Cryptographie
Introduction : courte histoire du chiffrement

Sorina Ionica

February 9, 2025

Organisation du cours

Contenu:

- 2 séances de cours, 3 TD/2 TP
- Tout matériel sur le moodle de l'université

Modalités de contrôle:

- Contrôle continu
- une note : Contrôle écrit (début mars) + rendu des TP

Un peu de vocabulaire sur la cryptologie

- *Cryptographie*: communiquer de façon confidentielle sur un canal susceptible à l'espionnage
  - *Cryptosystéme, schéma de chiffrement* (en non-pas un *code*...)
- *Cryptanalyse*: retrouver l'information sans être l'auteur ou le destinataire légitime
  - *Attaque, cassage* (total ou partiel)

Cryptographie et échange d'information

- **Confidentialité** : l'information est accésible qu'à ceux dont l'accés est autorisé.
- **Authentification**: vérifier l'identité de la personne/machine lors de la communication
- **L'integrité**: les données ne subissent pas d'altération.

Encore de la terminologie

- les attaques passives : consistent à écouter sans modifier les données ou le fonctionnement du réseau.
- les attaques actives : consistent à modifier des données ou des messages, à s'introduire dans des équipements réseau ou à perturber le bon fonctionnement de ce réseau.

La cryptographie n'est qu'un des volets de la sécurité des systèmes informatiques.

La confidentialité

Chiffrement de Caesar

Décalage de 3

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

V	I	V	E	L	E	P	R	I	N	T	E	M	P	S!
Y	L	Y	H	O	H	S	U	L	Q	W	H	P	S	V!

Supposons que l'attaquant recupère une paire message/chiffré.
Combien d'éssais doit-il faire afin de trouver la clé?

Chiffrement par substitution monoalphabétique

- Utiliser une permutation des lettres de l'alphabet

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
k	r	u	s	f	l	t	a	g	z	m	q	n	b	v	e	o	p	h	x	j	y	w	c	i	d

Combien de clés possibles il y-a-t-il?

Chiffrement par substitution monoalphabétique

- Utiliser une permutation des lettres de l'alphabet

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
k	r	u	s	f	l	t	a	g	z	m	q	n	b	v	e	o	p	h	x	j	y	w	c	i	d

Combien de clés possibles il y-a-t-il? $26! \simeq 10^{26} = 100$ quadrillion

Les cryptanalystes arabes ont decouvert la cryptanalyse fréquentielle vers 800 A.D.

Fréquence des lettres dans la langue française

Lettre	Fréquence	Lettre	Fréquence
A	8.40%	N	7.13%
B	1.06%	O	5.26%
C	3.03%	P	3.01%
D	4.18%	Q	0.99%
E	17.26%	R	6.55%
F	1.12%	S	8.08%
H	0.92%	U	5.74%
I	7.34%	V	1.32%
J	0.31%	W	0.04%
K	0.05%	X	0.45%
L	6.01%	Y	0.30%
M	2.96%	Z	0.12%

Chiffrement de Vigènere

- Proposé par Blaise de Vigènere pour la court de Henri III en 1586.
- **Substitution polyalphabétique** : une même lettre du message clair peut, suivant sa position, être remplacée par des lettres différentes.

V	I	V	E	L	E	P	R	I	N	T	E	M	P	S	E	T	L	E	B	E	A	U	T	E	M	P	S
F	L	E	U	R	F	L	E	U	R	F	L	E	U	R	F	L	E	U	R	F	L	E	U	R	F	L	E

Chiffrement de Vigènere

- Résistant à l'analyse frequentielle.
- Il constitue une manière sans faille de chiffrement pendant 300 ans.
  - Kasisky publie une attaque au XIX-ème siécle.

Lois de Kerchkoffs

Journal des Sciences Militaires 1883

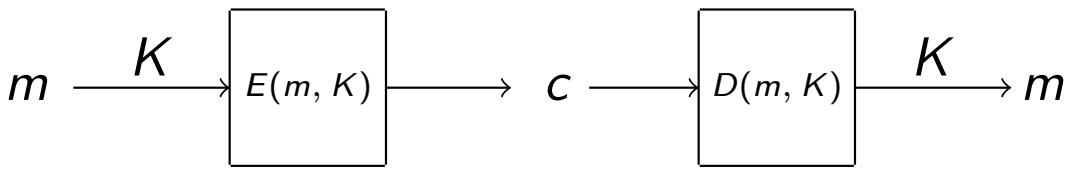
La sécurité ne repose pas sur le secret de la méthode, mais sur le secret de la clef utilisée.

Comment inverser un système quand on ne connaît pas son fonctionnement?

La rétro-ingénierie!

Confidentialité: cryptographie à clé secrète

- A et B choissisent une clef $K \in \mathcal{K}$.
- A chiffre son message $m \in \mathcal{M}$ à l'aide de K et envoie le chiffré $c \in \mathcal{C}$
- A envoie le chiffrement c à B.
- B déchiffre c à l'aide de K.



Les attaques

- chiffré seul: on connaît un chiffré.
  - Example : cryptanalyse fréquentielle
- clair connu: on connaît un ou plusieurs couples clair-chiffré.
- clair choisi: on a accès à la fonction de chiffrement.
  $m \rightarrow E(m, K)$ pour une ou plusieurs clefs k inconnues.
- chiffré choisi: on a accès à la fonction de déchiffrement.

