Cryptographie

Informatique

2017/2018

Table des matières

Objectifs

L'objectif générale de ce module est d'utiliser le système de clé publique et privée pour chiffrer et déchiffrer à l'aide des techniques anciennes et modernes de cryptographie.

A la fin de ce cours l'étudiant doit être capable de :

- Différencier entre un système de chiffrement à clé privé et un système de chiffrement à clé publique

- Utiliser les principaux algorithmes symétrique et asymétrique pour chiffrer et déchiffrer les messages

- Choisir les bons algorithmes pour chiffrer et déchiffrer selon les besoins.

Introduction

Avec l'avènement des réseaux et d'Internet, du commerce électronique, la cryptologie a connu un essor considérable où le transfert de l'information se fait à travers ces réseaux dans tous les domaines, ce qui a accru la nécessité de protéger ces informations pendant leur transfert. C'est le rôle de la cryptographie.

En revanche, la cryptanalyse est l'étude des procédé cryptographique, dans le but de trouver des faiblesses, en particulier de décrypter des messages chiffrés sans connaître la clé de déchiffrement. Pour que la cryptographie résiste à la cryptanalyse, des cryptosystèmes sont composés par diverses fonctions complexes qui assurent non seulement la sécurité des données mais aussi leur intégrité, authenticité,....

La cryptographie a connu deux types : la cryptographie symétrique qui utilise une seule clé secrète pour le chiffrement et le déchiffrement et la cryptographie asymétrique qui utilise une paire de clés, une clé publique pour le chiffrement et une clé privée pour le déchiffrement.

Ce cours est organisé en trois chapitres, le premier présente des généralités sur la cryptographie, le deuxième chapitre présente le système de chiffrement asymétrique a savoir les principaux algorithmes utiliser dans ce système et le troisième chapitre détaille le système de chiffrement symétrique.

En termine ce cours par la mise de l'étudiant dans un situation problématique pour employer les connaissance acquise.

Pré-requis

L'étudiant doit connaître comment calculer PGCD avec l'algorithme d'Euclide, déterminer des coefficients de Bézout et d'utiliser les technique de calcul dans les congruences.

Généralités sur la cryptographie

II

La cryptographie moderne a été développée pour atteindre certains buts tels que: l'authentification, la confidentialité, l'intégrité des données, la non répudiation, le contrôle d'accès et la gestion des clés. La cryptographie doit satisfaire ces principales fonctions de sécurité.

La cryptographie est essentiellement basée sur les mathématiques en utilisant des clés, et se partage en deux types : la cryptographie symétrique qui utilise une même clé pour le chiffrement/déchiffrement et la cryptographie asymétrique qui utilise une paire de clés : une clé publique pour le chiffrement et une clé privée pour le déchiffrement.

1. Terminologie sur la cryptographie

- Chiffrement : c'est la méthode ou l'algorithme utilisé pour transformer un texte en clair en un texte chiffré.
- Déchiffrement : c'est la méthode ou l'algorithme utilisé pour transformer un texte chiffré en un texte en clair.
- Clé : c'est le secret utilisé pour chiffrer un texte ou déchiffrer le texte chiffré.
- Cryptosystème: c'est l'ensemble des clés possibles (espace de clés), des textes clairs et chiffrés possibles associés à un algorithme donné. La figure 1.1 représente le schéma d'un cryptosystème

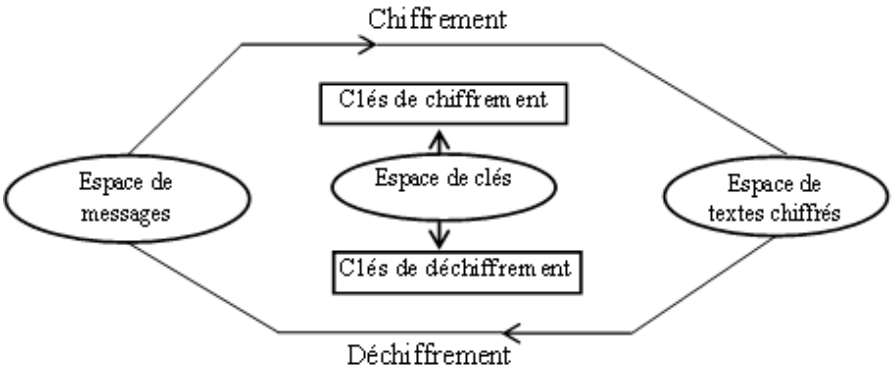

Figure 1.1 : Schéma d'un cryptosystème.

