ENSA
ÉCOLE NATIONALE DES SCIENCES APPLIQUÉES
KHOURIBGA

CRYPTOGRAPHIE

MODULE: Cryptographie

Ce cours est une initiation à la cryptographie. Il permet d'acquérir les connaissances théoriques nécessaires à une bonne compréhension de la cryptographie. Ces connaissances permettent de protéger des messages afin de mieux sécuriser des systèmes d'information.

Evaluation

Examen écrit : 70%

Projet : 30%

2

Programme

I. Introduction: Notions de base de la cryptographie (histoire, Chiffrement et déchiffrement, cryptanalyse, qualités d'un cryptosystème, …)

II. Cryptographie ancienne

2. Chiffrement par transposition

3. Chiffrement par substitution

III. Cryptographie moderne

4. Chiffrement asymétrique

5. Chiffrement symétrique

Projet : Programmation d'un algorithme de cryptage

3

Introduction

Problématique

Depuis l'Egypte ancienne, l'être humain a voulu pouvoir échanger des informations de façon **confidentielle**.

Il existe de nombreux domaines où ce besoin est vital :

— **militaire** (sur un champ de bataille, protéger l'accès à l'arme atomique, …) ;

— **commercial** (protection de secrets industriels) ;

— **bancaire** (protection des informations liées à une transaction financière) ;

— de la **vie privée** (protection de la messagerie entre les personnes) ;

— **diplomatique** (le fameux « téléphone rouge » entre Etats-Unis et Union soviétique) ;

5

Qu'est-ce que la cryptographie?

Origine du mot:

***Cruptos** : caché, dissimulé ; **Graphein** : écrire*

Cryptographie

La cryptographie est l'art de rendre inintelligible (incompréhensible), de crypter, de coder, un message pour ceux qui ne sont pas habilités à en prendre connaissance.

La cryptographie est traditionnellement utilisée pour dissimuler des messages aux yeux de certains utilisateurs. Cette utilisation a aujourd'hui un intérêt d'autant plus grand que les communications via internet circulent dans des infrastructures dont on ne peut garantir la fiabilité et la confidentialité.

La cryptographie est un outil qui permet d'atteindre des objectifs de sécurité

(d'autres outils comprennent des logiciels anti-virus, du matériel, etc.,)

6

Message chiffré et message en clair

La cryptographie est essentiellement basée sur l'arithmétique.

Dans le cas d'un texte, Il s'agit de transformer les lettres qui composent le message en une succession de chiffres, puis ensuite de faire des calculs sur ces chiffres pour les modifier de telle façon à les rendre incompréhensibles.

Le résultat de cette modification (***message chiffré***) est appelé **cryptogramme** (en anglais *ciphertext*) par opposition au message initial, appelé ***message en clair*** (en anglais *plaintext*).

7

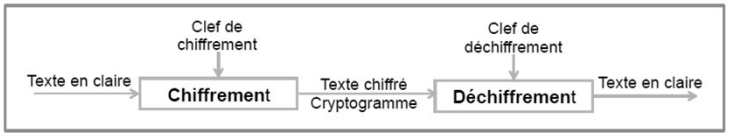
Chiffrement et déchiffrement

Le fait de coder un message pour le rendre secret s'appelle **chiffrement**.

La méthode inverse, consistant à retrouver le message original, est appelée **déchiffrement**.

Le chiffrement se fait généralement à l'aide d'une ***clef de chiffrement***,

le déchiffrement nécessite quant à lui une ***clef de déchiffrement***.



8

Cryptanalyse et cryptologie

La **cryptanalyse** est l'art pour une personne non habilitée, de décrypter (décoder, déchiffrer) un message. C'est donc l'ensemble des procédés d'attaque d'un système cryptographique.

Ainsi, tout cryptosystème doit nécessairement être résistant aux méthodes de cryptanalyse. Lorsqu'une méthode de cryptanalyse permet de déchiffrer un message chiffré à l'aide d'un cryptosystème, on dit alors que l'algorithme de chiffrement a été « cassé ».

La **cryptologie** est la science qui englobe la cryptographie et la cryptanalyse.

Cryptologie = Cryptographie + Cryptanalyse

9

Fonctions de chiffrement et de déchiffrement

Un expéditeur Alice veut envoyer un message à un destinataire Bob en évitant les oreilles indiscrètes d'Eve, et les attaques malveillantes de Martin.

Pour cela Alice se met d'accord avec Bob sur le cryptosystème qu'ils vont utiliser.

Soient:

M: le texte clair (l'information qu'Alice souhaite transmettre à Bob).

C: le message chiffré,

E: fonction de chiffrement définie par :

C = E(M).

D: **fonction de déchiffrement** (ou décodage). C'est le processus de reconstruction du message clair à partir du message chiffré.

On demande que pour tout message clair M:

D(C) = D(E(M)) = M

10

Algorithme cryptographique

Un algorithme cryptographique est l'ensemble des fonctions (mathématiques ou non) utilisées pour le chiffrement et le déchiffrement.

En pratique les fonctions E et D sont paramétrées par des clés:

- **Ke** la clé de chiffrement
- **Kd** la clef de déchiffrement;

Ces clés peuvent prendre l'une des valeurs d'un ensemble appelé espace des clefs.

On a donc la relation suivante:

$$\begin{cases} E_{K_e}(M) = C \\ D_{K_d}(C) = M \end{cases}$$

11

Méthodes anciennes de cryptographie: Substitution et transposition

Les chiffrements anciens partent d'un message contenant des lettres vers un cryptogramme contenant également des lettres.

Ces méthodes se décomposent en deux grandes familles de chiffrement :

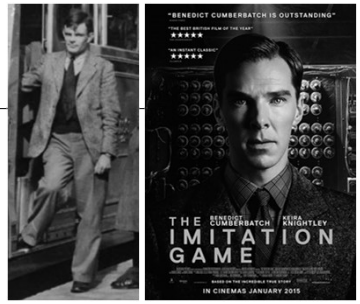
1) **Par transposition:** Modifier l'ordre des lettres du texte clair, pour obtenir le texte chiffré. On utilise le principe mathématique des **permutations.**
2) **Par Substitution** : Remplacer les caractères du texte clair par d'autres caractères.

12

cryptographie durant les deux guerres mondiales

Peu avant la Première Guerre mondiale a eu lieu une révolution technologique. Les communications entre l'état-major et les troupes se font désormais essentiellement par radio. Mais ces communications sont facilement interceptables par l'ennemi. Il faut impérativement les chiffrer!

Les chiffrements vont s'automatiser, surtout avec la naissance du premier ordinateur.



Le travail du mathématicien Alan Türing pour déchiffrer les messages allemands cryptés par la machine allemande Enigma a permis de sauver plusieurs centaines de navires avec leurs équipages!

13

Méthodes modernes de cryptographie

De nos jours, on distingue généralement deux types de chiffrements :

❖***Chiffrement symétrique (clé privée):*** La même clé doit être employée pour chiffrer et déchiffrer le message. (Exemple code DES). Expéditeur et destinataire doivent s'échanger cette clé, qui doit rester secrète sous peine qu'un tiers parvienne à déchiffrer les correspondances.

❖***Chiffrement asymétrique (clé publique): U***ne clé est utilisée pour le chiffrement et une autre pour le déchiffrement. (Exemple: code RSA)

14

Applications modernes de cryptographie

Depuis les années 1970, la cryptographie n'est plus seulement l'affaire des militaires.

Les applications civiles du chiffrement deviennent un moteur fondamental de progrès (banques, télécommunications, informatique,...)

Les cartes bancaires: Les banques font partie des premiers utilisateurs de systèmes cryptographies. Les cartes bancaires possèdent en général trois niveaux de sécurité (le code confidentiel, la signature RSA, l'authentification DES)

Les navigateurs Web: Les navigateurs, ou *broswers*, tels que Mozilla Firefox ou Internet Explorer, utilisent le protocole de sécurité SSL (*Secure Sockets Layers*), qui repose sur un procédé de cryptographie par clé publique : le RSA.

15

Principe important (Kerckhoffs 1883)

La sécurité d'un cryptosystème ne doit pas reposer sur le secret de l'algorithme de codage mais uniquement sur la clef secrète.

Cette clef secrète est un paramètre facile à changer, de taille réduite (actuellement de 64 à 2048 bits) et donc assez facile à transmettre secrètement.

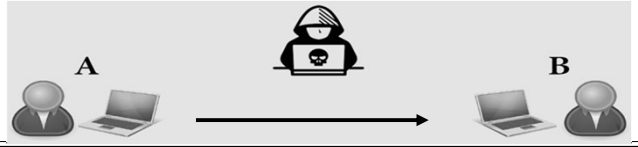
16

Qualités essentielles d'un cryptosystème.

1) Confidentialité: seules les personnes habilitées ont accès au contenu du message. Un attaquant ne peut pas voir le message.

2) Authenticité: le destinataire est sûr de l'identité de l'émetteur, et réciproquement.

3) Intégrité: le message ne peut pas être modifié par un attaquant sans qu'on s'en aperçoive.



17

Sécurité calculatoire

C'est la sécurité calculatoire que l'on utilise dans la plupart des évaluations de sécurité des systèmes cryptographiques.

La sécurité calculatoire repose sur l'impossibilité de faire en un temps raisonnable, compte tenu de la puissance de calcul disponible, les calculs nécessaires pour décrypter un message.

La notion de sécurité calculatoire repose sur la théorie de la complexité.

Exemple: même avec des ordinateurs faisant 10^9 opérations élémentaires par seconde, un calcul qui nécessite 2^{100} opérations élémentaires est hors de portée actuellement car pour l'effectuer il faut environ 4 x 10^{13} années!

18

PARTIE 1

CRYPTOGRAPHIE ANCIENNE

Chiffrement par transposition

Méthode de la grille

Chiffrement par transposition

Dans le chiffrement par transposition (permutation), on partage le texte en blocs, on garde le même alphabet mais on change la place des lettres à l'intérieur d'un bloc (on les permute).

