

HYIRECPOPBRATG

ALLOGHRCRYPER
PTFCPAOHYIRGR
VEGNRECALLYPO
YGPAAORHPTIRCH
IPRPOYAFEGTLOH
LFORHIPPYGPSCA
EOCYATRIPRGGHP
GCHIREYTROPAR
PHALRGIEOGRIPY
RAPEYPIIGCHORI
OPRGIREPHACTYI
CRYPTOGRAPHIE

David Kohel

Institut de Mathématiques de Luminy

Master ISARC 2008

CRYPTOGRAPHIE

David Kohel

Institut de Mathématiques de Luminy

Master ISARC 2008

PTFCPAOHYIRGR

David Kohel

Institut de Mathématiques de Luminy

Master ISARC 2008

REGHRPCAITYPO

David Kohel

Institut de Mathématiques de Luminy

Master ISARC 2008

YGPAQRHPTEIRC

David Kohel

Institut de Mathématiques de Luminy

Master ISARC 2008

IPRPCYAREGTOH

David Kohel

Institut de Mathématiques de Luminy

Master ISARC 2008

TROHIPYGPECA

David Kohel

Institut de Mathématiques de Luminy

Master ISARC 2008

EOCYATRIPRGHP

David Kohel

Institut de Mathématiques de Luminy

Master ISARC 2008

GCHIPEYTROPAR

David Kohel

Institut de Mathématiques de Luminy

Master ISARC 2008

PHATRGIEOCRPY

David Kohel

Institut de Mathématiques de Luminy

Master ISARC 2008

CRYPTOGRAPHIE

RAPEYPTGCHORI

David Kohel

Institut de Mathématiques de Luminy

Master ISARC 2008

CRYPTOGRAPHIE

David Kohel

Institut de Mathématiques de Luminy

Master ISARC 2008



CRYPTOGRAPHIE

David Kohel

Institut de Mathématiques de Luminy

Master ISARC 2008

RÉSUMÉ

1

Introduction

- Cryptographie, cryptanalyse, et cryptologie
- Transmission d'information
- Sécurité de l'information

2

Concepts cryptographiques

- Concepts et définitions
- Cryptosystèmes

RÉSUMÉ

1

Introduction

- Cryptographie, cryptanalyse, et cryptologie
- Transmission d'information
- Sécurité de l'information

2

Concepts cryptographiques

- Concepts et définitions
- Cryptosystèmes

Qu'est-ce que c'est la cryptographie ?

La **cryptographie** concerne les méthodes et les outils pour écriture secrète — envoyer des messages sur un canal non sécurisé tel que seuls l'expéditeur et le destinataire autorisé peuvent les lire.

La **cryptanalyse** concerne les méthodes et les outils pour trouver les faiblesses dans les communications cryptographiques.

L'ensemble de ce deux parties s'appelle la **cryptologie**.

Les problèmes de la théorie de l'information

- La représentation d'information — *concerne le codage : comment représenter les formes diverses d'information par les mots écrit avec les lettres d'un alphabet, soit $\{A, \dots, Z\}$ soit $\{0, 1\}$; et la compression : comment le faire en utilisant l'espace minimal.*
- L'intégrité d'information — *concerne la détection et la correction des erreurs qui surviennent lors de la transmission d'information.*
- La sécurité d'information — *concerne la confidentialité de l'information et la protection de son intégrité.*

Les problèmes de la théorie de l'information

- La représentation d'information — *concerne le **codage** : comment représenter les formes diverses d'information par les mots écrit avec les lettres d'un alphabet, soit $\{A, \dots, Z\}$ soit $\{0, 1\}$; et la **compression** : comment le faire en utilisant l'espace minimal.*
- L'intégrité d'information — *concerne la détection et la correction d'erreurs qui survient en raison du bruit dans le canal de transmission ; c'est traité dans la théorie des codes correcteurs d'erreurs.*
- La sécurité d'information

Les problèmes de la théorie de l'information

- La représentation d'information — *concerne le **codage** : comment représenter les formes diverses d'information par les mots écrit avec les lettres d'un alphabet, soit $\{A, \dots, Z\}$ soit $\{0, 1\}$; et la **compression** : comment le faire en utilisant l'espace minimal.*
- L'intégrité d'information — *concerne la détection et la correction d'erreurs qui survient en raison du bruit dans le canal de transmission ; c'est traité dans la théorie des codes correcteurs d'erreurs.*
- La sécurité d'information — *concerne la confidentialité des données transmises et l'authentification des messages et des personnes ; ce sont les objectifs principaux de la cryptographie.*