Un cryptosystème est en réalité un triplet d'algorithmes :

• L'un générant les clés

• L'autre pour chiffrer les messages

• Le troisième pour déchiffrer les messages.

2. Historique de la cryptographie

L'origine du mot cryptographie provient du grec kryptós (caché) et gráfein (écrire). On peut définir la cryptographie comme l'ensemble des techniques permettant de protéger une communication, par exemple l'assurance que l'information contenue dans un message n'est révélée qu'au seul destinataire de ce message.

Le code de César est la méthode cryptographique, par substitution mono alphabétique, la plus ancienne (1ier siècle av. J.-C.). Cette méthode est utilisée dans l'armée romaine.

Le cryptogramme de César

Le chiffre de César consiste simplement à décaler les lettres de l'alphabet de quelques crans vers la droite ou la gauche. Par exemple, décalons les lettres de 3 rangs vers la gauche, comme le faisait Jules César (d'où le nom de ce chiffre):

Clair	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
Chiffré	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

Figure 1.2 : Le chiffre de césar de décalage à 3 lettres.

Exemple

Donc le message "Avec cesar " devient "DYHF FHVDU" en utilisant le tableau précédent.

Le chiffrement de Vigenère

est une amélioration décisive du chiffre de César. Sa force réside dans l'utilisation non pas d'un, mais de 26 alphabets décalés pour chiffrer un message. On peut résumer ces décalages avec un carré de

Vigenère. Ce chiffre utilise une clef qui définit le décalage pour chaque lettre du message (A: décalage de 0 cran, B: 1 cran, C: 2 crans, ..., Z: 25 crans).

Exemple

Chiffrons le texte "CHIFFRE DE VIGENERE" avec la clef "BACHELIER" (cette clef est éventuellement répétée plusieurs fois pour être aussi longue que le texte clair).

Clair	C	H	I	F	F	R	E	D	E	V	I	G	E	N	E	R	E
Clef	B	A	C	H	E	L	I	E	R	B	A	C	H	E	L	I	E
Décalage	1	0	2	7	4	11	8	4	17	1	0	2	7	4	11	8	4
Chiffré	D	H	K	M	J	C	M	H	V	W	I	I	L	R	P	Z	I

Figure 1.3 : Exemple de chiffrement de Viginère.

La grande force du chiffre de Vigenère est que la même lettre sera chiffrée de différentes manières. Par exemple le E du texte clair ci-dessus a été chiffré successivement M V L P I.

3. Les types de la cryptographie

La cryptographie est une science permettant de correspondre de manière sécurisée en utilisant des canaux non sécurisés, elle permet de convertir des informations "en clair" en informations codées, c'est-à-dire non compréhensibles, puis à partir de ces informations codées, on restitue les informations originales.

Selon la notion de clé pour le chiffrement et déchiffrement, on peut distinguer deux types de cryptographie : la cryptographie symétrique et la cryptographie asymétrique.

La cryptographie symétrique

Aussi appelé chiffrement à clé privée ou chiffrement à clé secrète, elle consiste à utiliser la même clé pour le chiffrement/déchiffrement qui doit rester secrète. Son principal avantage est la rapidité du calcul car elle utilise des clés de petites tailles et se base sur des opérations simples : additions et décalages. Mais elle présente deux inconvénients majeurs qui sont l'échange de la clé secrète via un canal sécurisé non disponible et la gestion des clés où pour que n personnes puissent communiquer, il faut gérer n(n-1)/2 clés (une pour chaque paire de personnes). La figure 1.4 montre le principe du chiffrement symétrique.