21

Exemple: méthode de la grille (-450 AJC)

On veut envoyer le message suivant:

RENDEZ VOUS DEMAIN MIDI VILLETANEUSE

L'expéditeur et le destinataire du message se mettent d'accord sur une grille de largeur fixée à l'avance (ici une grille de 6 cases de large, c'est le nombre de colonnes).

L'expéditeur écrit le message dans la grille en remplaçant les espaces entre les mots par le symbole □.

R	E	N	D	E	Z
□	V	O	U	S	□
D	E	M	A	I	N
□	M	I	D	I	□
V	I	L	L	E	T
A	N	E	U	S	E

Il lit le texte en colonne et obtient ainsi le message crypté:

R□D□VAEVEMINNOMILEDUADLUESIIESZ□N□TE

22

Méthode de la grille avec clé secrète

Pour pouvoir changer facilement le cryptage d'un message tout en gardant le même algorithme de codage, on rajoute une clé secrète qui va indiquer l'ordre de lecture des colonnes.
Il y a 6! chiffrements différents.

Par exemple, on choisit la clé: **CAPTER**

On numérote les colonnes en fonction du rang des lettres du mot CAPTER dans l'alphabet:

2, 1, 4, 6, 3, 5

R	E	N	D	E	Z
□	V	O	U	S	□
D	E	M	A	I	N
□	M	I	D	I	□
V	I	L	L	E	T
A	N	E	U	S	E

et on lit les colonnes dans l'ordre indiqué pour trouver le message chiffré:

EVEMIN R□D□DAVA DUADLU Z□N□TE NOMILE ESIIES

23

Exercice

Avec la méthode de la grille et la clé « **MASTER** », crypter le message suivant:

« **Ceci passera aussi** »

24

Chiffrement par substitution

Chiffrement par substitution

Il consiste à remplacer les caractères du texte clair par d'autres caractères.

Les chiffrements les plus fréquents:

- **Substitution monoalphabétique:** consiste à remplacer chaque lettre du message par une autre lettre (Exemple: code César, code affine)
- **Substitution polyalphabétique:** consiste à utiliser une suite de chiffrement monoalphabétique réutilisée périodiquement (Exemple: code Vigenère)

26

Rappels
Arithmétique modulaire

Pourquoi l'arithmétique?

l'arithmétique est au cœur du cryptage des messages. Pour crypter un message on commence par le transformer en nombres.

Le processus de codage et décodage peut faire appel à plusieurs notions d'arithmétique:

- Les calculs dans Z/nZ
- Les *nombres premiers et la décomposition en facteurs premiers*
- Des théorèmes fondamentaux comme le *petit théorème de Fermat*.

28

Divisibilité et division euclidienne

Soient a et b deux entiers relatifs. On dit que a **divise** b, ou que a est un **diviseur** de b, s'il existe k∈Z tel que b=ka. On dit encore que b est un **multiple** de a.

Remarques

- (a/b et b/a) $\Longrightarrow b = \pm a$
- (a/b et b/c) $\Longrightarrow a/c$
- (a/b et a/c) $\Longrightarrow a/(b + c)$

Théorème (division euclidienne) : Soient a∈Z et b∈N^*. Il existe un unique couple (q,r)∈Z^2 tels que a=bq+r et 0≤r<b.

q s'appelle le **quotient** et r s'appelle le **reste**.

r = 0 si et seulement si *b* divise *a*.

29

Congruence modulo n

Soient a et b deux entiers relatifs et n un entier naturel.

On dit que a et b sont **congrus modulo n,** et on note a≡b[n] (ou a≡b (mod n)), si n divise a-b.

$$a \equiv b\ [n] \iff n/a-b \iff \exists\ k \in Z \text{ tel que } a-b=kn$$

On appelle **classe d'équivalence** modulo n d'un élément x de Z, notée $\bar{x}$, l'ensemble des y qui sont congrus à x modulo n: $\bar{x} = \{y \in \mathbb{Z} : y \equiv x[n]\}$

On a : $\bar{x} = \bar{y} \Leftrightarrow y \equiv x[n] \Leftrightarrow x \equiv y[n] \Leftrightarrow n/x\text{-}y$.

Il existe n classes d'équivalence. L'ensemble de toutes les classes d'équivalence est Z/nZ, appelé **l'ensemble quotient** de Z par la congruence modulo n.

$$Z/nZ = \{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1}\}$$

30

Arithmétique modulaire

On peut définir dans Z/nZ l'addition et la multiplication :

$$\bar{x} + \bar{y} = \overline{x+y} \qquad \bar{x}.\bar{y} = \overline{x.y}$$

(Z/nZ;+, .) est un anneau commutatif.

Exemple. Tables d'addition et de multiplication dans Z/4 Z.

+	0·	1·	2·	3·
0·	0·	1·	2·	3·
1·	1·	2·	3·	0·
2·	2·	3·	0·	1·
3·	3·	0·	1·	2·

×	0·	1·	2·	3·
0·	0·	0·	0·	0·
1·	0·	1·	2·	3·
2·	0·	2·	0·	2·
3·	0·	3·	2·	1·

31

Exercice

1) Calculer $\overline{2018}$ dans Z/7Z.

2) Calculer $\overline{213}$+ $\overline{17}$ et $\overline{213} - \overline{17}$ dans Z/7Z.

3) Tracer la table de multiplication modulo 7 (Z/7Z)

32

Substitution mono-alphabétique
Code de César

Code de César

Jules César

Il est plus facile de manipuler des nombres que des lettres.

Pour coder on remplace chaque lettre par son rang dans l'alphabet.

A=1, B=2, C=3,....,M=13, N=14,...,S=20,...,X=24, Y=25, Z=26

On a affaire à un code de substitution mono-alphabétique à clef secrète.

Pendant la guerre des Gaules, Jules César avait utilisé le code de substitution suivant:

lettre codée= lettre claire décalée de 3

Mathématiquement, ceci s'écrit:

lettre codée= lettre claire+3 modulo 26

Le message en clair

RENDEZ VOUS DEMAIN MIDI VILLETANEUSE

devient

UHQGHC YRXV GHPDLQ PLGL YLOOHWDQHXVH

34

Chiffrement de César de décalage k

On peut considérer toute la famille des codes:

lettre codée=lettre claire + k modulo 26

où k est un entier entre 0 et 25 appelé la clef du code (le décalage)

Le chiffrement de César est simplement une addition dans Z/26Z.

La ***fonction de chiffrement de César de décalage*** *k* est donnée par:

$$C_k : \begin{cases} \mathbb{Z}/26\mathbb{Z} & \longrightarrow & \mathbb{Z}/26\mathbb{Z} \\ x & \longmapsto & x+k \end{cases}$$

Par exemple, pour $k = 3$: $C3(0) = 3$, $C3(1) = 4$. . .

35

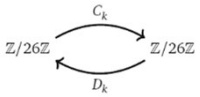
Déchiffrement de César de décalage k

Pour déchiffrer, Il suffit d'aller dans l'autre sens, c'est-à-dire de soustraire.

lettre claire=lettre codée -k mod 26

La ***fonction de déchiffrement de César de décalage*** *k* est:

$$D_k : \begin{cases} \mathbb{Z}/26\mathbb{Z} & \longrightarrow & \mathbb{Z}/26\mathbb{Z} \\ x & \longmapsto & x-k \end{cases}$$



D_k est la bijection réciproque de C_k, ce qui implique que pour tout $x \in \mathbb{Z}/26\mathbb{Z}$:

$$D_k(C_k(x)) = x$$

On remarquer que $D_k(x) = C_{-k}(x)$.

36

Exercice

Avec le code de César de décalage 8, chiffrer le mot « **SOS** ».

Indication:

Utiliser sous Excel la fonction MOD:

MOD(x;y) renvoie le reste de la division de x par y.

37

Cas particulier: Rot 13

Un exemple classique est le "rot13" (pour rotation par un décalage de 13) :

$C_{13}(x) = x + 13$

et comme -13 ≡ 13 (mod 26) alors $D_{13}(x) = x + 13$.

La fonction de déchiffrement est la même que la fonction de chiffrement !

38

Cryptanalyse du code de César

Le décalage *k* s'appelle la ***clé de chiffrement***, c'est l'information nécessaire pour crypter le message. Il y a donc 26 clés différentes et l'***espace des clés*** est Z/26Z.

Il y a donc 26 possibilités de chiffrement par la méthode de César.

Il est clair que ce chiffrement de César est d'une **sécurité très faible**.
Si Linda envoie un message secret à Sara et que Farid intercepte ce message, il sera facile pour lui de le décrypter même s'il ne connaît pas la clé secrète *k*.
L'attaque la plus simple pour Farid est de tester ce que donne chacune des 26 combinaisons possibles et de reconnaître parmi ces combinaisons laquelle donne un message compréhensible.

39

Autre code mono-alphabétique plus sécurisé

Pour mieux sécuriser le code de César, on associe maintenant à chaque lettre une autre lettre (sans ordre fixe ou règle générale). Par exemple :

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

Pour crypter le message

ETRE OU NE PAS ETRE TELLE EST LA QUESTION

on regarde la correspondance et on remplace la lettre **E** par la lettre **X**, puis la lettre **T** par la lettre **G**,..

Le message crypté est alors :

XGKX DR SX OFV XGKX GXWWX XVG WF ZRXVGPDS

40

Espace des clés

Mathématiquement, Il y a 26! Clés possibles. Ce qui fait environ 4 x 10^{26} clés.

Il y a plus de clés différentes que de grains de sable sur Terre !

Si un ordinateur pouvait tester 1 000 000 de clés par seconde, il lui faudrait alors 12 millions d'années pour tout énumérer.

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

41

Cryptanalyse d'un chiffrement par substitution mono-alphabétique : Technique d'analyse fréquentielle (Attaque statistique)

La principale faiblesse du chiffrement mono-alphabétique est qu'une même lettre est toujours chiffrée de la même façon.

Une technique de cryptanalyse permettant d'attaquer un chiffrement par substitution *mono-alphabétique* repose sur l'analyse des fréquences des symboles utilisés dans le texte chiffré. On utilise le fait que, dans chaque langue, certains symboles ou combinaisons de symboles apparaissent plus fréquemment que d'autres.

