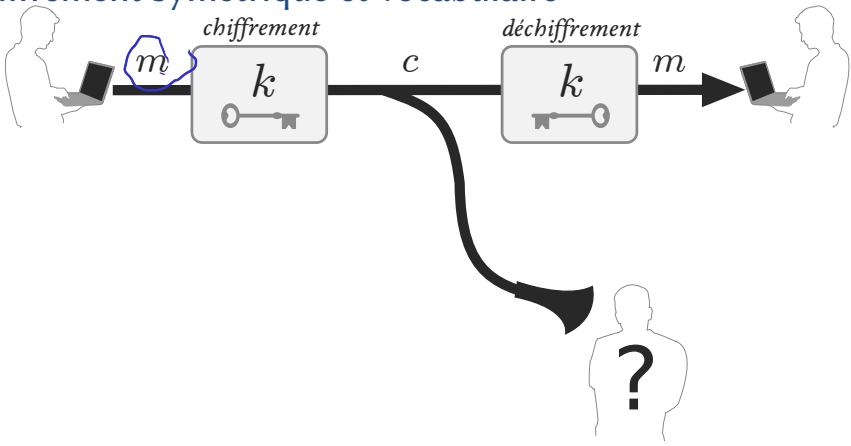
Cours 1. Introduction

HAI709I – Cryptographie

Bruno Grenet

Université de Montpellier – Faculté des Sciences

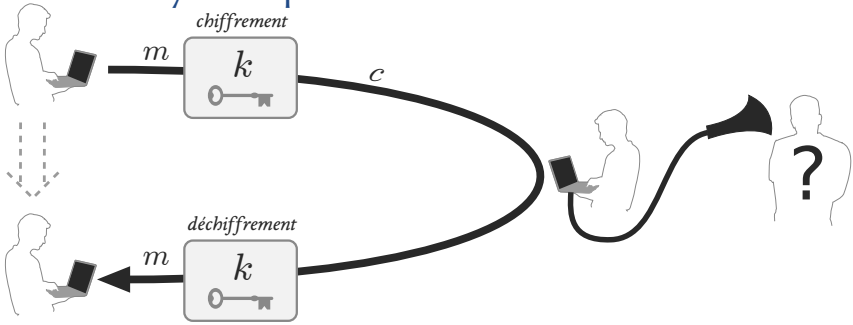
Chiffrement symétrique et vocabulaire



- m : message (clair)
- c : (message) chiffré
- k : clef

Source : J. Katz, Y. Lindell. Introduction to modern cryptography. 3rd ed, CRC Press, 2021. (modif.)

Chiffrement symétrique et vocabulaire



- m : message (clair)
- c : (message) chiffré
- k : clef

Source : J. Katz, Y. Lindell. Introduction to modern cryptography. 3rd ed, CRC Press, 2021. (modif.)

La syntaxe du chiffrement

Trois algorithmes

- Gen : génération de clef $\rightarrow$ Gen() (probabiliste)
- Enc : chiffrement $\rightarrow \mathrm{Enc}_k(m)$
- Dec : déchiffrement $\rightarrow \mathrm{Dec}_k(c)$

La syntaxe du chiffrement

Trois algorithmes

- Gen : génération de clef $\rightarrow$ Gen() (probabiliste)
- Enc : chiffrement $\rightarrow \mathrm{Enc}_k(m)$
- Dec : déchiffrement $\rightarrow \mathrm{Dec}_k(c)$

Pour tout m et k, $\mathrm{Dec}_k(\mathrm{Enc}_k(m)) = m$

La syntaxe du chiffrement

Trois algorithmes

- Gen : génération de clef $\rightarrow$ Gen() (probabiliste)
- Enc : chiffrement $\rightarrow \mathrm{Enc}_k(m)$
- Dec : déchiffrement $\rightarrow \mathrm{Dec}_k(c)$

Pour tout m et k, $\mathrm{Dec}_k(\mathrm{Enc}_k(m)) = m$

Utilisation

1. Génération de la clef : $k \leftarrow \mathrm{Gen}()$
2. Chiffrement du message : $c \leftarrow \mathrm{Enc}_k(m)$
3. Communication du message / passage du temps
4. Déchiffrement du message : $m \leftarrow \mathrm{Dec}_k(c)$