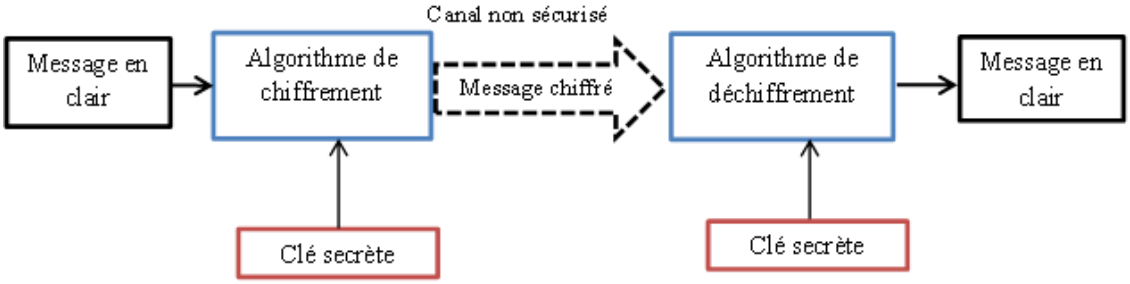

Figure 1.4 : Principe du chiffrement symétrique.

Il existe deux types d'algorithmes de chiffrement symétrique. Le premier type, qui est le plus utilisé, est le chiffrement par blocs, où les données sont traitées par bloc de bits et les standard les plus utilisés sont le DES (Data Encryption Standard) et l'AES (Advanced Encryption Standard). Le second type est le chiffrement à flot. Celui-ci permet après une période d'initialisation de chiffrer bit par bit [1, 2].

La cryptographie asymétrique

La cryptographie asymétrique ou à clé publique est couramment utilisée pour désigner une méthode de chiffrement d'un message en utilisant une clé publique pour obtenir un message chiffré qui sera transféré via un canal non sécurisé. Ce message chiffré sera déchiffré en utilisant une clé privée (ou secrète) pour retrouver le message d'origine comme le montre la figure 1.5. Dans ce type de cryptographie, les problèmes du transfert de la clé secrète et de la gestion des clés posés par la cryptographie à clé secrète sont réglés.

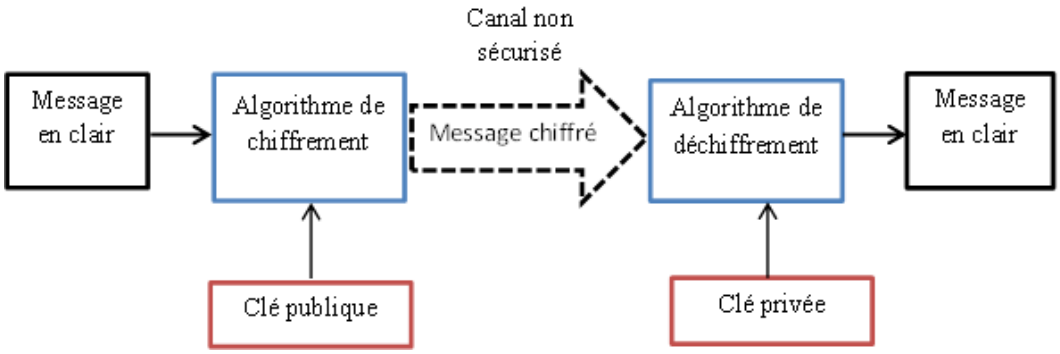

Figure 1.5 : Principe du chiffrement asymétrique.

4. Les types de la cryptanalyse

La cryptanalyse est la technique qui consiste à déduire un texte en clair d'un texte chiffré sans posséder la clé de chiffrement. Le processus par lequel on tente de comprendre un message en particulier est appelé une attaque. On peut résumer les attaques en :

• Attaques classiques : L'attaquant connaît les algorithmes de cryptage et décryptage

• Attaque à texte crypté uniquement : L'attaquant ne dispose que d'un ou plusieurs messages cryptés qu'il souhaite décrypter. C'est le type d'attaque le plus difficile.

• Attaque à texte clair connu : L'attaquant dispose d'exemples de messages clairs avec les messages cryptes correspondants, ou d'une partie claire d'un message crypte. Le but est d'obtenir de l'information sur la clé.

• Attaque à texte clair choisi : L'attaquant peut obtenir la version cryptée d'un certain nombre de

messages clairs choisis, soit avant l'attaque (attaque hors ligne), soit au fur et a mesure (attaque en ligne). Le but est encore d'obtenir de l'information sur la clé.

