

Cours sécurité informatique: Introduction à la cryptographie

Dr.Boujnah Noureddine

Faculté des Sciences de Gabès

2 novembre 2014

Plan

1 Introduction générale

Plan

- 1 Introduction générale
- 2 Mathématiques pour la cryptographie

Plan

- 1 Introduction générale
- 2 Mathématiques pour la cryptographie
- 3 Concepts cryptographiques

Plan

- 1 Introduction générale
- 2 Mathématiques pour la cryptographie
- 3 Concepts cryptographiques
- 4 La cryptographie classique

Notions de base

Définitions

- Cryptosystèmes : Mécanismes assurant les services requis
- Cryptographie : Art de concevoir des cryptosystèmes
- Cryptanalyses : Art de casser des cryptosystèmes
- Cryptologie : Science qui étudie les deux arts précédents.
- Chiffrement : Le chiffrement consiste à transformer une donnée (texte, message, ...) afin de la rendre incompréhensible par une personne autre que celui qui a créé le message et celui qui en est le destinataire.
- Déchiffrement : La fonction permettant de retrouver le texte clair à partir du texte chiffré.
- Steganographie : cacher le message pour que l'ennemi ne le trouve pas.

La figure 1 illustre le modèle du cryptosystème.

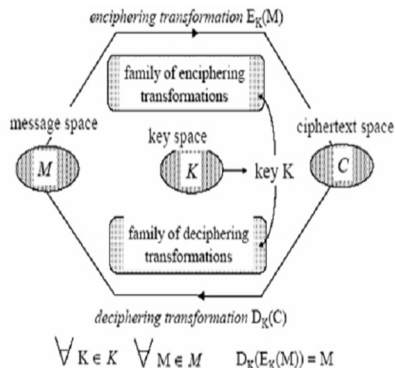


Figure : Modèle du cryptosystème

Historique

Jules César(Rome, 100-44 avant J.-C.)

Employait une substitution simple avec l'alphabet normal (il s'agissait simplement de décaler les lettres de l'alphabet d'une quantité fixe) dans les communications du gouvernement

Al-Kindi(arabe, 9^e siècle)

Rédige le plus ancien texte connu décrivant la technique de décryptage appelée des fréquences.

Blaise de Vigenère(France, 1585)

écrit son traité des chiffres ou secrètes manières d'écrire. Il présente entre autres un tableau du type Trithème, que l'on dénomme aujourd'hui carré de Vigenère.

Gilbert S. Vernam(France, 1917)

travaillant pour AT&T, a inventé une machine de chiffre polyalphabétique pratique capable d'employer une clef qui est totalement aléatoire et ne se répète jamais - un masque jetable. C'est seul le chiffre, dans nos connaissances actuelles, dont on a prouvé qu'il était indéchiffrable en pratique et en théorie.

Arthur Scherbius(Allemagne)

Fait breveter sa machine à chiffrer **Enigma**. Le prix d'un exemplaire s'élevait à 20'000 livres en valeur actuelle. Ce prix sembla décourager les acheteurs potentiels.

Lester S. Hill(1929)

Publie son article "Cryptography in an Algebraic Alphabet", dans American Mathematical Monthly, 36, 1929, pp. 306-312. C'est un chiffre polygraphique où l'on utilise des matrices et des vecteurs.

Whitfield Diffie et Martin Hellman(1976)

publient 'New Directions in Cryptography', introduisant l'idée de cryptographie à clef publique. Ils donnent une solution entièrement nouvelle au problème de l'échange de clefs.

Ron Rivest, Adi Shamir et Leonard Adleman(1977)

L'algorithme RSA basé sur la difficulté de factoriser un nombre n en deux nombres premiers p et q . Il utilise les notions de théorie des nombres. Il existe encore à nos jours. Le cryptage elliptique est un concurrent du RSA.

La machine allemande **Enigma** a joué un grand rôle pendant la guerre de l'Atlantique, et son décryptage par les alliés leur a assuré bon nombre de victoires (notamment parce que les Allemands ne se doutaient pas que leurs messages étaient déchiffrés).

Enigma ressemble à une machine à écrire : on frappe le clair sur un clavier, et des petites lampes s'allument pour éclairer les lettres résultant du chiffrement.