Si le message chiffré est suffisamment long, la recherche d'un symbole ayant une fréquence élevée permettra parfois de retrouver tout ou partie du message clair associé.

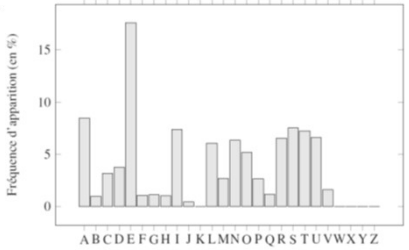
En français, les lettres les plus rencontrées sont dans l'ordre :

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

42

fréquences d'apparition des lettres en Français

Pour un texte rédigé en français, nous obtenons généralement les fréquences d'apparition (en pourcentage) proches des valeurs suivantes:



E	S	A	I	N	T	R	U	L	O	D
14.69%	8.01%	7.54%	7.18%	6.89%	6.88%	6.49%	6.12%	5.63%	5.29%	3.66%

43

Exercice

Déchiffrer la phrase suivante chiffrée par substitution mono-alphabétique:

LHLZ HFQ BC HFFPZ WH YOUPFH MUPZH

44

Chiffrement par substitution mono-alphabétique

Avantage :

- L'espace des clés est gigantesque et il n'est plus question d'énumérer toutes les possibilités.

Inconvénients :

- la clé à retenir est beaucoup plus longue, puisqu'il faut partager la clé constituée des 26 lettres
- Le fait qu'une lettre soit toujours cryptée de la même façon représente une trop grande faiblesse. Ce protocole de chiffrement est assez simple à « craquer » par une attaque statistique. Le chiffrement polyalphabétique (par exemple Vigenère) remédie à ce problème.

45

Substitution mono-alphabétique
Code affine

Code affine (extension du code de César)

Le chiffrement affine est un système de chiffrement par substitution mono-alphabétique plus général que celui de César.

La clé consiste en un couple d'entiers $(a, b) \in (Z/26Z) \times (Z/26Z)$, avec a inversible dans Z/26Z.

Un code affine sur cet alphabet est un code dont la fonction de codage est

$$C: \mathbb{Z}/26\mathbb{Z} \to \mathbb{Z}/26\mathbb{Z}$$

$$x \mapsto ax + b$$

Puisque a est inversible dans (Z/26Z), cette transformation est bien une permutation (bijection) de (Z/26Z).

47

Exercice

On considère le code affine dans Z/26Z avec a = 7, b = 5.

1) Montrer que 7 est inversible dans Z/26Z.

(Indication: 26x3 – 11x7 = 1)

2) Déduire que ce code affine est valide.

3) Codez la phrase suivante :

Hakuna matata

N.B. Utiliser la fonction MOD sous Excel pour calculer le modulo dans Z/26Z (le reste de la division par 26)

48

Substitution poly-alphabétique
Code de Vigenère

Faiblesse des codes mono-alphabétiques

La faiblesse du code de César et généralement des systèmes mono-alphabétiques est le fait qu'une lettre soit toujours cryptée de la même façon. La fréquence des lettres est donc conservée ce qui permet une cryptanalyse aisée par analyse de fréquences.

Pour améliorer la sécurité on peut faire un code de César par blocs dans lequel on change de substitution pour chaque lettre d'un bloc. On obtient ainsi le code de Vigénère, mis au point par Leon Batista Alberti au 15ème siècle et développé par Blaise de Vigénère.

Blaise de Vigenère.

50

Code de Vigénère: Exemple

On regroupe les lettres de notre texte par blocs, par exemple ici par blocs de longueur 4 :

CETTE PHRASE NE VEUT RIEN DIRE

Devient **CETT EPHR ASEN EVEU TRIE NDIR E**

si on choisit comme clé (3, 1, 5, 2) alors pour le premier bloc "**CETT**" :

- un décalage de 3 pour **C** donne **F**
- un décalage de 1 pour **E** donne **F**,
- un décalage de 5 pour le premier **T** donne **Y**
- un décalage de 2 pour le deuxième **T** donne **V**.

Ainsi "**CETT**" de vient "**FFYV**". On continue ensuite avec le deuxième bloc, ... etc

Remarque: Les deux lettres **T** ne sont pas cryptées par la même lettre.

51

Code de Vigénère: Méthode

- On se fixe une longueur de bloc k, et on découpe le message en blocs de k lettres.
- On choisit une clé constituée de *k* nombres de 0 à 25 : (*n*1, *n*2, . . . , *nk*).

Le chiffrement consiste à effectuer un chiffrement de César, dont le décalage dépend du rang de la lettre dans le bloc :

- un décalage de *n*1 pour la première lettre de chaque bloc,
- un décalage de *n*2 pour la deuxième lettre de chaque bloc,
- ...
- un décalage de *nk* pour la *k*-ème et dernière lettre de chaque bloc.

52

Code de Vigénère: fonction de chiffrement

La fonction de chiffrement associe à un bloc de longueur *k*, un autre bloc de longueur *k*, ce qui donne :

$$C_{n_1,n_2,\ldots,n_k} : \begin{cases} \mathbb{Z}/26\mathbb{Z} \times \mathbb{Z}/26\mathbb{Z} \times \cdots \times \mathbb{Z}/26\mathbb{Z} & \longrightarrow & \mathbb{Z}/26\mathbb{Z} \times \mathbb{Z}/26\mathbb{Z} \times \cdots \times \mathbb{Z}/26\mathbb{Z} \\ (x_1, x_2, \ldots, x_k) & \longmapsto & (x_1 + n_1, x_2 + n_2, \ldots, x_k + n_k) \end{cases}$$

Chacune des composantes de cette fonction est un chiffrement de César.

La fonction de déchiffrement est juste:

$$C_{-n_1,-n_2,\ldots,-n_k}.$$

53

Cryptanalyse du code de Vigénère

Le chiffre de Vigenère restera inviolable pendant plusieurs siècles.

Charles Babbage effectua une véritable cryptanalyse du chiffre de Vigenère vers 1854.

54

Exercice 1: Chiffrement

Avec le code de Vigénère, chiffrer le texte « SECRET » avec la clef « TOP ».

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Exercice 2: Déchiffrement

Déchiffrez **à la main** le texte suivant avec le chiffre de Vigenère en utilisant le mot-clef «BIEN » (équivalent numérique 1 8 4 13):

CZEIP

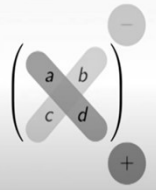
55

Rappel: Déterminant & Inverse d'une matrice

$\mathbb{K} = \mathbb{R}$ ou $\mathbb{K} = \mathbb{C}$

Matrice 2×2

$$\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc$$



58

Matrice 3×3

- Soit $A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$
- $\det A = a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{31}a_{22}a_{13} - a_{32}a_{23}a_{11} - a_{33}a_{21}a_{12}$
- La *règle de Sarrus*

59

Exemple

- Calculons le déterminant de $A = \begin{pmatrix} 2 & 1 & 0 \\ 1 & -1 & 3 \\ 3 & 2 & 1 \end{pmatrix}$
- Par la règle de Sarrus :

$$\begin{aligned} \det A &= 2 \times (-1) \times 1 + 1 \times 3 \times 3 + 0 \times 1 \times 2 \\ &\quad - 3 \times (-1) \times 0 - 2 \times 3 \times 2 - 1 \times 1 \times 1 \\ &= -6 \end{aligned}$$

60

Définition

Soit $A = (a_{ij}) \in M_n(\mathbb{K})$ une matrice carrée

- A_{ij} est la matrice extraite obtenue en effaçant la ligne i et la colonne j de A
- Le nombre $\det A_{ij}$ est un *mineur d'ordre* $n-1$ de la matrice A
- Le nombre $C_{ij} = (-1)^{i+j} \det A_{ij}$ est le *cofacteur* de A relatif au coefficient a_{ij}

61

- A_{ij} = matrice obtenue en effaçant la ligne i et la colonne j de A
- $C_{ij} = (-1)^{i+j} \det A_{ij}$ cofacteur de A relatif au coefficient a_{ij}
- $C_{ij} = +\det A_{ij}$ ou $C_{ij} = -\det A_{ij}$?

$$A = \begin{pmatrix} + & - & + & - & \dots \\ - & + & - & + & \dots \\ + & - & + & - & \dots \\ \vdots & \vdots & \vdots & \vdots & \end{pmatrix}$$

Le signe $(-1)^{i+j}$ peut être évalué rapidement en partant de la case a_{11} avec un signe + et en basculant au signe opposé chaque fois qu'en se déplace d'une case horizontalement ou verticalement jusqu'à la case a_{ij}.