• Attaque à texte crypte choisi : L'attaquant peut obtenir la version cryptée d'un certain nombre de messages clairs choisis, et aussi la version claire d'un certain nombre de messages cryptés choisis. On distingue encore entre attaques hors ligne et en ligne.

• Attaque par le paradoxe des anniversaires : Il s'agit d'obtenir des collisions (utilisation deux fois d'une même valeur) pour obtenir de l'information. Si on utilise 2n valeurs possibles, on peut espérer la première collision avec environ 2n=2 valeurs.

• Attaque par pré-calcul : Il s'agit pour l'attaquant de pré-calculer des informations et de s'en servir pour identifier des messages ou des clés. Cela nécessite plus de travail mais permet aussi plus de flexibilité. Un cas extrême est la recherche exhaustive.

• Attaque de différentiation : Il s'agit d'une attaque qui permet de différencier le protocole de cryptage utilisé d'un protocole de cryptage parfait. Cela couvre les attaques citées précédemment et toutes les attaques a venir !

5. Exercices

Exercice N° 1

En utilisant la substitution mono-alphabétique suivante:

Lettre en clair : a b c d e f g h i f k l m n o p q r s t u v w x y z

Lettre chiffrée : m n b v c x z a s d f g h j k l p o i u y t r e w q

- Chiffrez le message "This is an easy problem."

Exercice N° 2

Un alphabet réversible (ou réciproque) est un alphabet désordonné qui, quand on l'applique deux fois à un message clair, redonne le message clair. En français, un alphabet réversible s'obtient en prenant les 13 couples de 2 des 26 lettres utilisées et en considérant les lettres de chaque couple comme chiffrées et déchiffrées l'une de l'autre. Voici un exemple.

A B C D E G K L N O P Q R

F S W Z M Y X U J I V T H

Appelons invariant une lettre chiffrée par elle-même. Un alphabet réversible sans invariants peut s'écrire sur deux lignes d'un tableau (exemple précédent).

1. Construire un tableau pour la clé MAISON.
2. Chiffrer avec la clé MAISON le message « BONJOUR ».

Exercice N° 3

Voici un texte chiffré par le chiffre de César:

YRLFL XQWHA WHFKL IIUHS DUOHF KLIIU HGHFH VDU

1. Quel est la taille de l'espace de clés.
2. Retrouvez le texte clair.
3. Appliquer deux fois le chiffre de César sur le message trouvé (avec la clé H, puis la clé O).
4. It-il plus difficile de retrouver le message clair.

Exercice N° 4

Soit le vecteur de substitution suivant à utiliser pour le cryptage de Viginère : V=(14,12,20,1,14)

1. déterminer la clé
2. trouver le message crypté du message « ce message est top secret »

Exercice N° 5

Ce message a été obtenu par chiffrement de Vigenère avec le mot-clé "RAYMOND"

RILEW FRETJ QGZRV UPERR VDAJQ

GRWUE QRSZH CLCER NQJLC DSTQV

ALUAN OUEDM QBQGR MHWQH ETGQZ

YH

- trouver le message clair.

La cryptographie asymétrique

III

En 1975, W. Diffie et M.E. Hellman révolutionnaient la science de la cryptographie en démontrant l'existence d'un protocole qui ne pouvait être déchiffré par un intercepteur à moins que ce dernier ne disposât de conséquentes ressources informatiques. Le plus fascinant dans leur méthode - dont le principe est encore en usage aujourd'hui - c'est que le code utilisé ne nécessite pas le camouflage de la méthode employée et qu'il peut servir à maintes reprises sans aucune modification (principe de Kerchoff). Ils ont à l'époque tout simplement créé le concept de cryptographie à clé publique, ou cryptographie asymétrique (dont nous avons déjà fait mention au tout début de ce chapitre), invention qui suscita l'émergence d'une communauté universitaire et industrielle dynamique.

1. La sécurité des cryptosystèmes à clé publique

La sécurité d'un cryptosystème à clé publique est dite calculatoire car il n'est pas possible de retrouver l'information secrète à partir des informations transmises publiquement sans faire un quelconque calcul d'une complexité exagérée.

