de plusieurs messages, tous ayant été chiffrés avec le même algorithme. La tâche du cryptanalyste est de retrouver le texte en clair du plus grand nombre possible de messages ou mieux encore de trouver la ou les clefs qui ont été utilisées pour chiffrer les messages ce qui permettrait de déchiffrer d'autres messages chiffrés avec ces mêmes clefs.

[a] Ciphertext Only Attacks (COA)

# Attaques cryptographiques

Classification des attaques (suite 1)

- **L'attaque à texte en clair connu**[a]. Le cryptanalyste a non seulement accès aux textes chiffrés de plusieurs messages mais aussi aux textes en clair correspondants. La tâche est de retrouver la ou les clefs utilisées pour chiffrer ces messages ou un algorithme qui permet de déchiffrer n'importe quel nouveau message chiffré avec la même clef.

[a] Known Plaintext Attack (KPA)

# Attaques cryptographiques

Classification des attaques (suite 2)

- **L'attaque à texte en clair choisi**[a]. Non seulement le cryptanalyste a accès aux textes chiffrés et aux textes en clair, mais de plus il peut choisir les textes en clair à chiffrer. Cette attaque est plus efficace que l'attaque à texte en clair connu car le cryptanalyste peut choisir des textes en clair spécifiques qui donneront plus d'informations sur la clef. La tâche consiste à retrouver la ou les clefs utilisées pour chiffrer ces messages ou un algorithme qui permette de déchiffrer n'importe quel nouveau message chiffré avec la même clef.

[a] Chosen Plaintext Attack (CPA)

# Attaques cryptographiques

Classification des attaques (suite 3)

- **L'attaque à texte en clair choisi adaptative (ou dynamique)**. C'est un cas particulier de l'attaque à texte en clair choisi. Non seulement le cryptanalyste peut choisir les textes en clair mais il peut également adapter ses choix en fonction des textes chiffrés précédents. Dans une attaque à texte en clair choisi, le cryptanalyste est juste autorisé à choisir un grand bloc de texte en clair au départ tandis que dans une attaque à texte en clair adaptative, il choisit un bloc initial plus petit et ensuite il peut choisir un autre bloc en fonction du résultat pour le premier et ainsi de suite.

# Attaques cryptographiques

Classification des attaques (suite 4)

- **L'attaque à texte chiffré choisi**. Le cryptanalyste peut choisir différents textes chiffrés à déchiffrer. Les textes déchiffrés lui sont alors fournis. Par exemple, le cryptanalyste a un dispositif qui ne peut être desassemblé et qui fait du déchiffrement automatique; sa tâche est de retrouver la clef. Ce type d'attaque est principalement applicable aux cryptosystèmes à clef publique.

# Attaques cryptographiques

Classification des attaques (suite 4)

- **L'attaque à texte chiffré choisi**. Le cryptanalyste peut choisir différents textes chiffrés à déchiffrer. Les textes déchiffrés lui sont alors fournis. Par exemple, le cryptanalyste a un dispositif qui ne peut être desassemblé et qui fait du déchiffrement automatique; sa tâche est de retrouver la clef. Ce type d'attaque est principalement applicable aux cryptosystèmes à clef publique.
- **L'attaque à clef choisie**. Cela n'est pas une attaque où le cryptanalyste peut choisir la clef; il est seulement au courant de quelques relations entre différentes clefs.

# Attaques cryptographiques

Classification des attaques (suite 5)

- **Attaque par dictionnaire**. Cette attaque a de nombreuses variantes, qui impliquent toute la compilation d'un «dictionnaire». Dans la méthode la plus simple de cette attaque, l'attaquant construit un dictionnaire des textes chiffrés et des textes en clair correspondants qu'il a appris sur une période de temps. À l'avenir, lorsqu'un attaquant obtient le texte chiffré, il se refère au dictionnaire pour trouver le texte en clair correspondant.

# Attaques cryptographiques

Classification des attaques (suite 6)

- **Attaque par force brute**[a]: Dans cette méthode, l'attaquant essaie de déterminer la clé en essayant toutes les clés possibles. Si la clé est de 8 bits, alors le nombre de clés possibles est $2^8 = 256$. L'attaquant connaît le texte chiffré et l'algorithme, maintenant il tente toutes les 256 clés une par une pour le décryptage.

[a] Brute Force Attack (BFA)
[b] Man in Middle Attack (MIM)

# Attaques cryptographiques

Classification des attaques (suite 6)

- **Attaque par force brute**[a]: Dans cette méthode, l'attaquant essaie de déterminer la clé en essayant toutes les clés possibles. Si la clé est de 8 bits, alors le nombre de clés possibles est $2^8 = 256$. L'attaquant connaît le texte chiffré et l'algorithme, maintenant il tente toutes les 256 clés une par une pour le décryptage.
- **L'Attaque de l'homme du milieu** [b]: Les cibles de cette attaque sont principalement des cryptosystèmes à clé publique où l'échange de clés est engagé avant que la communication ait lieu.

[a] Brute Force Attack (BFA)
[b] Man in Middle Attack (MIM)

# Fin du chapitre

Merci de votre Attention