

LIQPIRATALE DEOT PCRYEIGHRAP

David Kohel

Institut de Mathématiques de Luminy

Pratique de la Cryptographie 2009

TAURQPIEDA LE YROCT PPAERIGH

David Kohel

Institut de Mathématiques de Luminy

Pratique de la Cryptographie 2009

IPTQAIR F.ELDA P YTROCHGPIAER

David Kohel

Institut de Mathématiques de Luminy

Pratique de la Cryptographie 2009

RUIAPTQ A DEELCOPR YTREHAGPI

David Kohel

Institut de Mathématiques de Luminy

Pratique de la Cryptographie 2009

QTRPUJIALE EA DTYC QPRIPRGEHA

David Kohel

Institut de Mathématiques de Luminy

Pratique de la Cryptographie 2009

AIQUTRPD LAE ERPTOYC AHIEPRG

David Kohel

Institut de Mathématiques de Luminy

Pratique de la Cryptographie 2009

PRATIQUE DE LA CRYPTOGRAPHIE

David Kohel

Institut de Mathématiques de Luminy

Pratique de la Cryptographie 2009

RÉSUMÉ

- 1 **Transmission d'information**
- 2 **Codage et compression**
- 3 **Codage et correction des erreurs**
- 4 **Cryptographie, cryptanalyse, et cryptologie**
 - Sécurité de l'information

RÉSUMÉ

- 1 Transmission d'information**
- 2 Codage et compression
- 3 Codage et correction des erreurs
- 4 Cryptographie, cryptanalyse, et cryptologie
 - Sécurité de l'information

Les problèmes de la transmission 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 de transmission.*
- **La sécurité d'information** — *concerne la confidentialité et l'authenticité de l'information transmise par les mots d'un alphabet, ou la cryptographie.*

Les problèmes de la transmission 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 transmission 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** de l'information transmises et l'**authentification** des messages et des personnes ; ce sont les objectifs principaux de la cryptographie.*

Les problèmes de la transmission 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 le **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** de l'information transmises et l'**authentification** des messages et des personnes ; ce sont les objectifs principaux de la cryptographie.*

Les problèmes de la transmission 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 le **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** de l'information transmises et l'**authentification** des messages et des personnes ; ce sont les objectifs principaux de la cryptographie.*

Les problèmes de la transmission 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 le **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 le **confidentialité** de l'information transmises et le **authentification** des messages et des personnes ; ce sont les objectifs principaux de la cryptographie.*

RÉSUMÉ

- 1 Transmission d'information
- 2 Codage et compression**
- 3 Codage et correction des erreurs
- 4 Cryptographie, cryptanalyse, et cryptologie
 - Sécurité de l'information

Qu'est-ce que c'est le compression de l'information ?

La compression de données traite de la réduction de l'espace nécessaire pour la représentation d'une certaine quantité d'information.

0000	0000	0101	0111	0000	⟶	0	0	10	11	0
0000	0101	0000	0000	0101	⟶	0	10	0	0	10
0101	0101	0000	0000	0000	⟶	10	10	0	0	0

Qu'est-ce que c'est le compression de l'information ?

La compression de données traite de la réduction de l'espace nécessaire pour la représentation d'une certaine quantité d'information.

0000	0000	0101	0111	0000	⟶	0	0	10	11	0
0000	0101	0000	0000	0101	⟶	0	10	0	0	10
0101	0101	0000	0000	0000	⟶	10	10	0	0	0

RÉSUMÉ

- 1 Transmission d'information
- 2 Codage et compression
- 3 Codage et correction des erreurs**
- 4 Cryptographie, cryptanalyse, et cryptologie
 - Sécurité de l'information

Qu'est-ce que c'est la correction d'erreurs ?

Le principe des codes correcteurs d'erreurs est de rajouter une information supplémentaire redondante de manière à détecter et corriger d'erreurs provoquées du bruit.



0010110	↦	00101101	↔	00101101	↦	0010110
0100010	↦	01000100	↔	01010100	↦	0101010*
1010000	↦	10100000	↔	10100000	↦	1010000

RÉSUMÉ

- 1 Transmission d'information
- 2 Codage et compression
- 3 Codage et correction des erreurs
- 4 **Cryptographie, cryptanalyse, et cryptologie**
 - Sécurité de l'information

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 buts de la cryptographie

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

- Confidentialité
- Intégrité des données
- Authentification
- Signatures