Cette sécurité est basée sur des problèmes mathématiques considérés comme difficiles à résoudre tels que :

• La factorisation de grands nombres entiers : exemple du crypto système RSA ;

• Le calcul du logarithme discret dans le groupe multiplicatif d'un corps fini : le protocole d'échange de clés de Diffie-Hellman et le cryptosystème El Gamal ;

• Le calcul du logarithme discret dans le groupe additif des points d'une courbe elliptique définie sur un corps fini : Elliptic Curve Cryptography(ECC).

2. Les principaux algorithmes à clés publiques

Le protocole d'échange de clés de Diffie-Hellman

Ce n'est pas un système à clé publique, il s'agit d'un protocole qui permet à deux communicants qui partagent seulement de l'information publique d'établir une clé commune. La sécurité se fonde sur la difficulté de calculer des logarithmes discrets.

Principe du protocole

Soit A et B, les deux entités qui veulent s'échanger une clé K :
• A génère un nombre premier p et un générateur a (1<a<p, p et a sont publics).
• A génère un nombre aléatoire : $X_A < p$, et B génère un autre nombre aléatoire : $X_B < p$ (gardés secrets).
• A calcule $y_A = a^{X_A} [\text{mod } p]$, et B calcule $y_B = a^{X_B} [\text{mod } p]$ (yA et yB sont publics).
• A calcule $KAB = y_B^{X_A} [\text{mod } p]$, et B calcule $KBA = y_A^{X_B} [\text{mod } p]$
• A et B partagent ainsi la même clé KAB = KBA.
Si quelqu'un a espionné : p, a, y_A et y_B, pour obtenir K, il doit pouvoir calculer X_A. Autrement dit, il doit pouvoir résoudre l'équation: $X_A = \log_a^{y_A} [\text{mod } p]$
On appelle ceci résoudre ≤ problème du logarithme discret. Quand les valeurs de p, a et yA sont très grandes, il s'agit d'un problème très difficile.

L 'algorithme d'El Gamal

C'est un système à clé publique basé sur le problème de Diffie-Hellman. Il fut inventé par Taher El Gamal [3].

Il est basé sur la difficulté de calculer des logarithmes discrets.problème du logarithme discret consiste à retrouver un entier λ tel que :

$$h = g^{\lambda} \text{ mod } p.$$

Principe de l'algorithme

L'algorithme est présenté en trois étapes, soient X et Y, les deux parties qui veulent communiquer :

1 – Génération de la clé
• X génère un grand nombre premier p et un générateur g tel que : $2 \leq g \leq p-1$.
• X choisit de façon aléatoire un exposant $a \in \{0,1,2,\ldots,P-1\}$ et on calcule : $A = g^a \text{ mod } p$, la clé publique est (A), la clé sécrète est l'exposant a pour l'entité X.
De même pour Y, on choisit un exposant aléatoire $b \in \{0,1,2,\ldots,P-1\}$ et on calcule :
$B = g^b \text{ mod } p$, la clé publique est (B), La clé sécrète est l'exposant b pour l'entité Y.
2 – Chiffrement
Si l'entité Y veut chiffrer un message m, on calcule $c = Abm \text{ mod } p$.
Donc ≤ code chiffré comprend :
• La clé publique de Y : $(B = g^b \text{ mod } p)$.
• ≤ message chiffré $(c = A^b m \text{ mod } p)$.
3 – Déchiffrement
A la réception de (B, c), on divise c par $B^a \text{ mod } p$ comme suit : $m = c / B^a \text{ mod } p$.

L'algorithme R.S.A

RSA (Rivest-Shamir-Adleman), inventé en 1978, est le cryptosystème le plus utilisé de nos jours. Sa sécurité dépend de la difficulté à trouver la factorisation du produit de deux grands nombres premiers.

Principe de l'algorithme

L'algorithme est en trois étapes résumées comme suit :

1 – Génération des clés
• On génère deux grands nombres premiers P *et* Q.
• On calcule n. *Il doit s'agir d'une valeur assez élevée, c'est ≤ produit de P et Q.*
La taille de n peut varier : 512 bits, 768, 1024, 2048…
• On choisit un très grand entier e, *relativement premier avec* $\phi(n)=[(P-1)(Q-1)]$. *La clé publique sera formée par* (e,n).
• On choisit ensuite un d *tel que :* $e*d \equiv 1 \bmod[\phi(n)]$, *la clé privée sera donnée par* (d,n).
• On jette P et Q, il faut les détruire pour éviter les fuites.
2 – Chiffrement : Pour chiffrer un message M, on calcule $C=M^e \bmod n$.
3 – Déchiffrement : Pour déchiffrer un message chiffré C, on calcule $M=C^d \bmod n$.