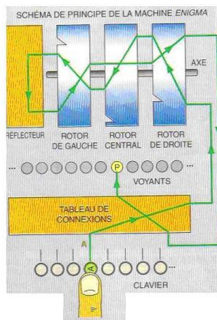


Figure : Machine **Enigma**

Les menaces

- **Les menaces accidentelles** : Les menaces accidentelles ne supposent aucune préméditation. Dans cette catégorie, sont repris les bugs logiciels, les pannes matérielles, et autres défaillances "incontrôlables".
- **Les menaces intentionnelles** : reposent sur l'action d'un tiers désirant s'introduire et relever des informations. Dans le cas d'une attaque passive, l'intrus va tenter de dérober les informations par audit, ce qui rend sa détection relativement difficile. En eet, cet audit ne modifie pas les fichiers, ni n'altère les systèmes. Dans le cas d'une attaque active, la détection est facilitée, mais il peut être déjà trop tard lorsque celle-ci a lieu. Ici, l'intrus aura volontairement modifié les fichiers ou le système en place pour s'en emparer.

Les menaces

Les menaces actives appartiennent principalement à quatre catégories :

- **Interruption** : problème lié à la disponibilité des données
- **Interception** : problème lié à la confidentialité des données
- **Modification** : problème lié à l'intégrité des données
- **Fabrication** : problème lié à l'authenticité des données

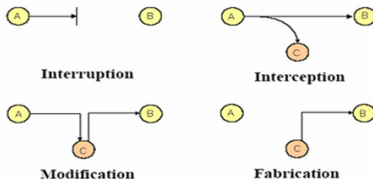


Figure : Menaces actives

objectifs de la sécurité

- **Confidentialité** : l'information n'est connue que des entités communicantes
- **Intégrité** : l'information n'a pas été modifiée entre sa création et son traitement (en ce compris un éventuel transfert)
- **Disponibilité** : l'information est toujours accessible et ne peut être bloquée/perdue

Arithmétiques : Définitions

- L'ensemble des entiers naturels est noté \mathbb{N}
- L'ensemble des entiers relatifs est noté \mathbb{Z}
- Divisibilité : on dit a est divisible par b ou que b divise a s'il existe $n \in \mathbb{Z}$ tel que $a = nb$.
- Plus Grand Commun Diviseur (pgcd) : noté $\text{pgcd}(a, b) = a \wedge b$
- p est un nombre premier s'il est divisible par 1 et par lui même seulement.
- a et b sont premiers entre eux ssi $a \wedge b = 1$
- $\forall n \in \mathbb{N}, \exists ! p_1, p_2, \dots, p_r, r$ nombres premiers et $\alpha_1, \alpha_2, \dots, \alpha_r$ tels que $n = \prod_{j=1}^r p_j^{\alpha_j}$.

Arithmétiques : Définitions

- **Fonction d'Euler** : c'est la fonction de \mathbb{N} dans lui même, qui à tout n associe $\varphi(n)$ le nombre des entiers premiers avec n .
- **Division euclidienne** : Soient a et b deux entiers, la division euclidienne de a par b est donnée par :

$$a = bq + r \tag{1}$$

Avec, $0 \leq r \leq b - 1$ est le reste de la division euclidienne.

- on écrit $a \equiv r[b]$ et on lit a est congru à r modulo b
- Une permutation est une fonction $\pi(.)$ de $E = \{0, 1, \dots, n\}$ dans lui même et bijective, il existe $n!$ permutation de E .

Propriétés de la congruence

Propriétés de la congruence

Si $a_1 \equiv r_1[b]$ et $a_2 \equiv r_2[b]$ alors :

- $a_1 + a_2 \equiv r_1 + r_2[b]$
- $a_1 * a_2 \equiv r_1 * r_2[b]$
- $a_1^n \equiv r_1^n[b]$
- Si $r_1 = r_2$ alors $b|(a_2 - a_1)$
- Si p est premier et a et b sont deux entiers, alors
 $ab \equiv 0[p] \Leftrightarrow a \equiv 0[p] \text{ ou } b \equiv 0[p]$
- Si $ab \equiv 1[p]$ alors a est l'inverse de b modulo p

Théorèmes

Theorem (Théorème1)

Soit p un nombre premier et a tel que $a \wedge p = 1$ alors
 $a^{p-1}(p-1)! \equiv (p-1)! [p]$

Démonstration :

p ne divise pas a ni $j \in \{1, 2, \dots, p-1\}$, soit Π une permutation de $\{1, 2, \dots, p-1\}$ dans $\{1, 2, \dots, p-1\}$ donc $\forall 0 < j \leq p-1$ on a :

$$ja \equiv \pi(j)[p]. \Rightarrow \prod_{j=1}^{p-1} ja \equiv \prod_{j=1}^{p-1} \pi(j)[p] \text{ Donc } a^{p-1}(p-1)! \equiv (p-1)! [p]$$

Theorem (Théorème2)

Soit p un nombre premier et a est un entier alors $a^p \equiv 1 + (a-1)^p [p]$

Théorèmes

Démonstration :