62

Exemple

Soit $A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 2 & 1 \\ 0 & 1 & 1 \end{pmatrix}$. Calculons $A_{11}, C_{11}, A_{32}, C_{32}$

$$A_{11} = \begin{pmatrix} \mathbf{1} & \mathbf{2} & \mathbf{3} \\ \mathbf{4} & 2 & 1 \\ \mathbf{0} & 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \qquad C_{11} = (-1)^{1+1} \det A_{11} = +1$$

$$A_{32} = \begin{pmatrix} 1 & \mathbf{2} & 3 \\ 4 & \mathbf{2} & 1 \\ \mathbf{0} & \mathbf{1} & \mathbf{1} \end{pmatrix} = \begin{pmatrix} 1 & 3 \\ 4 & 1 \end{pmatrix} \qquad \begin{aligned} C_{32} &= (-1)^{3+2} \det A_{32} \\ &= (-1) \times (-11) \\ &= 11 \end{aligned}$$

63

Développement suivant une ligne ou une colonne

Théorème

Formule de développement par rapport à la ligne i

$$\det A = \sum_{j=1}^{n} (-1)^{i+j} a_{ij} \det A_{ij} = \sum_{j=1}^{n} a_{ij} C_{ij}$$

Formule de développement par rapport à la colonne j

$$\det A = \sum_{i=1}^{n} (-1)^{i+j} a_{ij} \det A_{ij} = \sum_{i=1}^{n} a_{ij} C_{ij}$$

64

Exemple

Retrouvons la règle de Sarrus en développement par rapport à la première ligne

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = a_{11}C_{11} + a_{12}C_{12} + a_{13}C_{13}$$

$$= a_{11}\begin{vmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{vmatrix} - a_{12}\begin{vmatrix} a_{21} & a_{23} \\ a_{31} & a_{33} \end{vmatrix} + a_{13}\begin{vmatrix} a_{21} & a_{22} \\ a_{31} & a_{32} \end{vmatrix}$$

$$= a_{11}(a_{22}a_{33} - a_{32}a_{23}) - a_{12}(a_{21}a_{33} - a_{31}a_{23}) + a_{13}(a_{21}a_{32} - a_{31}a_{22})$$

$$= a_{11}a_{22}a_{33} - a_{11}a_{32}a_{23} + a_{12}a_{31}a_{23} - a_{12}a_{21}a_{33} + a_{13}a_{21}a_{32} - a_{13}a_{31}a_{22}$$

65

Exemple

$$A = \begin{pmatrix} 4 & 0 & 3 & 1 \\ 4 & 2 & 1 & 0 \\ 0 & 3 & 1 & -1 \\ 1 & 0 & 2 & 3 \end{pmatrix}$$

$$\det A = 0C_{12} + 2C_{22} + 3C_{32} + 0C_{42} \quad \text{dévelop. par rapport à C2}$$

$$= +2\begin{vmatrix} 4 & 3 & 1 \\ 0 & 1 & -1 \\ 1 & 2 & 3 \end{vmatrix} - 3\begin{vmatrix} 4 & 3 & 1 \\ 4 & 1 & 0 \\ 1 & 2 & 3 \end{vmatrix} \quad \text{on développe les déterminants } 3 \times 3$$

$$= 2\left(+4\begin{vmatrix} 1 & -1 \\ 2 & 3 \end{vmatrix} - 0\begin{vmatrix} 3 & 1 \\ 2 & 3 \end{vmatrix} + 1\begin{vmatrix} 3 & 1 \\ 1 & -1 \end{vmatrix}\right) \quad \text{par rapport à C1}$$

$$-3\left(-4\begin{vmatrix} 3 & 1 \\ 2 & 3 \end{vmatrix} + 1\begin{vmatrix} 4 & 1 \\ 1 & 3 \end{vmatrix} - 0\begin{vmatrix} 4 & 3 \\ 1 & 2 \end{vmatrix}\right) \quad \text{par rapport à L2}$$

$$= 2(4 \times 5 + 1 \times (-4)) - 3(-4 \times 7 + 1 \times 11) = 83$$

66

Soit $A \in M_n(\mathbb{K})$
La *comatrice* C est la matrice des cofacteurs

$$C = (C_{ij}) = \begin{pmatrix} C_{11} & C_{12} & \cdots & C_{1n} \\ C_{21} & C_{22} & \cdots & C_{2n} \\ \vdots & \vdots & & \vdots \\ C_{n1} & C_{n2} & \cdots & C_{nn} \end{pmatrix}$$

Théorème

Soient A une matrice inversible et C sa comatrice. On a alors

$$\boxed{A^{-1} = \frac{1}{\det A} C^T}$$

67

Exemple

Soit $A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}$

- $\det A = 2 \implies A$ est inversible
- La comatrice C s'obtient en calculant 9 déterminants 2×2 (sans oublier les signes $+/-$)

$$C = \begin{pmatrix} 1 & 1 & -1 \\ -1 & 1 & 1 \\ 1 & -1 & 1 \end{pmatrix}$$

- Donc

$$A^{-1} = \frac{1}{\det A} \cdot C^T = \frac{1}{2}\begin{pmatrix} 1 & -1 & 1 \\ 1 & 1 & -1 \\ -1 & 1 & 1 \end{pmatrix}$$

68

Chiffrement de Hill

On décrit maintenant un autre système cryptographique appelé chiffrement de Hill. Ce chiffre publié en 1929 par **Lester S. Hill** (1891-1961) est poly-alphabétique.

L'idée consiste à transformer m caractères d'un bloc de texte clair en m caractères d'un bloc de texte chiffré par des combinaisons linéaires.

On prend pour clef K une matrice carrée de taille mxm.

Pour x = (x_1; … ; x_m) un bloc de texte clair en m caractères et y = C(x) = (y_1; …. ; y_m) le bloc de texte chiffré, on a :

$$\begin{pmatrix} y_1 \\ \vdots \\ y_m \end{pmatrix} = \begin{pmatrix} k_{1,1} & \cdots & k_{1,m} \\ \vdots & \cdots & \vdots \\ k_{m,1} & \cdots & k_{m,m} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix}$$

69

Cas m=2: Chiffrement

Regardons le cas le plus simple correspondant à m=2.

Chiffrement

Soit x le bloc à chiffrer, $x = (x_1, x_2)$ et y le résultat chiffré : $y = (y_1, y_2)$
On a : $y_1 = k_{1,1}\, x_1 + k_{1,2}\, x_2 \mod 26$
Et $y_2 = k_{2,1}\, x_1 + k_{2,2}\, x_2 \mod 26$
Donc :

$$\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} k_{1,1} & k_{1,2} \\ k_{2,1} & k_{2,2} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$$

La clef est donc une matrice $m \times m$ notée K, appelée matrice de chiffrement.
On a : y=K x.

70

Déchiffrement

Déchiffrement
Pour déchiffrer le code, il faut donc pouvoir calculer K^{-1} et ainsi faire $x=K^{-1}\, y$.

Ordinairement dans $\mathbb{R}$, si det K = ad-bc est non nul, alors l'inverse de la matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ est:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad-bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

Généralement pour une matrice carrée à coefficients complexes (ou réels), il est bien connu qu'une telle matrice est inversible si, et seulement si, son déterminant est non nul. Cependant ce n'est pas vrai dans Z=26/Z ni dans Z/nZ en général. Le résultat analogue est celui-ci :

71

Condition d'application du code

Une matrice K à coefficients dans Z/nZ est inversible
si, et seulement si, son déterminant est inversible modulo n,
c'est-à-dire pgcd(det K;n) = 1.

Dans notre cas, pour que la matrice K soit inversible modulo 26, on doit avoir pgcd (det K, 26)=1, c'est-à-dire que det K et 26 sont premiers entre eux (n'ont pas de diviseur commun positif autre que 1).

Autrement, il faut contrôler que (ad–bc) est impair et n'est pas multiple de 13.

72

Exemple

En utilisant une matrice *A* dont le déterminant est premier avec 26, on cherche à chiffrer le message suivant :

TEXTEACRYPTER

On prend :

$$A = \begin{pmatrix} 3 & 5 \\ 6 & 17 \end{pmatrix}$$

dont le déterminant est 21. Comme 5 × 21 = 105 ≡ 1 (mod 26), 5 est un inverse de det(*A*) modulo 26.

Chiffrement

On remplace chaque lettre par son rang. Puis on code le message :

TEXTEACHIFFRER→ 19 ; 4 ; 23 ; 19 ; 4 ; 0 ; 2 ; 7 ; 8 ; 5 ; 5 ; 17 ; 4 ; 17

On regroupe les lettres par paires créant ainsi 7 vecteurs de dimension deux, la dernière paire étant complétée arbitrairement :

$$X_1 = (19;4); X_2 = (23;19); X_3 = (4;0); X_4 = (2;7); X_5 = (8;5); X_6 = (5;17); X_7 = (4;17).$$

On multiplie ensuite ces vecteurs par la matrice *A* en travaillant sur des congruences modulo 26 :

$$Y_1 = \begin{pmatrix} 3 & 5 \\ 6 & 17 \end{pmatrix}\begin{pmatrix} 19 \\ 4 \end{pmatrix} = \begin{pmatrix} 25 \\ 0 \end{pmatrix} \text{ etc.}$$

On obtient alors 7 vecteurs, soit 14 lettres. Le premier vecteur est (25 ; 0) . Les deux premières lettres chiffrées sont donc « ZA ».

Question: Trouver le texte chiffré en entier. Comment peut-on déchiffrer ce texte?

Exercice

On cherche à chiffrer le mot « ENSA » à l'aide du chiffrement de Hill (26 caractères), et en utilisant la matrice suivante :

$$A = \begin{pmatrix} 5 & 1 \\ 4 & 3 \end{pmatrix}$$

On remplace chaque lettre par son rang à l'aide du tableau suivant :

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

1) La matrice A est-elle inversible dans Z/26Z ? Justifier votre réponse.

2) Chiffrer puis déchiffrer le mot « ENSA ».

Chiffrement à l'aide d'une matrice de codage

Exemple Considérons le message

PREPARE TO NEGOTIATE

Un type de code, qui est extrêmement difficile à déchiffrer, se sert d'une matrice de codage.

Soit par exemple la matrice de codage :

$$\begin{bmatrix} -3 & -3 & -4 \\ 0 & 1 & 1 \\ 4 & 3 & 4 \end{bmatrix}$$

Chiffrement à l'aide d'une matrice de codage

Nous assignons un nombre à chaque lettre de l'alphabet :

A = 1, B = 2, … , Z = 26

Espace entre deux mots = 27

P	R	E	P	A	R	E	*	T	O	*	N	E	G	O	T	I	A	T	E
16	18	5	16	1	18	5	27	20	15	27	14	5	7	15	20	9	1	20	5

77

Chiffrement à l'aide d'une matrice de codage

P	R	E	P	A	R	E	*	T	O	*	N	E	G	O	T	I	A	T	E
16	18	5	16	1	18	5	27	20	15	27	14	5	7	15	20	9	1	20	5

Puisque nous employons une matrice 3x3,

nous décomposons le message en une suite de vecteurs 3x1 :

$$\begin{bmatrix}16\\18\\5\end{bmatrix}\begin{bmatrix}16\\1\\18\end{bmatrix}\begin{bmatrix}5\\27\\20\end{bmatrix}\begin{bmatrix}15\\27\\14\end{bmatrix}\begin{bmatrix}5\\7\\15\end{bmatrix}\begin{bmatrix}20\\9\\1\end{bmatrix}\begin{bmatrix}20\\5\\27\end{bmatrix}$$

N.B. pour compléter le dernier vecteur, on ajoute un espace.