Le principe de fonctionnement du protocole RSA est représenté sur la figure 1.6.

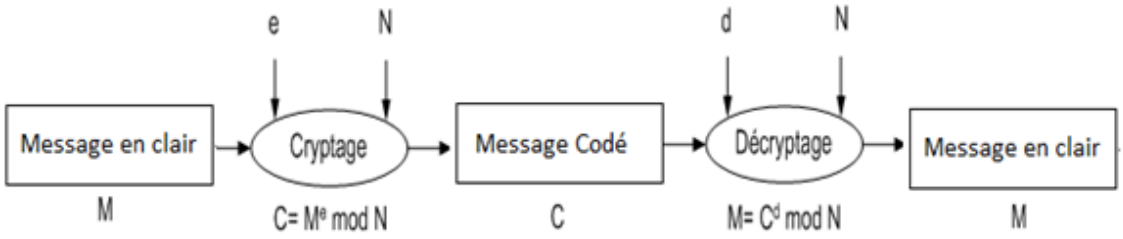

Figure 1.6 : Schéma bloc du principe de fonctionnement du RSA.

Exemple

cet exemple illustre le déroulement de RSA

Préparation des clés			
·	Deux nombres premiers tenus secrets	p et q	3 et 7
·	Son produit n est diffusé	n = p.q	n = 21
·	On calcule f	Q(n) = (p – 1) (q – 1)	Q(n) = 2x6 = 12
·	Un nombre e est, lui aussi, diffusé	e premier avec Q(n)	e = 5
·	Je calcule d, inverse de e mod f	e.d = 1 mod Q(n)	5d = 1 mod 12
			5x5 = 1 mod 12
			d = 5
Préparation du message			
·	Le message est converti en chiffres	x1 … xi …avec xi < n	x = 2, par exemple
·	On va coder chaque chiffre		
Chiffrement du message			
·	Chaque x est codé par y		$y = 2^5 \bmod 21$
			y = 32 mod 21
			y = 11
·	Les valeurs de y sont transmises		11 st transmis
Déchiffrement du message			
·	Je calcule z	z = y d mod n	$z = 11^5 \bmod 21$
			z = 11 x121x121 mod 21
			z = 11 x 16 x 16 mod 21
			z = 11 x 256 mod 21
			z = 44 mod 21
			z = 2 mod 21
·	Car en fait z = x mod n		z = 2 mod 21

3.

Exercices

Exercice 1 :

On considère les valeurs p = 53, q = 11 et e = 3.

1. Calculez la valeur publique n.
2. Calculez la fonction d'Euler $\phi(n) = (p - 1)(q - 1)$.
3. Rappeler l'algorithme étendu d'Euclid.
4. Utilisez l'algorithme étendu d'Euclid pour calculer la valeur d de la clé privée.
5. Chiffrer le message m = 64, puis m=18447754454.

Exercice 2 :

1. Dire si les paramètres privés (p, q, a) suivants sont corrects et, le cas échéant, calculer les paramètres publics correspondants : (i) (5, 7, 5), (ii) (13, 7, 9), (iii) (63, 47, 17), (iv) (229, 257, 125).
2. Soient les paramètres publics (n = 187, b = 3), chiffrer le message m = 64.

Exercice 3 :

Soient Ai, $i \in \{1, 2, 3, 4\}$ possédant chacun un module RSA ni. On suppose qu'ils possèdent tous la même clé de chiffrement bi = 4. Un même message x est chiffré et leur est envoyé à chacun.

1. Montrer qu'en interceptant les différents chiffrés (i.e. yi = x 4 mod ni) un attaquant peut déchiffrer le message sans connaître la clé de déchiffrement.
2. Appliquer cette attaque au cas : n1 = 38, n2 = 51, n3 = 65, n4 = 77 et y1 = 23, y2 = 16, y3 = 40, y4 = 4.