Chiffres historiques

- Chiffrements par décalage – César (env. 50 av. J.-C.), `rot13`
- Chiffrements par substitution (500-600 av. J.-C.)
- Chiffrements par transposition – scytale (404 av. J.-C.)
- Chiffre de Vigenère (1553)
- …

Chiffres historiques

- Chiffrements par décalage – César (env. 50 av. J.-C.), `rot13`
- Chiffrements par substitution (500-600 av. J.-C.)
- Chiffrements par transposition – scytale (404 av. J.-C.)
- Chiffre de Vigenère (1553)
- …

- Aucun n'est sûr : force brute, analyse fréquentielle (1863)
- Leçons apprises :
  - Il faut un *espace de clefs* suffisamment grand
  - Concevoir un système de chiffrement est *difficile*

Chiffres historiques

- Chiffrements par décalage – César (env. 50 av. J.-C.), `rot13`
- Chiffrements par substitution (500-600 av. J.-C.)
- Chiffrements par transposition – scytale (404 av. J.-C.)
- Chiffre de Vigenère (1553)
- …

- Aucun n'est sûr : force brute, analyse fréquentielle (1863)
- Leçons apprises :
  - Il faut un *espace de clefs* suffisamment grand
  - Concevoir un système de chiffrement est *difficile*

→ *cf* TD

Principe(s) de Kerckhoffs

JOURNAL

DES

SCIENCES MILITAIRES.

Janvier 1883.

LA CRYPTOGRAPHIE MILITAIRE.

« La cryptographie est un auxiliaire puissant de la tactique militaire. »
(Général Lewal, *Études de guerre.*)

I.

LA CRYPTOGRAPHIE DANS L'ARMÉE

A. Notions historiques.

La *Cryptographie* ou l'*Art de chiffrer* est une science vieille comme le monde ; confondue à son origine avec la télégraphie militaire, elle a été cultivée, dès la plus haute antiquité, par les Chinois, les Perses, les Carthaginois ; elle a été enseignée dans les écoles tactiques de la Grèce, et tenue en haute estime par les plus illustres généraux romains [1].

Depuis la modeste scytale des Lacédémoniens et les *trucs* inventés ou rapportés par Æneas-le-Tacticien [2], jusqu'au fameux

[1] C'est sous la rubrique : *Stéganographie, chiffre* ou *écritures secrètes*, que certains dictionnaires encyclopédiques donnent les renseignements qui se rapportent à la cryptographie. Les anciens auteurs l'appellent plus ou moins correctement : *ars notarum, ars zipherarum, polygraphia, steatographia, cryptologia, steganologia, cryptomenytices*, etc. ; les Allemands disent aujourd'hui : *Geheimschrift* ou *Chiffreschrift* et les Anglais : *cryptography*.

[2] Lettres mises entre les semelles du messager, communications cachées dans

II.

DESIDERATA DE LA CRYPTOGRAPHIE MILITAIRE.

Il faut bien distinguer entre un système d'écriture chiffrée, imaginé pour un échange momentané de lettres entre quelques personnes isolées, et une méthode de cryptographie destinée à régler pour un temps illimité la correspondance des différents chefs d'armée entre eux. Ceux-ci, en effet, ne peuvent, à leur gré et à un moment donné, modifier leurs conventions ; de plus, ils ne doivent jamais garder sur eux aucun objet ou écrit qui soit de nature à éclairer l'ennemi sur le sens des dépêches secrètes qui pourraient tomber entre ses mains.

Un grand nombre de combinaisons ingénieuses peuvent répondre au but qu'on veut atteindre dans le premier cas ; dans le second, il faut un système remplissant certaines conditions exceptionnelles, conditions que je résumerai sous les six chefs suivants :

1° Le système doit être matériellement, sinon mathématiquement, indéchiffrable ;

2° Il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi ;

3° La clef doit pouvoir en être communiquée et retenue sans le secours de notes écrites, et être changée ou modifiée au gré des correspondants ;

4° Il faut qu'il soit applicable à la correspondance télégraphique ;

5° Il faut qu'il soit portatif, et que son maniement ou son fonctionnement n'exige pas le concours de plusieurs personnes ;

6° Enfin, il est nécessaire, vu les circonstances qui en commandent l'application, que le système soit d'un usage facile, ne demandant ni tension d'esprit, ni la connaissance d'une longue série de règles à observer.