78

Chiffrement à l'aide d'une matrice de codage

Nous codons le message en multipliant la matrice des vecteurs par la matrice de codage.

$$\begin{bmatrix}-3 & -3 & -4\\0 & 1 & 1\\4 & 3 & 4\end{bmatrix}\begin{bmatrix}16 & 16 & 5 & 15 & 5 & 20 & 20\\18 & 1 & 27 & 27 & 7 & 9 & 5\\5 & 18 & 20 & 14 & 15 & 1 & 27\end{bmatrix}$$

$$=\begin{bmatrix}-122 & -123 & -176 & -182 & -96 & -91 & -183\\23 & 19 & 47 & 41 & 22 & 10 & 32\\138 & 139 & 181 & 197 & 101 & 111 & 203\end{bmatrix}$$

79

Chiffrement à l'aide d'une matrice de codage

Message codé

Les colonnes de cette matrice donnent le message codé :

PREPARE TO NEGOTIATE

⇩

−122, 23, 138, −123, 19, 139, −176, 47, 181,
−182, 41, 197, −96, 22, 101, −91, 10, 111,
−183 32 203.

80

Chiffrement à l'aide d'une matrice de codage

Décodage du message

Inverse de la matrice de codage

$$\begin{bmatrix} 1 & 0 & 1 \\ 4 & 4 & 3 \\ -4 & -3 & -3 \end{bmatrix}$$

Message codé sous forme d'une matrice

$$\begin{bmatrix} -122 & -123 & -176 & -182 & -96 & -91 & -183 \\ 23 & 19 & 47 & 41 & 22 & 10 & 32 \\ 138 & 139 & 181 & 197 & 101 & 111 & 203 \end{bmatrix}$$

$$= \begin{bmatrix} 16 & 16 & 5 & 15 & 5 & 20 & 20 \\ 18 & 1 & 27 & 27 & 7 & 9 & 5 \\ 5 & 18 & 20 & 14 & 15 & 1 & 27 \end{bmatrix}$$

81

Chiffrement à l'aide d'une matrice de codage

Décodage du message

Les colonnes de cette matrice, écrites en forme linéaire, donnent le message original :

16 18 5 16 1 18 5 27 20 15 27 14 5 7 15 20 9 1 20 5

⇩

P R E P A R E * T O * N E G O T I A T E

82

Exercice: Chiffrement à l'aide d'une matrice de codage

Chiffrer puis déchiffrer le message « PAS DEMAIN » à l'aide de la matrice de codage suivante:

$$B = \begin{bmatrix} 2 & 1 & 0 \\ 3 & 0 & 3 \\ 2 & 2 & 1 \end{bmatrix}$$

Nous assignons un nombre à chaque lettre de l'alphabet :

A = 1, B = 2, … , Z = 26 ; Espace entre deux mots = 27

83

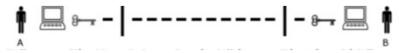
PARTIE 2 CRYPTOGRAPHIE MODERNE

Méthodes modernes de cryptographie

De nos jours, on distingue généralement deux types de chiffrements :

❖***Chiffrement symétrique (clé privée):*** La même clé doit être employée pour chiffrer et déchiffrer le message. (Exemple code DES). Expéditeur et destinataire doivent s'échanger cette clé, qui doit rester secrète sous peine qu'un tiers parvienne à déchiffrer les correspondances.

❖***Chiffrement asymétrique (clé publique): U***ne clé est utilisée pour le chiffrement et une autre pour le déchiffrement. (Exemple: code RSA)



85

Cryptographie symétrique

Chiffrement symétrique (clé privée)

La **cryptographie symétrique**, également dite **à clé privée** (par opposition à la cryptographie asymétrique) permet à la fois de chiffrer et de déchiffrer des messages à l'aide d'un même mot clé.

Expéditeur et destinataire doivent s'échanger cette clé, qui doit rester secrète sous peine qu'un tiers parvienne à déchiffrer les correspondances.

87

Types de chiffrement symétrique

il existe deux grandes catégories de chiffrements modernes. La principale différence vient du découpage des données en blocs de taille généralement fixe.

1) Le **chiffrement par flot** (ou **chiffrement de flux,** en anglais *stream cipher*) :

2) Le **chiffrement par bloc** (en anglais *block cipher*)

88

1. Chiffrement par flot

Ce chiffrement arrive à traiter les données de longueur quelconque et n'a pas besoin de les découper.

Exemples:

- A5/1, algorithme publié en 1994, utilisé dans les téléphones mobiles de type GSM,
- RC4, le plus répandu, conçu en 1987
- E0 utilisé par le protocole Bluetooth.

89

2. Chiffrement par blocs

Chaque texte clair est découpé en blocs de même longueur et chiffré bloc par bloc. La taille de bloc est comprise entre 32 et 512 bits. Les blocs sont ensuite chiffrés les uns après les autres. Dans le milieu des années 1990 le standard était de 64 bits mais depuis 2000 et le concours AES le standard est de 128 bits.

Exemples.

- **DES** (Data Encryption Standard): DES transforme un bloc de 64 bits en un autre bloc de 64 bits. Il manipule des clés individuelles de 56 bits. Ce système est basé sur le schéma de Feistel (du nom de Horst Feistel). Conçu dans les années 1970, l'emploi de DES n'est plus recommandé aujourd'hui, du fait de sa lenteur à l'exécution et de son espace de clés trop petit permettant une attaque systématique en un temps raisonnable.
- **AES** (Advanced Encryption Standard), le remplaçant de DES. Depuis 2000, il est devenu le nouveau standard de chiffrement pour les organisations du gouvernement des États-Unis. Il est actuellement le plus utilisé et le plus sûr
- **Blowfish, Serpent et Twofish**, des alternatives à AES.

90

Exemple de chiffrement symétrique

LE MASQUE JETABLE

Le masque jetable (chiffre de Vernam)

Le masque jetable, également appelé chiffre de Vernam, est un chiffrement par flot inventé par Gilbert Vernam en 1917. Ce chiffrement consiste à combiner le message en clair avec une clé présentant les caractéristiques très particulières suivantes :

- ❑ La clé doit être une suite de caractères au moins aussi longue que le message à chiffrer.
- ❑ Les caractères composant la clé doivent être choisis de façon totalement aléatoire.
- ❑ Chaque clé, ou « masque », ne doit être utilisée qu'une seule fois (d'où le nom de masque jetable).

92

Simplicité et sécurité théorique absolue

La méthode de combinaison entre le clair et la clé est suffisamment simple pour être employée « à la main » sans dispositif informatique, mécanique ou autre. Elle sera décrite ci-dessous.

L'intérêt considérable de cette méthode de chiffrement est que si les trois règles ci-dessus sont respectées strictement, le système offre une sécurité théorique absolue, comme l'a prouvé Claude Shannon en 1949.

Bien que ce chiffrement est théoriquement impossible à casser, mais il présente d'importantes difficultés de mise en œuvre qui le rendent impossible à utiliser dans de nombreux cas comme la sécurisation des échanges sur Internet.

93

1) Masque jetable : méthode à la main

Supposons que la clé aléatoire retenue, ou « masque », soit :

WMCKL

Cette clé est choisie à l'avance entre les deux personnes souhaitant communiquer. Elle n'est connue que d'eux.

94

Chiffrement

On veut chiffrer le message « HELLO ». Pour cela, on attribue un nombre (par exemple de 0 à 25) à chaque lettre. Ensuite on additionne la valeur de chaque lettre avec la valeur correspondante dans le masque (calcul modulo 26) :

7 (H) 4 (E) 11 (L) 11 (L) 14 (O) message

+ 22 (W) 12 (M) 2 (C) 10 (K) 11 (L) masque

= 29 16 13 21 25 masque + message

= 3 (D) 16 (Q) 13 (N) 21 (V) 25 (Z) masque + message modulo 26

Le texte reçu par le destinataire est « DQNVZ ».

95

Déchiffrement

Il s'effectue de manière similaire, sauf que l'on soustrait le masque au texte chiffré au lieu de l'additionner. Ici encore on ajoute éventuellement 26 au résultat pour obtenir des nombres compris entre 0 et 25 :

3 (D) 16 (Q) 13 (N) 21 (V) 25 (Z) message chiffré

- 22 (W) 12 (M) 2 (C) 10 (K) 11 (L) masque

= -19 4 11 11 14 message chiffré - masque

= 7 (H) 4 (E) 11 (L) 11 (L) 14 (O) message chiffré - masque modulo 26

On retrouve bien le message initial « HELLO ».

96

Un chiffrement à la main par la méthode du masque jetable fut utilisé par Che Guevara pour communiquer avec Fidel Castro.

97

2. Masque jetable : Méthode informatisée

Lorsque les données sont informatisées, donc mises sous forme binaire, le message en clair, à chiffrer, se présente comme une suite de bits. La clé est une autre suite de bits, de même longueur.

On traite un à un les bits du clair, en combinant chacun avec le bit de même rang dans la clé.

Appelons *A* un bit du clair et *B* le bit de même rang de la clé. Le chiffrement consiste à calculer un bit C en effectuant sur A et B la fonction OU exclusif, notée XOR (eXclusive OR). Celle-ci est définie par le tableau suivant, qui indique pour toutes les valeurs possibles de A et B la valeur du résultat, que l'on note A ⊕ B :

A	B	C = A ⊕ B
0	0	0
0	1	1
1	0	1
1	1	0

98

Chiffrement et déchiffrement

Chiffrement: Pour chiffrer on calcule donc $C = A \oplus B$. Le résultat *C* est le chiffré de *A*. L'opération est effectuée pour chaque bit du clair avec le bit correspondant de la clé.

Le **déchiffrement** s'effectue en combinant le chiffré *C* avec le bit de clé *B* par la simple opération : $C \oplus B$. Il se trouve qu'elle fait retrouver le clair *A*, comme nous allons le montrer.