Les problèmes de la théorie de l'information

- La représentation d'information — *concerne le **codage** : comment représenter les formes diverses d'information par les mots écrit avec les lettres d'un alphabet, soit $\{A, \dots, Z\}$ soit $\{0, 1\}$; et la **compression** : comment le faire en utilisant l'espace minimal.*
- L'intégrité d'information — *concerne la détection et la correction d'erreurs qui survient en raison du bruit dans le canal de transmission ; c'est traité dans la théorie des codes correcteurs d'erreurs.*
- La sécurité d'information — *concerne la confidentialité des données transmises et l'authentification des messages et des personnes ; ce sont les objectifs principaux de la cryptographie.*

Les problèmes de la théorie de l'information

- La représentation d'information — *concerne le **codage** : comment représenter les formes diverses d'information par les mots écrit avec les lettres d'un alphabet, soit $\{A, \dots, Z\}$ soit $\{0, 1\}$; et la **compression** : comment le faire en utilisant l'espace minimal.*
- L'intégrité d'information — *concerne la détection et la correction d'erreurs qui survient en raison du bruit dans le canal de transmission ; c'est traité dans la théorie des codes correcteurs d'erreurs.*
- La sécurité d'information — *concerne la confidentialité des données transmises et l'authentification des messages et des personnes ; ce sont les objectifs principaux de la cryptographie.*

Les problèmes de la théorie de l'information

- La représentation d'information — *concerne le **codage** : comment représenter les formes diverses d'information par les mots écrit avec les lettres d'un alphabet, soit $\{A, \dots, Z\}$ soit $\{0, 1\}$; et la **compression** : comment le faire en utilisant l'espace minimal.*
- L'intégrité d'information — *concerne la détection et la correction d'erreurs qui survient en raison du bruit dans le canal de transmission ; c'est traité dans la théorie des codes correcteurs d'erreurs.*
- La sécurité d'information — *concerne la confidentialité des données transmises et l'authentification des messages et des personnes ; ce sont les objectifs principaux de la cryptographie.*

Les buts de la cryptographie

Les objectifs principaux de sécurité de l'information peuvent être classifiés dans les objectifs suivants :

- Confidentialité
- Intégrité des données
- Authentification
- Non-répudiation
- Signature
- Contrôle d'accès
- Gestion des clés

Confidentialité

La confidentialité est la propriété qu'une information n'est ni disponible, ni divulguée aux personnes, entités ou processus non autorisés. Lors d'une communication, il s'agit d'empêcher un tiers de prendre connaissance de l'information contenue dans un message transmis sur un canal non sécurisé.

Intégrité des données

L'intégrité est la prévention d'une modification non autorisée de l'information. L'intégrité du système et de l'information garantit que ceux-ci ne sont modifiés que par une action volontaire et légitime. Les attaques contre l'intégrité sont appelées **substitutions**.

Authentification

L'authentification concerne la vérification de l'identité des différents participants impliqués dans une communication. Il peut s'agir d'authentifier des personnes (l'expéditeur et le destinataire), une machine (dans le cadre d'une relation client-serveur), ou un document (son auteur et le contenu). Les attaques contre l'authentification sont appelées **mascarades**.

Non-répudiation

La non-répudiation consiste en un mécanisme pour prouver, par exemple, que l'expéditeur d'un message est l'auteur ou que le destinataire a bien reçu le message.

Signature

Une signature est un mécanisme pour garantir l'authentification de l'expéditeur, l'intégrité des données et la non-répudiation.

Contrôle d'accès

Le contrôle d'accès est un mécanisme pour limiter l'accès d'une ressource aux seules personnes autorisées.

Gestion des clés

La gestion des clés concerne la génération, la distribution, le stockage, l'intégrité, le recouvrement et la révocation des clés utilisées dans les systèmes cryptographiques. La gestion des clés fait partie de ce qu'on s'appelle la PKI (Public Key Infrastructure) ou IGC (Infrastructure de Gestion de Clés).

RÉSUMÉ

1 Introduction

- Cryptographie, cryptanalyse, et cryptologie
- Transmission d'information
- Sécurité de l'information

2 Concepts cryptographiques

- Concepts et définitions
- Cryptosystèmes

Définitions

Un **alphabet** est un ensemble de lettres ou de symboles, et un **mot** est une séquence finie de ces éléments.

Exemples d'alphabets sont l'ensemble $\{A, \dots, Z\}$, l'alphabet binaire $\{0, 1\}$, ou les alphabets ASCII ou ISO-8859-1 (qui sont eux-mêmes des mots binaires).

Les mots valides d'une langue s'appellent les **messages** ou les **textes clairs**. Une **fonction de chiffrement** transforme les messages en des **textes chiffrés** ou **cryptogrammes**.

Un **protocole** est un algorithme, défini par une liste d'étapes, qui précise les actions des parties multiples pour accomplir une action.

Les espaces de messages, de textes chiffrés, etc.