Tout le monde est d'accord pour admettre la raison d'être des

sonnes qui voudraient approfondir la question : ils leur seront d'autant plus utiles que, à deux ou trois exceptions près, les ouvrages cités se trouvent tous à la Bibliothèque nationale.

Principe(s) de Kerckhoffs

- Le chiffrement doit reposer sur des *clefs de chiffrement et déchiffrement*
- Le système de chiffrement ne doit pas être secret, seules les clefs doivent l'être

Principes de la cryptographie moderne

Définitions formelles

- Exemple : que veut dire *chiffrement sûr* ?
  - Un attaquant ne peut pas retrouver la clef
  - Un attaquant ne peut pas retrouver le message depuis le chiffré
  - Un attaquant ne peut retrouver aucun caractère du message depuis le chiffré

Principes de la cryptographie moderne

Définitions formelles

- Exemple : que veut dire *chiffrement sûr* ?
  - (bonne définition) Quelque soit l'information dont un attaquant dispose sur le message, le chiffré ne lui fournit aucune information *supplémentaire*

Principes de la cryptographie moderne

Définitions formelles

- Exemple : que veut dire *chiffrement sûr* ?
  - (bonne définition) Quelque soit l'information dont un attaquant dispose sur le message, le chiffré ne lui fournit aucune information *supplémentaire*
- Exemple : qu'est qu'un *attaquant* ?
  - Attaque à texte chiffré seulement
  - Attaque à texte clair connu
  - Attaque à texte clair choisi
  - Attaque à texte chiffré choisi

Principes de la cryptographie moderne

Définitions formelles

- Exemple : que veut dire *chiffrement sûr* ?
  - (bonne définition) Quelque soit l'information dont un attaquant dispose sur le message, le chiffré ne lui fournit aucune information *supplémentaire*
- Exemple : qu'est qu'un *attaquant* ?
  - Attaque à texte chiffré seulement
  - Attaque à texte clair connu
  - Attaque à texte clair choisi
  - Attaque à texte chiffré choisi

Hypothèses précises

- Capacité de calcul d'un attaquant (théorie de la complexité)
- Validité des hypothèses, comparaison entre hypothèses et hypothèses *nécessaires*

Principes de la cryptographie moderne

Définitions formelles

- Exemple : que veut dire *chiffrement sûr* ?
  - (bonne définition) Quelque soit l'information dont un attaquant dispose sur le message, le chiffré ne lui fournit aucune information *supplémentaire*
- Exemple : qu'est qu'un *attaquant* ?
  - Attaque à texte chiffré seulement
  - Attaque à texte clair connu
  - Attaque à texte clair choisi
  - Attaque à texte chiffré choisi

Hypothèses précises

- Capacité de calcul d'un attaquant (théorie de la complexité)
- Validité des hypothèses, comparaison entre hypothèses et hypothèses *nécessaires*

Preuves de sécurité

Prouver qu'une construction satisfait une *définition de sécurité*, supposant des *hypothèses*

1. Principes généraux

2. Chiffrement inconditionnellement sûr

Définitions

Schéma de chiffrement

- Trois algorithmes Gen, Enc, Dec
- Un *espace de message* $\mathcal{M}$
- Un *espace de clefs* $\mathcal{K}$ (fini)

Propriétés

- Gen tire aléatoirement $k \in \mathcal{K}$
- Enc : $\mathcal{K} \times \mathcal{M} \to \mathcal{C}$ où $\mathcal{C}$ est l'*espace des chiffrés*
- Dec : $\mathcal{K} \times \mathcal{C} \to \mathcal{M}$

Définitions

Schéma de chiffrement

- Trois algorithmes Gen, Enc, Dec
- Un *espace de message* $\mathcal{M}$
- Un *espace de clefs* $\mathcal{K}$ (fini)

Propriétés

- Gen tire aléatoirement $k \in \mathcal{K}$
- Enc : $\mathcal{K} \times \mathcal{M} \to \mathcal{C}$ où $\mathcal{C}$ est l'*espace des chiffrés*
- Dec : $\mathcal{K} \times \mathcal{C} \to \mathcal{M}$

Algorithmes probabilistes et déterministes

- Gen est forcément probabiliste
- Enc peut être probabiliste
- Dec est déterministe

Pour tout $k \in \mathcal{K}$, $m \in \mathcal{M}$, et $c \leftarrow \mathrm{Enc}_k(m) \in \mathcal{C}$, $\mathrm{Dec}_k(c) = m$.