$a^p = ((a-1) + 1)^p = 1 + (a-1)^p + \sum_{j=1}^{p-1} C_p^j (a-1)^j$, avec $C_p^j = \frac{p!}{j!(p-j)!}$,
 puisque p est premier donc $p | C_p^j \implies \exists k$ tel que $a^p = ((a-1)^p + 1 + pk$

Theorem (Théorème3 : petit théorème de Fermat)

Soit p un nombre premier et a tel que $a \wedge p = 1$ alors $a^{p-1} \equiv 1[p]$

Démonstration 1 :

$a^{p-1}(p-1)! \equiv (p-1)![p]$ Donc $(a^{p-1} - 1)(p-1)! \equiv 0[p]$, p est premier
 donc p ne divise pas $(p-1)!$ ainsi p divise $(a^{p-1} - 1)$, d'où $a^{p-1} \equiv 1[p]$.

Théorèmes

Démonstration 2 :

$$\sum_{j=1}^a (j^p - (j-1)^p) \equiv \sum_{j=1}^a 1[p] \text{ D'après théorème 2. Donc}$$

$$a^p \equiv a[p] \Rightarrow p | (a^p - a) \text{ lorsque } a \text{ et } p \text{ sont premiers entre eux ;}$$
$$p | (a^{p-1} - 1)$$

Exemples

Congruence : $30 \equiv 4[26]$

Inverse : $9 * 3 \equiv 1[26]$

Fermat : $1000^{30} \equiv 1[31]$

Totient d'Euler

Theorem (Théorème 4 : Fonction totient d'Euler)

Soit $n \in \mathbb{N}$ et $n = \prod_{j=1}^r p_j^{\alpha_j}$ sa décomposition en facteurs premiers. La fonction totient d'Euler est donnée par :

$$\varphi(n) = \frac{n}{\prod_{j=1}^r p_j} \prod_{j=1}^r (p_j - 1) \quad (2)$$

Démonstration : Il vient à montrer les trois points :

- Si p est premier $\varphi(p) = p - 1$
- $\varphi(p^m) = (p - 1)p^{m-1}$
- si k et l sont premiers entre eux alors : $\varphi(kl) = \varphi(k)\varphi(l)$

Exemples

$$\varphi(7) = 6$$

$\varphi(28) = \varphi(2^2 * 7) = 2 * (7 - 1) = 12$ Donc il y a 12 nombres premiers à 28

Theorem (Théorème 5 : Euler)

Soit $a \wedge n = 1$ alors $a^{\varphi(n)} \equiv 1[n]$

Démonstration : Selon Fermat : $a^{p-1} \equiv 1[p]$ Donc en utilisant la formule du binôme $a^{(p-1)p^{\alpha_1-1}} \equiv 1[p^{\alpha_1}]$, en l'appliquant aux autres facteurs et en utilisant la propriété de l'opérateur modulo nous aurons : $a^{\varphi(n)} \equiv 1[n]$
La théorème d'Euler est utilisée dans l'algorithme RSA

Algorithm d'Euclide

L'algorithme d'Euclide : est un processus itératif dont le but est la détermination du pgcd de deux entiers a et b . Voilà les étapes de l'algorithme : Considérons $a > b$ on veut déterminer $d = a \wedge b$

$$\begin{aligned}a &= bq_0 + r_0 \\b &= r_0q_1 + r_1 \\r_0 &= r_1q_2 + r_2 \\&\vdots \\r_{N-2} &= r_{N-1}q_N + r_N\end{aligned}\tag{3}$$

- ❶ Arrêt de l'algorithme si $r_N = 0$
- ❷ $0 < r_{N-1} < r_{N-2} < r_{N-3} < \dots < r_0$
- ❸ $d = a \wedge b = b \wedge r_0 = r_0 \wedge r_1 = \dots = r_{N-1}$

Theorem (Théorème de Bezout)

Soit a et b deux entiers et $d = a \wedge b$, $\exists (u, v) \in \mathbb{Z}^2$ tel que :
 $au + bv = d$

Démonstration et exemple :

- 1 Existence : en utilisant l'algorithme d'Euclide
- 2 Détermination : en utilisant l'algorithme d'Euclide étendu
- 3 Exemple d'application : Déterminer l'inverse de 19 modulo 101 (algorithme d'Euclide)
- 4 Déterminer $19^{99} \bmod 101$ (théorème de Fermat)
- 5 on trouve $19^{99} \equiv 16[101]$

Exercices

Déterminer x :

- $x \equiv -1[26]$
- $x \equiv 57[26]$
- $3x \equiv 2[26]$
- $5x^2 \equiv 1[11]$
- $77^{33} \equiv x[31]$

Déterminer u et v :