Remarquons que l'opération XOR possède les deux propriétés suivantes, faciles à vérifier :

$A \oplus A = 0$; $A \oplus 0 = A$

Le calcul de déchiffrement peut donc s'écrire :

$C \oplus B = (A \oplus B) \oplus B = A \oplus (B \oplus B) = A \oplus 0 = A$

Il fait bien retrouver le bit de clair *A*. L'application de l'opération XOR étant simple en informatique, ces traitements peuvent s'effectuer à très grande vitesse.

99

Exemple

Voici un exemple numérique de la méthode précédente :

A = 0110101011010100 (message en clair)

B = 0101011011100110 (la clé ; à garder secrète bien évidemment)

Donc: A ⊕ B = C. Le "C" représente le message chiffré:

Chiffrement : $C = A \oplus B$ = 0011110000110010 (message chiffré)

Déchiffrement : $A = C \oplus B$ = 0110101011010100 (message déchiffré)

100

Applications

Ce système de chiffrement a été utilisé pour le téléphone rouge, en fait un télex, reliant directement le Kremlin à la Maison-Blanche, les clés transitant alors par valises diplomatiques.

La totalité des chiffreurs symétriques utilise l'opérateur XOR.

Le nouvel algorithme de cryptographie haute sécurité AES en particulier, en utilise un très grand nombre.

101

Inconvénients du masque jetable

Difficulté de produire une clé parfaitement aléatoire : Des clés parfaitement aléatoires ne peuvent pas être produites par un ordinateur par un simple calcul : en effet ce calcul est déterministe, dont le résultat est totalement prévisible quand on connaît l'algorithme et les données initiales.

Problème de l'utilisation unique de chaque clé : Le risque que fait courir la réutilisation d'une clé est facile à montrer.

Soit un message M_1 masqué grâce à la clé K, nous obtenons le chiffré C_1. Supposons qu'un autre message M_2 soit chiffré avec le même masque K, fournissant le chiffré C_2. Nous avons :

$$C_1 = M_1 \oplus K \qquad C_2 = M_2 \oplus K$$

C'est dangereux, car tout effet de masque de la clé K a disparu. Si par exemple un adversaire connaît les deux messages chiffrés et l'un des messages en clair, il peut trouver instantanément le deuxième message en clair par le calcul :

$$C_1 \oplus C_2 \oplus M_1 = M_2$$

102

Exercices

Exercice 1.

Avec le code de Vernam, déchiffrer le mot « SSXHMAZCUA » en utilisant la clé "SHRTVSGVIW".

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

103

Exercices

Exercice 2.

Chiffrer le message « SOS » par la méthode du masque jetable, en passant par le code binaire (Voir ci-dessous le tableau ASCII) et en faisant appel à l'opérateur XOR. Prendre pour clé « YEN ».

Comment on retrouve le texte en clair ? Justifier votre réponse.

Déchiffrer le message.

ASCII Code: Character to Binary

Character	Binary Code	Character	Binary Code	Character	Binary Code	Character	Binary Code	Character	Binary Code
A	01000001	Q	01010001	g	01100111	w	01110111	-	00101101
B	01000010	R	01010010	h	01101000	x	01111000	.	00101110
C	01000011	S	01010011	i	01101001	y	01111001	/	00101111
D	01000100	T	01010100	j	01101010	z	01111010	0	00110000
E	01000101	U	01010101	k	01101011	!	00100001	1	00110001
F	01000110	V	01010110	l	01101100	"	00100010	2	00110010
G	01000111	W	01010111	m	01101101	#	00100011	3	00110011
H	01001000	X	01011000	n	01101110	$	00100100	4	00110100
I	01001001	Y	01011001	o	01101111	%	00100101	5	00110101
J	01001010	Z	01011010	p	01110000	&	00100110	6	00110110
K	01001011	a	01100001	q	01110001	'	00100111	7	00110111
L	01001100	b	01100010	r	01110010	(	00101000	8	00111000
M	01001101	c	01100011	s	01110011	)	00101001	9	00111001
N	01001110	d	01100100	t	01110100	*	00101010	:	00111111
O	01001111	e	01100101	u	01110101	+	00101011	@	01000000
P	01010000	f	01100110	v	01110110	,	00101100	_	01011111

104

Cryptographie symétrique
DES & AES

DES (Data Encryption Standard) - 1976

DES est un chiffrement symétrique développé dans les années 70 par IBM. La méthode DES fut adoptée et rendue standard par le gouvernement des Etats Unis. Elle utilise des clés d'une taille de 56 bits ce qui la rend de nos jours facile à casser avec les nouvelles technologies de cryptanalyse.

Principe de l'algorithme

L'algorithme utilise une clé de 56 bits. Le nombre de clés est:

2^56=72.057.595.037.927.936

Le texte en clair est découpé en bloc de 64 bits qui seront chiffrés un par un.

L'algorithme est basé sur des opérations faciles (en tout 19 étapes) à réaliser par un processeur. :

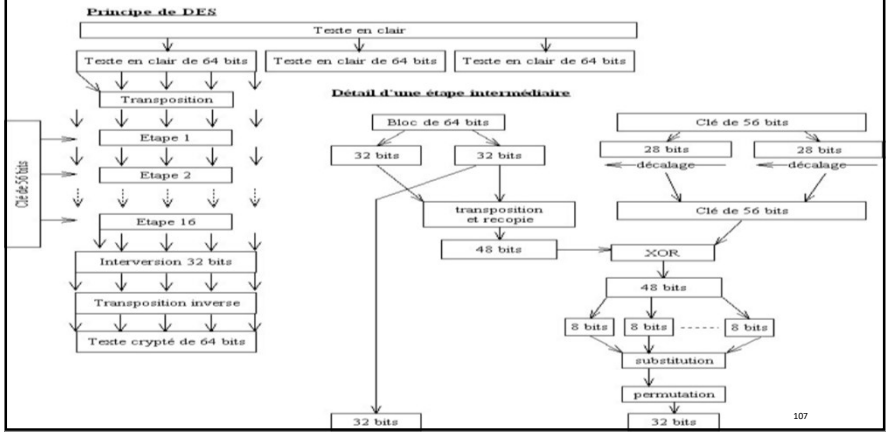
— Décalage ;

— « ou exclusif » ;

— Transposition/recopie

106

DES: Principe de fonctionnement



107

AES (Advanced Encryption Standard) - 1997

L'AES est un standard de cryptage symétrique destiné à remplacer le DES qui est devenu trop faible au regard des attaques. DES a été remplacé en 2001 par l'AES.

Appelé également **Rijndael** au nom de ses deux concepteurs belges Joan Daemen et Vincent Rijmen, AES devint le nouveau standard de chiffrement pour les organisations du gouvernement des États-Unis. Il est actuellement le code symétrique le plus utilisé et le plus sûr.

L'AES

— est un standard, libre d'utilisation, sans restriction d'usage ni brevet ;

— est un algorithme de chiffrement par blocs (comme le DES) ;

108

AES: cryptanalyse

AES a été conçu de façon à résister aux méthodes classiques d'attaque.

L'AES n'a pour l'instant pas été cassé, même théoriquement, au sens où il n'existe pas d'attaque significativement plus efficace que l'attaque par force brute (tester, une à une, toutes les combinaisons possibles).

109

Cryptographie asymétrique (à clé publique)

Cryptographie à clé publique
Chiffrement RSA

Code RSA
Rappels en arithmétique

Algorithme d'Euclide

Soient $a \in Z$ et $b \in N^*$. Il existe un unique couple $(q,r) \in Z^2$ tels que:

$$a=bq+r \quad \text{et} \quad 0 \leq r < b.$$

De plus on sait que : $a \wedge b = b \wedge r$.

On en déduit l'algorithme suivant pour calculer le pgcd pour $a \geq b \geq 0$:

On pose $r_0=a$ et $r_1=b$.

Pour $i \in N^*$: si $r_i=0$, on pose $r_{i+1}=0$

si $r_i \neq 0$, on note r_{i+1} le reste de la division euclidienne de r_{i-1} par r_i.

Le dernier reste non nul est le pgcd de a et b.

113

Exemple

Calculons le pgcd de a = 600 et b = 124.

$$\begin{aligned} 600 &= 124 \times 4 + 104 \\ 124 &= 104 \times 1 + 20 \\ 104 &= 20 \times 5 + 4 \\ 20 &= 4 \times 5 + 0 \end{aligned}$$

Ainsi pgcd(600, 12

114

Exercice

Calculer Pgcd(25872;484)

115

Nombres premiers entre eux

On dit que deux entiers relatifs

sont premiers entre eux

si leur pgcd vaut 1.

Exemple

6 et 35 sont premiers entre eux.

116

Théorème de Bézout.

Soient a, b des entiers relatifs.

Alors il existe deux entiers u, v ∈ Z tels que

au + bv = pgcd(a, b).

117

Remarques

Si on trouve deux entiers *u'*, *v'* tels que *au'* + *bv'* = *d*, cela n'implique pas que *d* = pgcd(*a*, *b*).

Par exemple *a* = 12, *b* = 8 ; 12 x 1 + 8 x 3 = 36 mais pgcd(*a*, *b*) = 4.

Les entiers u, v sont des coefficients de Bézout. Ils ne sont pas uniques. Ils s'obtiennent en « remontant » l'algorithme d'Euclide.

118

Exemple

Calculons les coefficients de Bézout pour *a* = 600 et *b* = 124. La partie gauche est l'algorithme d'Euclide. La partie droite s'obtient de *bas en haut*.

$$
\begin{aligned}
600 &= 124 \times 4 + 104 & 4 &= \begin{bmatrix} 600 \times 6 + 124 \times (-29) \\ 124 \times (-5) + (600 - 124 \times 4) \times 6 \end{bmatrix} \\
124 &= 104 \times 1 + 20 & 4 &= \begin{bmatrix} 124 \times (-5) + 104 \times 6 \\ 104 - (124 - 104 \times 1) \times 5 \end{bmatrix} \\
104 &= 20 \times 5 + 4 & 4 &= \begin{bmatrix} 104 - 20 \times 5 \end{bmatrix} \\
20 &= 4 \times 5 + 0
\end{aligned}
$$

Ainsi pour *u* = 6 et *v* = -29 alors 600 x 6 + 124 x(-29) = 4.