Principes de Shannon 1948

- Confusion : Il n'y a pas de relation simple entre le clair et le chiffré. Connaître un certain nombre de couples clair-chiffré ne permet pas d'en déduire la fonction de chiffrement pour les autres messages.
- Diffusion : La modification d'une lettre du clair doit modifier l'ensemble du chiffré.

Travaux de Shannon

Un attaquant peut tomber par hasard sur la bonne clé: la sécurité est donc probabiliste!

- $Pr(M = m)$ la probabilité que le message envoyé soit m.
- $Pr(M = m|C = c)$ la probabilité que le message émi soit m alors qu'on a intercepté c.

Un attaquant peut tomber par hasard sur la bonne clé: la sécurité est donc probabiliste!

- $Pr(M = m)$ la probabilité que le message envoyé soit m.
- $Pr(M = m|C = c)$ la probabilité que le message émi soit m alors qu'on a intercepté c.

Chiffrement parfait

Un système de chiffrement est dit parfait si le chiffré c ne donne aucune information sur le message clair à partir duquel il est obtenu:

$$Pr(M = m|C = c) = Pr(M = m).$$

Théorème du secret parfait

Supposons que $\mathcal{M}$, $\mathcal{K}$ et $\mathcal{C}$ ont le même nombre d'élements.
Alors le chiffrement est parfait si et seulement si:

- Les clés sont distribués suivant une loi uniforme.
- Pour tout message clair $m \in \mathcal{M}$, on a une bijection :

$$\begin{aligned} \phi : \mathcal{K} &\to \mathcal{C} \\ K &\to E(m, K) \end{aligned}$$

est une bijection.

Preuve

2. Supposons qu'il existe m tel que $K \to E(m, K)$ n'est pas surjective. Alors il existe $c \in \mathcal{C}$ tel que $\forall K \in \mathcal{K}$:

$$E(m, K) \neq c$$

Alors $Pr(C = c|M = m) = 0$ donc par la formule de Bayes:

$$Pr(M = m|C = c) = \frac{Pr(C = c|M = m)Pr(M = m)}{Pr(C = c)} = 0.$$

Contradiction avec $Pr(M = m|C = c) = Pr(m) > 0$.

Un chiffrement parfait: One-Time Pad

Idée: Chiffrer le texte par addition d'une clef aussi longue que le texte et aléatoire

message clair	C	R	Y	P	T	O	G	R	A	P	H	E
clé	A	J	T	P	V	N	Q	P	G	B	Q	F
chiffré	D	A	S	F	P	C	X	H	H	R	Y	K

ou plus formellement:

Un chiffrement parfait: One-Time Pad

Idée: Chiffrer le texte par addition d'une clef aussi longue que le texte et aléatoire

message clair	C	R	Y	P	T	O	G	R	A	P	H	E
clé	A	J	T	P	V	N	Q	P	G	B	Q	F
chiffré	D	A	S	F	P	C	X	H	H	R	Y	K

ou plus formellement:

OTP

L'espace de clé $\mathcal{K}$, de message $\mathcal{M}$ et de chiffrés $\mathcal{C}$ sont $\{0,1\}^l$.
Pour chiffrer, on prend $E(m, K) = m \oplus K$.

One-Time Pad est parfait

Théorème

Le One-Time Pad est un chiffrement parfait.

Preuve.

1. La clé est choisie uniformement dans $\mathcal{K} = \{0,1\}^l$. Combien vaut $P(k)$?

One-Time Pad est parfait

Théorème

Le One-Time Pad est un chiffrement parfait.

Preuve.

1. La clé est choisie uniformement dans $\mathcal{K} = \{0,1\}^l$. Combien vaut $P(k)$?

$$P(k) = \frac{1}{2^l}.$$

One-Time Pad est parfait

2. Nous avons que $P(C = c|M = m) = Pr(M \oplus K = c|M = m) = Pr(m \oplus K = c) = Pr(K = m \oplus c) = \frac{1}{2^l}$.
D'autre part:

$$\begin{aligned} Pr(c) &= \sum_{m \in \mathcal{M}} Pr(C = c|M = m) Pr(M = m) \\ &= \frac{1}{2^l} \sum_{m \in \mathcal{M}} Pr(M = m) = \frac{1}{2^l}. \end{aligned}$$

Alors par la formule de Bayes:

$$Pr(M = m|C = c) = \frac{Pr(C = c|M = m) Pr(M = m)}{Pr(C = c)} = Pr(M = m).$$

Dans la pratique

- Comment fait-on pour générer les clés aléatoirement?
- Comment fait-on pour échanger ces clés?

En cryptographie moderne, on renonce à la sécurité de Shannon au profit d'une approche qui fonctionne dans la pratique.

Ordre de grandeur

- Nombre de gouttes d'eau dans les océans

$$4.2 \cdot 10^{25}$$

- Nombre de graines de sable sur Terre

$$2 \cdot 10^{26}$$

- Une clé aléatoire de 128 bits. Quelle est la taille de l'espace des clés $\mathcal{K}$?

Approche pratique

On souhaite avoir la plus grande sécurité possible en prenant une clé aussi grande que possible.

Attaque par force brute

Pour tout $k \in \mathcal{K}$

vérifier si $E(m, k) == c$

Le standard actuel AES fonctionne avec des clés de 128, 192, 256 bits.

La confidentialité aujourd'hui

- La clé de chiffrement est égale à la clé de déchiffrement
  - chiffrement symétrique : le standard est AES
- Les clés de chiffrement et déchiffrement sont différentes.
  - chiffrement asymétrique : Bob n'a pas besoin de connaître la clé de chiffrement pour déchiffrer.
  - Example : RSA