Probabilités partout !

- Gen et éventuellement Enc probabilistes $\rightarrow$ k et c aléatoires
- Messages pas tous *équiprobables* $\rightarrow$ distribution de probabilité sur m

Probabilités partout !

- Gen et éventuellement Enc probabilistes $\rightarrow$ k et c aléatoires
- Messages pas tous *équiprobables* $\rightarrow$ distribution de probabilité sur m

Variables aléatoires

- K : variable aléatoire décrivant la clef k produite par Gen
- M : variable aléatoire décrivant le message
- C : variable aléatoire décrivant le chiffré

Probabilités partout !

- Gen et éventuellement Enc probabilistes $\rightarrow$ k et c aléatoires
- Messages pas tous *équiprobables* $\rightarrow$ distribution de probabilité sur m

Variables aléatoires

- K : variable aléatoire décrivant la clef k produite par Gen
- M : variable aléatoire décrivant le message
- C : variable aléatoire décrivant le chiffré

Exemples

- $\Pr[K = k]$ est la probabilité que Gen renvoie la clef k
- Distribution de M : information dont l'attaquant dispose sur le message
  - Distribution uniforme : aucune information
- $\Pr[C = c | M = m \wedge K = k]$ est la probabilité que $\mathrm{Enc}_k(m)$ renvoie c

Probabilités partout !

- Gen et éventuellement Enc probabilistes $\rightarrow$ k et c aléatoires
- Messages pas tous *équiprobables* $\rightarrow$ distribution de probabilité sur m

Variables aléatoires

- K : variable aléatoire décrivant la clef k produite par Gen
- M : variable aléatoire décrivant le message
- C : variable aléatoire décrivant le chiffré

Exemples

- $\Pr[K = k]$ est la probabilité que Gen renvoie la clef k
- Distribution de M : information dont l'attaquant dispose sur le message
  - Distribution uniforme : aucune information
- $\Pr[C = c | M = m \wedge K = k]$ est la probabilité que $\mathrm{Enc}_k(m)$ renvoie c

Les variables M et K sont *indépendantes* !

$\Pr[M = m \wedge K = k] = \Pr[M = m] \Pr[K = k]$

Que veut dire *inconditionnellement sûr* ?

Quelque soit l'information dont un attaquant dispose sur le message, connaître le chiffré ne lui fournit aucune information supplémentaire

Que veut dire *inconditionnellement sûr* ?

Quelque soit l'information dont un attaquant dispose sur le message, connaître le chiffré ne lui fournit aucune information supplémentaire

- *quelque soit l'information* : quelque soit la distribution de M
- *connaître le chiffré* : si on sait que $C = c$
- *aucune information supplémentaire* : la probabilité que $M = m$ ne change pas

Que veut dire *inconditionnellement sûr* ?

Quelque soit l'information dont un attaquant dispose sur le message, connaître le chiffré ne lui fournit aucune information supplémentaire

- *quelque soit l'information* : quelque soit la distribution de M
- *connaître le chiffré* : si on sait que $C = c$
- *aucune information supplémentaire* : la probabilité que $M = m$ ne change pas

Définition

Un schéma de chiffrement (Gen, Enc, Dec) est **inconditionnellement sûr** si pour toute distribution de probabilité pour M, pour tout $m \in \mathcal{M}$ et $c \in \mathcal{C}$ tq $\Pr[C = c] > 0$,

$$\Pr[M = m | C = c] = \Pr[M = m].$$

Le chiffre de Vernam ou *one-time pad*

Définition

- $\mathcal{K} = \mathcal{M} = \mathcal{C} = \{0,1\}^\ell$
- Gen : tirage aléatoire uniforme d'un mot binaire de longueur ℓ
- $\mathrm{Enc}_k(m)$ et $\mathrm{Dec}_k(c)$?