119

Exercice

Calculer les coefficients de Bézout de 50 et 17.

120

Inverse modulaire

Dans Z/nZ, Une classe $\overline{x}$ est inversible s'il existe $\overline{y}$ tel que

$$\overline{x}.\overline{y} = \overline{1}.$$

Dans ce cas $\overline{y}$ est appelé l'inverse de $\overline{x}$

(y est dit inverse de x modulo n).
Cet inverse $\overline{y}$ est unique. On le note $\overline{x}^{-1}$.

$$\overline{x}.\overline{y} = \overline{1} \Leftrightarrow xy \equiv 1[n] \Leftrightarrow \exists v \in \mathbb{Z} \quad xy + nv = 1$$

121

Propriétés

$\overline{x}$ est inversible dans Z/nZ ⟺ pgcd(*x; n*) = 1.

Si n est premier, alors tout élément non nul de Z/nZ est inversible. (Z/nZ est dit un corps)

Si $\overline{x}$ n'est pas inversible dans Z/nZ, alors il existe $\overline{y}$ tel que $\overline{x}.\overline{y} = \overline{0}$. $\overline{x}$ est dit diviseur de zéro.
Ainsi tout élément de Z/nZ est soit inversible soit diviseur de zéro.

122

Théorème de Bézout (cas des entiers premiers entre eux)

Soient $(a,b) \in \mathbb{Z}^2$. On a:

$a \wedge b = 1 \Leftrightarrow \exists (u,v) \in \mathbb{Z}^2$, $au+bv=1$.

123

Méthode pratique pour trouver l'inverse modulo n

Si xy + nv = 1 alors y est un inverse de x modulo n.

En d'autres termes, trouver un inverse de x modulo n revient à calculer les coefficients de Bézout associés à la paire (x, n).

124

Exemple

Cherchons l'inverse de 17 modulo 50.

Pgcd(17;50) = 1, de plus le calcul des coefficients de Bézout donne:

1 = 17x3 + 50x(-1)

Donc 17x3 ≡ 1 [50], d'où l'inverse de 17 modulo 50 est 3.

125

Exercice 1. (Algorithme d'Euclide étendu)

1) A l'aide de l'algorithme d'Euclide, calculer le PGCD de 120 et 23.

2) Avec l'algorithme d'Euclide étendu, déduire les coefficients de Bézout (deux entiers u et v tels que $120u + 23v = \text{PGCD}(120, 23)$)

3) Déduire l'inverse de 23 modulo 120.

126

Nombres premiers

Un entier p≥2 est dit premier

si ses seuls diviseurs positifs sont 1 et p.

127

Propriétés

Tout entier n > 2 admet un diviseur qui est un nombre premier.

L'ensemble des nombres premiers est infini.

Deux nombres premiers différents sont premiers entre eux.

Soient a,b∈Z et p premier. Si p/ab alors p/a ou p/b.

128

Décomposition en facteurs premiers

Tout entier $n \geq 2$ s'écrit de manière unique

$$n = {p_1}^{\alpha_1} \dots \dots {p_r}^{\alpha_r}$$

où $p_1 < p_2 < \cdots < p_r$ sont des nombres premiers et $\alpha_1, \dots, \alpha_k$ sont dans N^*.

On dit que $n = {p_1}^{\alpha_1} \dots \dots {p_r}^{\alpha_r}$ est la décomposition en produit de facteurs premiers de *n*.

Exemple : $24 = 2^3 \times 3$

129

Remarque

La principale raison pour laquelle on choisit de dire que 1 n'est pas un nombre premier, c'est que sinon il n'y aurait plus unicité de la décomposition :

$24 = 2^3 \times 3 = 1 \times 2^3 \times 3 = 1^2 \times 2^3 \times 3 = \dots\dots$

130

Exponentielle modulaire

Exponentielle modulaire

Le calcul naïf de l'exponentielle modulaire $b^e \bmod n$ est le suivant :

on multiplie ***e*** fois le nombre *b* par lui-même, et une fois l'entier b^e obtenu, on calcule son reste modulo *m via* l'algorithme de division euclidienne.

Cependant cette méthode n'est pas pratique pour les grands nombres. L'exponentielle modulaire rapide réduit drastiquement à la fois le nombre d'opérations et la place en mémoire nécessaires à l'exécution de l'exponentiation modulaire.

132

Exponentielle modulaire rapide

Tout d'abord il faut convertir l'exposant *e* en notation binaire, c'est-à-dire qu'on écrit :

$$e = \sum_{i=0}^{n-1} a_i 2^i.$$

Dans cette notation, la *longueur* de *e* est de *n* bits. a_i peut prendre la valeur 0 ou 1 pour tout *i* tel que $0 \leq i < n - 1$. Par définition, $a_{n-1} = 1$.

La valeur b^e peut alors être écrite :

$$b^e = b^{\left(\sum_{i=0}^{n-1} a_i 2^i\right)} = \prod_{i=0}^{n-1} \left(b^{2^i}\right)^{a_i}.$$

133

Rappel: convertir du décimal au binaire

Un nombre décimal $\overline{a_n a_{n-1} \ldots a_2 a_1 a_0}^{10}$ s'écrit sous la forme $\sum_{k=0}^{n} a_k 10^k$.

Un nombre binaire $\overline{a_n a_{n-1} \ldots a_2 a_1 a_0}^{2}$ s'écrit sous la forme $\sum_{k=0}^{n} a_k 2^k$.

Pour convertir un nombre décimal en binaire, il faut donc le décomposer en puissances de 2.

134

Exemple: convertir du décimal au binaire

Par exemple, pour convertir le nombre décimal 324 :

$$\begin{aligned}
324 &= 2 \times 162 + \mathbf{0} \\
162 &= 2 \times 81 + \mathbf{0} \\
81 &= 2 \times 40 + \mathbf{1} \\
40 &= 2 \times 20 + \mathbf{0} \\
20 &= 2 \times 10 + \mathbf{0} \\
10 &= 2 \times 5 + \mathbf{0} \\
5 &= 2 \times 2 + \mathbf{1} \\
2 &= 2 \times 1 + \mathbf{0} \\
1 &= 2 \times 0 + \mathbf{1}
\end{aligned}$$

Donc 324 est 101000100 en binaire.

Vérification : $2^2+2^6+2^8=324$.

135

Exercice. (Exponentiation modulaire)

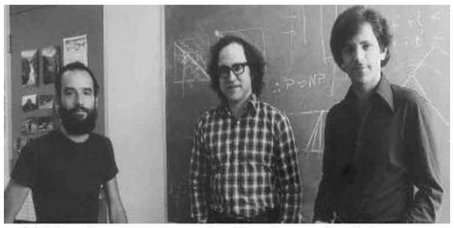
Calculer $51447^{21} \bmod 17$

Calculer $156^{17} \bmod 437$

136

RSA (1977)

Le chiffrement RSA, nommé par les initiales de ses trois inventeurs Ronald Rivest, Adi Shamir et Leonard Adleman, est un algorithme de cryptographie asymétrique (système à clé publique), qui a été décrit en 1977.



Adi Shamir Ron Rivest Len Adleman

137

RSA : le Chiffrement le plus populaire dans le monde

RSA est devenu un système universel servant dans une multitude d'applications : systèmes d'exploitation (Microsoft, Apple,…), cartes à puces bancaires et bien sûr le réseau Internet pour assurer la confidentialité du courrier électronique. Il est partout !

138

L'idée de génie (RSA)

Facile

$n = p \times q$

Difficile

p , q: nombres premiers ayant un nombre de chiffres >300

139

Principe de fonctionnement du RSA

Le système RSA est un système à clé publique, ce qui signifie que :

- ~~l'algorithme de calcul n'est pas caché, ni la clé de codage (dite clé publique) ;~~
- la connaissance de la clé publique du destinataire permet à tous les émetteurs de crypter le messages qui ne pourra être décrypté que par le destinataire, grâce à sa clé secrète.

Un système à clé publique est fondé sur l'existence de **fonctions à sens unique**. Il est simple d'appliquer cette fonction à un message, mais extrêmement difficile de retrouver ce message à partir du moment où on l'a transformé.

140

Avantage du système à clé publique

Ce type de systèmes possédant une clé de décodage différente de la clé de codage (système dissymétrique) présente un avantage sur les systèmes classiques (dits symétriques, la même clé servant à la fois pour le codage et le décodage) car les deux interlocuteurs n'ont pas besoin de se rencontrer pour convenir d'une clé secrète et encore moins de prendre le risque de la faire circuler. Seule la clé publique, insuffisante pour le décryptage, est connue préalablement aux échanges cryptés.

141

LE THÉORÈME RSA

Soient p et q deux nombres premiers et n=pq.

Soit e un entier premier avec $\phi(n) = (p-1)(q-1)$

($\phi(n)$ l'indicatrice d'Euler en n).