Un cryptosystème repose sur

- Un ensemble \mathcal{M} de **messages** ou de **textes clairs** m .
- Un ensemble \mathcal{C} de **textes chiffrés** c .
- Un ensemble \mathcal{K} de **clés** K .

Les ensembles \mathcal{M} , \mathcal{C} et \mathcal{K} s'appellent l'**espace de messages**, **de textes chiffrés** et de **clés**.

Il est possible que $\mathcal{M} = \mathcal{C}$, mais on peut néanmoins distinguer les deux espaces par les probabilités de leurs mots.

Cryptosystèmes à clé secrète

Un **cryptosystème** consiste d'un ensemble de fonctions de chiffrement inversibles, tel que chacune correspond à une clé unique. Alors on définit un cryptosystème à clé secrète comme les ensembles de fonctions de chiffrement et déchiffrement :

$$\mathcal{E} = \{E_K : \mathcal{M} \longrightarrow \mathcal{C} \mid K \in \mathcal{K}\}.$$
$$\mathcal{D} = \{D_K : \mathcal{C} \longrightarrow \mathcal{M} \mid K \in \mathcal{K}\}.$$

tel que $D_K \circ E_K = \text{Id}$. Ou bien on peut définir \mathcal{E} et \mathcal{D} comme fonctions $\mathcal{E} : \mathcal{K} \times \mathcal{M} \longrightarrow \mathcal{C}$ et $\mathcal{D} : \mathcal{K} \times \mathcal{C} \longrightarrow \mathcal{M}$, telles que, pour tout K les fonctions E_K et D_K sont

$$E_K(m) = \mathcal{E}(K, m) \text{ et } D_K(m) = \mathcal{D}(K, m).$$

Cryptosystèmes à clé secrète (suite)

La conception moderne d'un cryptosystème est basée sur le **principe de Kerckhoff** : la sécurité d'un cryptosystème ne doit reposer que sur le secret de la clé (et ne dépend pas de la connaissance ou non du cryptosystème).

Alors, pour un cryptosystème à clé secrète, nous arrivons au protocole suivant :

Initialisation :

1. Alice et Bob choisissent un cryptosystème. (publique)

Pour chaque message de Alice → Bob :

1. Alice et Bob choisissent une clé secrète.

2. Alice chiffre son message avec la clé.

3. Alice envoie le texte chiffré à Bob. (publique)

4. Bob déchiffre le texte chiffré pour obtenir le message.

Cryptosystèmes à clé secrète (suite)

La conception moderne d'un cryptosystème est basée sur le **principe de Kerckhoff** : la sécurité d'un cryptosystème ne doit reposer que sur le secret de la clé (et ne dépend pas de la connaissance ou non du cryptosystème).

Alors, pour un cryptosystème à clé secrète, nous arrivons au protocole suivant :

Initialisation :

1. **Alice et Bob choisissent un cryptosystème.** (publique)

Pour chaque message de Alice → Bob :

1. Alice et Bob choisissent une clé secrète.

2. Alice chiffre son message avec la clé.

3. **Alice envoie le texte chiffré à Bob.** (publique)

4. Bob déchiffre le texte chiffré pour obtenir le message.

Cryptosystèmes à clé publique

Les cryptosystèmes à clé publique ont été introduit par Diffie et Hellman en 1976. La clé est remplacée par un couple (K, K') de clés — une **clé publique** servant au chiffrement et une **clé privée** au déchiffrement. Pour un cryptosystème à clé publique, nous avons

$$\mathcal{E} = \{E_K : \mathcal{M} \longrightarrow \mathcal{C} \mid K \in \mathcal{K}\}.$$

$$\mathcal{D} = \{D_{K'} : \mathcal{C} \longrightarrow \mathcal{M} \mid K' \in \mathcal{K}'\}.$$

tel que $D_{K'} \circ E_K = \text{Id}$. Chaque utilisateur dispose d'un couple de clés (K, K') . L'existence d'un tel cryptosystème est basée sur la possibilité de construire des fonctions $(E_K, D_{K'})$ tel que E_K est dure à inverser.

Cryptosystèmes à clé publique (suite)

Ainsi, pour un cryptosystème à clé publique, nous arrivons au protocole suivant :

Initialisation :

1. Alice et Bob choisissent un cryptosystème à clé publique.
2. Bob envoie Alice sa clé publique. (authentifié)

Pour chaque message de Alice \rightarrow Bob :

1. Alice chiffre son message avec la clé publique de Bob.
2. Alice envoie le texte chiffré à Bob. (publique)
3. Bob déchiffre le texte chiffré avec sa clé privée.

Les chiffrements à clé publique créent des problèmes de gestion des clés.

Les chiffrements à clé publique sont moins efficaces ; leur rôle le plus important est d'établir une clé secrète commune.