L. $c \leftarrow m+k$ → longueur $\ell+1$

$c \leftarrow m \| k$ → — 2ℓ

0 1 0 1 1 0

- Si $k_{[i]} = 1$ $c_{[i]} \leftarrow 1 - m_{[i]}$
  Sinon $c_{[i]} \leftarrow m_{[i]}$

) XOR

Le chiffre de Vernam ou *one-time pad*

Définition

- $\mathcal{K} = \mathcal{M} = \mathcal{C} = \{0,1\}^\ell$
- Gen : tirage aléatoire uniforme d'un mot binaire de longueur ℓ
- $\mathrm{Enc}_k(m)$ et $\mathrm{Dec}_k(c)$?

$$\mathrm{Enc}_k(m) = m \oplus k \text{ et } \mathrm{Dec}_k(c) = c \oplus k$$

$(m \oplus k) \oplus k = m \oplus (k \oplus k) = m$
0^ℓ

Le chiffre de Vernam ou *one-time pad*

Définition

- $\mathcal{K} = \mathcal{M} = \mathcal{C} = \{0,1\}^\ell$
- Gen : tirage aléatoire uniforme d'un mot binaire de longueur ℓ
- $\mathrm{Enc}_k(m)$ et $\mathrm{Dec}_k(c)$?

$$\mathrm{Enc}_k(m) = m \oplus k \text{ et } \mathrm{Dec}_k(c) = c \oplus k$$

- Utilisé pendant la guerre froide
- Inconditionnellement sûr

- Clef aussi longue que le message
- Utilisable une seule fois

Preuve de sécurité du chiffre de Vernam

Théorème

Le chiffre de Vernam est inconditionnellement sûr.

Idée de la preuve

Puisque K est aléatoire uniforme, $M \oplus K$ l'est aussi quelque soit (la distribution de) M

Preuve

On veut $\forall \Pr[\Pi = m \mid C = c] = \Pr[\Pi = m]$

$$\Pr[\Pi = m \wedge C = c] = \Pr[\Pi = m \wedge K = m \oplus c]$$
$$= \Pr[\Pi = m] \Pr[K = m \oplus c] = \tfrac{1}{2^\ell} \Pr[\Pi = m]$$

$$\Pr[C = c] = \sum_{m \in \Pi} \Pr[\Pi = m \wedge K = m \oplus c] = \sum_{m \in \Pi} \Pr[\Pi = m] \Pr[K = m \oplus c]$$
$$= \tfrac{1}{2^\ell} \sum_{m \in \Pi} \Pr[\Pi = m] = \tfrac{1}{2^\ell}.$$

✓

Limitations de la sécurité inconditionelle

Théorème

Si (Gen, Enc, Dec) *est inconditionnellement sûr, alors* $|\mathcal{K}| \geq |\mathcal{M}|$.

Preuve par l'absurde. On suppose $|K| < |M|$

- On veut montrer $\exists$ distribution uniforme, un message m et un chiffré c tq $\Pr[M = m \mid C = c] \neq \Pr[M = m]$

$$M(c) = \{ m \in M : \exists k \in K \quad Dec_k(c) = m \}$$

$|M(c)| \leq |K|$ car Dec est déterministe

$\hookrightarrow |M(c)| < |M|$.

On prend $m \in M \setminus M(c)$. Alors $\Pr[M = m \mid C = c] = 0 \neq \Pr[M = m] = 1/|M|$

Conclusion

Difficultés

- Chiffrement de Vernam : inconditionnellement sûr mais…
- … sécurité inconditionnelle impossible avec des *petites* clefs

Conclusion

Difficultés

- Chiffrement de Vernam : inconditionnellement sûr mais…
- … sécurité inconditionnelle impossible avec des *petites* clefs

Relaxation de la notion de sécurité :

- Obtenir de l'information sur le message devient *possible*…
- … mais *trop coûteux* en temps de calcul (sécurité *calculatoire*)

Conclusion

Difficultés

- Chiffrement de Vernam : inconditionnellement sûr mais…
- … sécurité inconditionnelle impossible avec des *petites* clefs

Relaxation de la notion de sécurité :

- Obtenir de l'information sur le message devient *possible*…
- … mais *trop coûteux* en temps de calcul (sécurité *calculatoire*)

Suite du cours

- Chiffrement symétrique : imiter Vernam
- Cryptographie symétrique :
  - au delà du chiffrement (authentification, hachage)
  - primitives utilisées en pratique (3-DES, AES, SHA)
- La *révolution* asymétrique :
  - échange de clefs (Diffie-Hellman)
  - chiffrement asymétrique (dont RSA, ElGamal)
  - au delà du chiffrement (signatures, …)