Introduction à la cryptographie

Théorie et pratique

Nathanaël Cottin

contact@ncottin.net

http://www.ncottin.net

version 0.0.2

Plan général

- Partie 1 : Introduction générale
- Partie 2 : Les systèmes cryptographiques
- Partie 3 : Chiffrement et déchiffrement de messages
- Partie 4 : La cryptanalyse
- Partie 5 : La cryptographie à clé secrète
- Partie 6 : La cryptographie à clé publique
- Partie 7 : La stéganographie
- Partie 8 : Conclusion

Partie 1 : Introduction générale

Partie 2 : Les systèmes cryptographiques

3 Modèle formel

4 Systèmes cryptographiques équivalents

5 Sécurité des systèmes cryptographiques

Partie 3 : Chiffrement et déchiffrement de messages

6 Classification des méthodes de chiffrement

7 Opérations de chiffrement et déchiffrement

Partie 4 : La cryptanalyse

8 Histoire

9 Classification des attaques

10 Présentation de quelques techniques de cryptanalyse

11 Mesure de complexité

Partie 5 : La cryptographie à clé secrète

Partie 6 : La cryptographie à clé publique

Partie 7 : La stéganographie

Partie 8 : Conclusion

Partie I

Introduction générale

Histoire de la cryptographie, concepts fondamentaux

Terminologie

Cryptographie

Science de la dissimulation de messages

Cryptanalyse

Science de la découverte (ou reconstitution) des informations cachées par un processus cryptographique

Terminologie

Cryptanalyste

Se dit d'une personne qui pratique la cryptanalyse

Cryptologie

Regroupe cryptographie et cryptanalyse

Partie II

Les systèmes cryptographiques

Définition formelle

Modélisation des systèmes cryptographiques

$$S = \{P, C, K_E, K_D, E, D\}$$

- $E : P \times K_E \mapsto C$ règle de chiffrement
- $D : C \times K_D \mapsto P$ règle de déchiffrement

Relation d'involution

$D(E(x, k), k') = x, k \in K_E, k' \in K_D, x \in P$

Systèmes équivalents

$$S_x = \left\{ P_x, C_x, K_{E,x}, K_{D,x}, E_x, D_x \right\}$$

$$S_1 \equiv S_2 \Leftrightarrow \begin{cases} P_i = P_j \\ C_i = C_j \\ \forall k_i \in K_{E,i}, \forall m \in P, \exists k_j \in K_{E,j}, E_i\left(m, k_i\right) = E_j\left(m, k_j\right) \end{cases}$$

Classification des systèmes

- *Cassage complet*
- *Obtention globale*
- *Obtention locale*
- *Obtention d'informations*

Sécurité d'un système cryptographique et entropie

$$H(X) = -\sum_{i=1}^{i=N} p_i \times \log_2(p_i)$$

avec :

- X variable discrète à N états disjoints, uniformément distribuée
- $p_i = \frac{n_i}{N}$ probabilité associée à l'évènement $i \in [1; N]$

Partie III

Chiffrement et déchiffrement de messages

Notions théoriques, techniques de mise en oeuvre

Chiffrement par substitution

Définition

Un *chiffre à substitution* est un chiffre dans lequel chaque caractère *remplace* le caractère d'origine. Le déchiffrement consiste à effectuer la substitution inverse

Méthodes de chiffrement

- Le *chiffrement à substitution simple* ou *mono-alphabétique*
- Le *chiffrement à substitution homophonique*
- Le *chiffrement à substitution simple par polygrammes*
- Le *chiffrement à substitution polyalphabétique*

Chiffrement par transposition

Définition

La technique de *chiffrement par transposition* consiste à *échanger* les caractères du texte en clair

Transposition simple en colonnes

Texte en clair

```
LE COLONNEL MOUTARDE AVEC UN COUTEAU
```

Texte chiffré sur 4 lignes

```
LLEUDECE
EOLTECOA
CNMAAUUU
ONORVNT.
```

Partie IV

La cryptanalyse

L'art de décrypter les messages

Classification des attaques

- *A texte chiffré*
- *A texte clair connu*
- *A texte clair choisi*
- *A texte clair choisi adaptative*

Recherche exhaustive

Définition

Essayer l'ensemble des clés possibles jusqu'à obtenir un texte en clair cohérent

Analyse fréquentielle

Définition

Analyse de la fréquence d'apparition des lettres dans les mots d'une langue donnée

Partie V

La cryptographie à clé secrète

Une clé unique partagée

Définition

Une même clé est utilisée pour à la fois chiffrer et déchiffrer les messages ($k = k'$)

Chiffre de César

Caractère en clair	Chiffre correspondant
A	D
B	E
C	F
...	...
W	Z
X	A
Y	B
Z	C

Tableau: Table de correspondances du chiffrement de César

Exemple de chiffrement

Texte en clair	M	E	S	S	A	G	E
Texte chiffré	P	H	V	V	D	J	H

Tableau: Exemple de chiffrement de César

Equivalences

$$S_{x,m} \equiv S_{y,m} \Leftrightarrow x \bmod m = y \bmod m$$

Ainsi $S_{1,26}$, $S_{-27,26}$ et $S_{53,26}$ sont deux systèmes équivalents.

Exemple de chiffrement

Texte en clair	M	E	S	S	A	G	E
Clé	C	L	E	C	L	E	C
Texte chiffré	P	Q	X	V	M	L	H

Tableau: Exemple de chiffrement de Vigenère

Partie VI

La cryptographie à clé publique

Bi-clé

Définition

Une clé de chiffrement et de la clé de déchiffrement qui lui correspond

Fonction employée

$$\begin{cases} f : P \times K \mapsto R \\ f(x,k) = x \times k, \forall x \in \mathrm{N}, \forall k \in R^* \end{cases}$$

Cryptosystème

$$S_k = \{P, C, \mathrm{N}, Q, \{f\}, \{f\}\}$$

Fondements de RSA

$$m^{\Phi} = 1 \bmod n, \Phi = (p-1) \times (q-1)$$

$$m^{\Phi+1} = m \bmod n$$

Expression générale

$$(m^e \bmod n)^d \bmod n = m \bmod n, e \times d = \Phi + 1$$

Théorème d'Euler

Théorème d'Euler

Soient p et q deux nombres premiers distincts et n le produit de ces nombres. Si e désigne un entier premier avec Φ, produit de $p-1$ par $q-1$, alors :

$$e \times d = 1 \bmod \Phi, \Phi = (p-1) \times (q-1)$$

Il suit : $m^{e \times d} = m \bmod n$

Composition du bi-clé

- Pour le déchiffrement : $\{e, p, q\}$
- Pour le chiffrement : $\{e, n\}$

Chiffrement d'un texte en clair

$$\mathrm{C} = \mathrm{M}'^{e} \bmod n$$

Déchiffrement du texte chiffré

$$\mathrm{M}' = \mathrm{C}^d \bmod n$$

Partie VII

La stéganographie

Partie VIII

Conclusion

Quel système cryptographique choisir ?

Existe-t-il un système cryptographique parfait ?

Quel avenir pour la cryptographie ?