- $101u + 31v = 1$
- $909u + 33v = 3$
- Calculer $\varphi(26)$ et déterminer u et v : $uv \equiv 1[26]$
- Calculer $\varphi(11)$ et déterminer u et v : $uv \equiv 1[11]$

Clé symétrique

- Les clés sont identiques : $K_E = K_D = K$
- La clé doit rester secrète.
- Les algorithmes les plus répandus sont le DES, AES, 3DES, ...
- Au niveau de la génération des clés, elle est choisie aléatoirement dans l'espace des clés,
- Ces algorithmes sont basés sur des opérations de transposition et de substitution des bits du texte clair en fonction de la clé,
- La taille des clés est souvent de l'ordre de 128 bits. Le DES en utilise 56, mais l'AES peut aller jusqu'à 256,
- L'avantage principal de ce mode de chiffrement est sa rapidité,
- désavantage : pour N utilisateurs il faut : $\frac{N(N-1)}{2}$ clés.

Clé asymétrique

- Une clé publique P_K
- Une clé privée S_K
- La connaissance de P_K ne permet pas déduire S_K .
- $D_{S_K}(E_{P_K}(M)) = M$
- L'algorithme de cryptographie asymétrique le plus connu est le RSA
- La taille des clés s'étend de 512 bits à 2048 bits en standard
- Au niveau des performances, le chiffrement par voie asymétrique est environ 1000 fois plus lent que le chiffrement symétrique.

Introduction

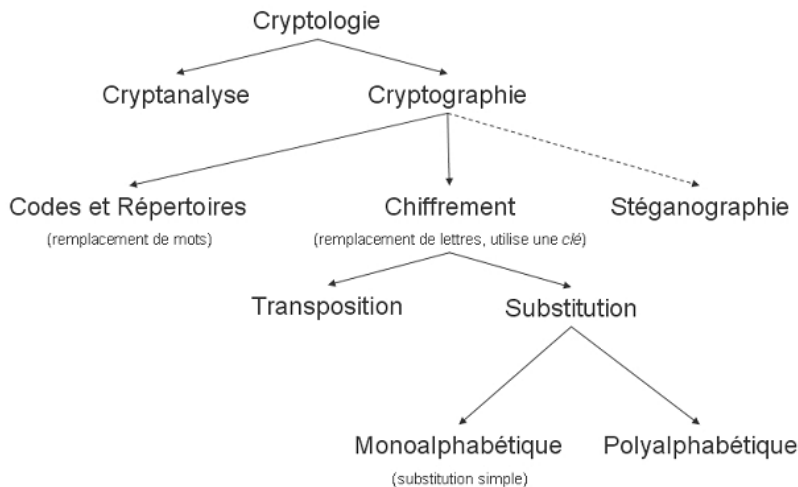


Figure : Domaines inclus dans la cryptologie

Code César(50 avant J-C)

Décalage des lettres de l'alphabet. Soit p l'indice de la lettre et k le décalage (la clé).

- Chiffrement : $c = E(p) \equiv p + k[26]$
- Déchiffrement : $p = D(c) \equiv c - k[26]$
- Il y a 25 clés.

Cryptanalyse

- Force brute : test des clés
- Analyse des fréquences des lettres : A et E sont les plus fréquentes en français, le moins fréquent : W.
- Test de digrammes : $ES \leftarrow 3318$, $DE \leftarrow 2409$, $LE \leftarrow 2366, \dots$
- Test de trigrammes : $ENT \leftarrow 900$, $LES \leftarrow 801$, $EDE \leftarrow 630, \dots$

Code affine

Une fonction de la forme : $x \mapsto ax + b$ est dite affine.

- Chiffrement affine : soit $(k_1, k_2) \in [1, 25] \times [0, 25]$ le message chiffré est : $c \equiv k_1 m + k_2 [26]$
- Déchiffrement : $k_1 \wedge 26 = 1$ et $m \equiv (k_1)^{-1}(c - k_2)[26]$
- Il y a $[n\varphi(n) - 1]$ clés.

Cryptanalyse

- texte chiffré : HGAHY RAEFT GAGRH DGAGM OEHIY RAAOT ZGAGJ GKFDG AZGSB INNTG KGRHE NNIRG \Rightarrow On remarque que G apparaît 12 fois et A 8 fois.
- E, A, S, I sont les lettres les plus fréquentes, donc $E \rightarrow G$ et $S \rightarrow A$
- Trouver (k_1, k_2) tel que, $4k_1 + k_2 \equiv 6[26]$ et $18k_1 + k_2 \equiv 0[26]$
 $14k_1 \equiv -6[26] \Rightarrow 7k_1 \equiv 10[13] \Rightarrow k_1 = 7, k_2 = 4$