Alors il existe un entier naturel d tel que

$ed=1 \bmod \phi(n)$ et pour tout entier M:

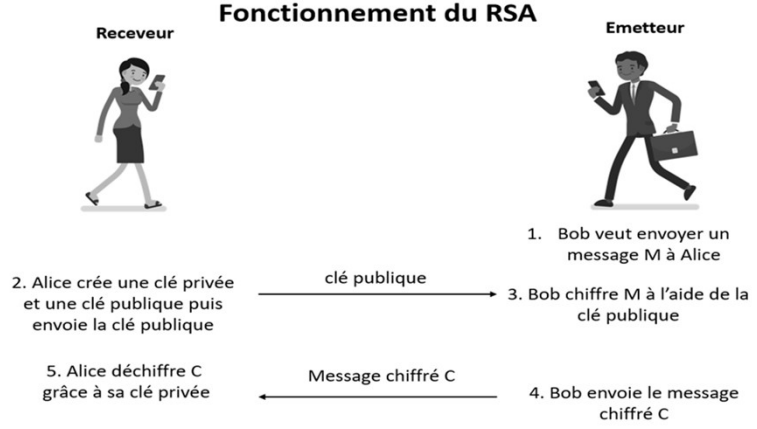
$M = M^{ed} \bmod (n)$

Ingrédients de la preuve (mathématiques du 18ème siècle):

Petit théorème de Fermat, Formule d'Euler, théorème de Bézout

142

Fonctionnement du RSA



143

Algorithme RSA: Création des clés

1) Choisir p et q, deux nombres premiers et calculer leur produit $n = pq$;

2) Calculer $\phi(n) = (p - 1)(q - 1)$; (c'est la valeur de l'indicatrice d'Euler en n) ;

3) Choisir un entier naturel e premier avec $\phi(n)$ et strictement inférieur à $\phi(n)$, appelé *exposant de chiffrement* ;

4) Calculer l'entier naturel d, inverse de e modulo $\phi(n)$ appelé *exposant de déchiffrement* (algorithme d'Euclide étendu).

144

Clés

Comme *e* est premier avec ϕ(*n*), d'après le théorème de Bézout il existe deux entiers *d* et *k* tels que

$$ed + k\phi(n) = 1,$$

c'est-à-dire que $ed \equiv 1 \pmod{\phi(n)}$: *e* est bien inversible modulo ϕ(*n*).

Le couple (*n*,*e*) est la ***clé publique*** du chiffrement, alors que le nombre *d* est sa ***clé privée***.

145

Algorithme RSA: Ciffrement et déchiffrement

Chiffrement:

Si M est un entier naturel représentant un message, alors le message chiffré sera représenté par l'entier naturel C:

$$C \equiv M^e \pmod{n},$$

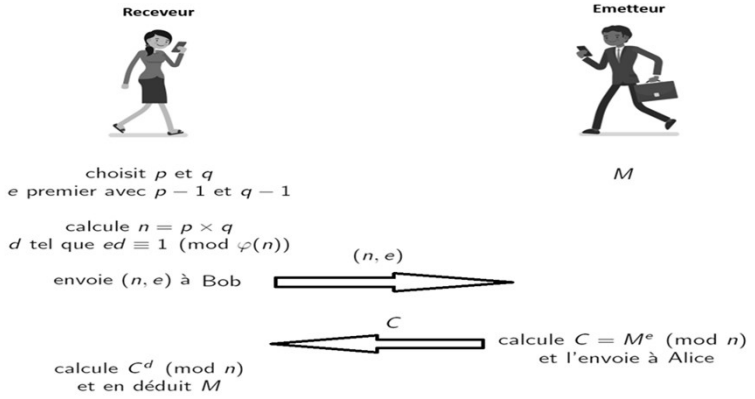
Déchiffrement:

Pour déchiffrer C, on utilise d et l'on retrouve le message clair M par :

$$M \equiv C^d \pmod{n}.$$

Technique utilisée: exponentiation modulaire

146



Connaitre p & q → connaitre $\varphi(n)$→ connaitre d → connaitre M

147

Exemple simple (petits nombres premiers)

On choisit deux nombres premiers *p* = 3, *q* = 11 ;

Leur produit *n* = 3 × 11 = 33 ;

ϕ(*n*) = (3 – 1) × (11 – 1) = 2 × 10 = 20 ;

on choisit *e*= 3 (premier avec 20) ;

L'inverse de 3 modulo 20 est d=7 (algorithme d'Euclide étendu).

Chiffrement de *M* = 4 : $C = M^e \bmod n = 4^3 \equiv 31 \bmod 33$

Déchiffrement de *C* : $M = C^d \bmod n = 31^7 \equiv 4 \bmod 33$, (on retrouve le message initial *M* = 4).

148

Alternative quantique ?

- Peter Shor (1994): Avec un ordinateur quantique on peut factoriser efficacement des entiers (réponse en temps polynomial).
- Des experts en sécurité estimaient plusieurs dizaines d'années nécessaires à un ordinateur quantique pour casser un chiffrement RSA de 2048 bits, et ont développé des chiffrements que même un ordinateur quantique ne sera pas capable de cracker.

149

TD - Chiffrement RSA

Exercice 1. (Algorithme d'Euclide étendu)

1) A l'aide de l'algorithme d'Euclide, calculer le PGCD de 120 et 23.

2) Avec l'algorithme d'Euclide étendu, déduire les coefficients de Bézout (deux entiers u et v tels que $120u + 23v = \text{PGCD}(120, 23)$)

3) Déduire l'inverse de 23 modulo 120.

Exercice2. (Exponentiation modulaire)

1) Calculer $156^{17} \mod 437$

2) Calculer $51447^{21} \mod 17$

150

Exercice 3. Pour p = 19 et q = 23, trouver parmi les exposants de chiffrement suivants ceux qui sont valides : e = 9; e = 14 et e = 17. Pour ces exposants valides, déterminer les exposants de déchiffrement.

Exercice 4.

1) Prenons p = 29; q = 31 et e = 13: Utiliser le protocole RSA pour chiffrer et déchiffrer M = 123.

2) Même question pour p = 47; q = 59 et e = 17.

151

L'algorithme d'échange de clés Diffie-Hellman

Codes à clefs publiques et difficulté calculatoire

Diffie et Hellman ont dégagé vers 1976 la notion de code à clef publique fondé sur la difficulté calculatoire (fonction à sens unique).

Les autres codes asymétriques les plus utilisés :

- **RSA** basé sur la difficulté calculatoire de la factorisation des grands entiers.
- **El Gamal** basé sur la difficulté calculatoire de calculer le logarithme discret dans un corps fini.
- **Menezes-Vanstonne** basé sur le logarithme associé au groupe des points d'une courbe elliptique sur un corps fini. C'est une modification d'autres cryptosystèmes, comme El Gamal.

153

L'algorithme Diffie-Hellman - 1976

Parallèlement à leur découverte du principe de la cryptographie à clé publique, Diffie et Hellman ont proposé en 1976 un protocole d'échange de clés totalement sécurisé.

Cette découverte de Diffie et Hellman est une vraie révolution dans l'histoire de la cryptographie. Le problème de l'échange des clés est en effet résolu. Cette idée valut en 2015 aux deux auteurs le prix Turing.

L'objectif est de permettre l'établissement d'une clé privée entre deux parties, à l'aide de messages envoyés sur un canal non sécurisé. De plus, toute personne qui intercepte ces messages transmis ne doit pas pouvoir en déduire la clé générée.

154

Position du problème

Le problème est le suivant:

Alice et Bob veulent s'échanger un message crypté en utilisant un algorithme nécessitant une clé K. Ils veulent s'échanger cette clé K, mais ils ne disposent pas de canal sécurisé pour cela. Le protocole d'échange de clés de Diffie et Hellman répond à ce problème.

Ce protocole s'applique dans le cadre d'un groupe cyclique, en particulier le groupe multiplicatif Z/pZ^* , avec p un nombre premier.

155

Rappels sur le groupe des inversibles de Z/nZ

Soit n un entier naturel non nul. On note Z/nZ^* (ou $\mathbf{Z_n}^*$) l'ensemble des éléments inversibles de Z/nZ :

$$Z/nZ^* = \{\bar{k}, \text{PGCD}(k, n) = 1\}.$$

C'est un groupe multiplicatif.

Si p est premier alors Z/pZ^* est cyclique, càd fini et engendré par un seul élément :

$$\mathbb{Z}/p\mathbb{Z}^* = \{1, \alpha, \alpha^2, \ldots, \alpha^{p-2}\}.$$

156

Exercices

Exo 1.

a) Enumérer tous les éléments de Z_{30}^*.

b) Calculer l'inverse de 13 dans Z_{30}

Exo 2.

Supposons que p est premier.

a) Montrer que tout élément non nul de Z/pZ est inversible.

b) Déduire le nombre d'éléments de Z/pZ*.

157

Difficulté calculataoire

L'algorithme Diffie-Hellman repose sur le postulat suivant :

Étant donnés des entiers p, a, x, avec p premier et $1 \leq a \leq p-1$:

- il est facile de calculer l'entier $y = a^x \pmod{p}$.
- si on connait $y = a^x \pmod{p}$, a et p, il est très difficile de retrouver x, pourvu que p soit assez grand.

Retrouver x connaissant $a^x \pmod{p}$, a et p s'appelle résoudre le problème du **logarithme discret**. Comme pour la factorisation d'entiers, c'est un problème pour lequel on ne dispose pas d'algorithme efficace.

158

Etapes d'échange de la clé

	Alice	Bob
Étape 1 :	Alice et Bob choisissent ensemble un grand nombre premier p et un entier $1 \leq a \leq p-1$. Cet échange n'a pas besoin d'être sécurisé.	
Étape 2 :	Alice choisit secrètement x_1.	Bob choisit secrètement x_2.
Étape 3 :	Alice calcule $y_1 = a^{x_1} \pmod{p}$.	Bob calcule $y_2 = a^{x_2} \pmod{p}$.
Étape 4 :	Alice et Bob s'échangent les valeurs de y_1 et y_2. Cet échange n'a pas besoin d'être sécurisé.	
Étape 5 :	Alice calcule $y_2^{x_1} = (a^{x_2})^{x_1} = a^{x_1 x_2} \pmod{p}$ et appelle ce nombre K, la clé secrète à partager avec Bob.	Bob calcule $y_1^{x_2} = (a^{x_1})^{x_2} = a^{x_1 x_2} \pmod{p}$ et appelle ce nombre K, la clé secrète à partager avec Alice.

159

Exemple

Alice et Bob choisissent un nombre premier p = 23 et un générateur a = 3
Alice choisit un nombre secret x_1 = 6 et Bob choisit à son tour un nombre secret x_2 = 15.
Donner les étapes du protocole de Diffie-Hellman et trouver la clé d'échange.

160

1.Alice et Bob ont choisi un nombre premier *p* et un générateur a. Dans notre exemple, *p*=23 et *a*=5

2.Alice choisit un nombre secret x_1=6

3.Elle envoie à Bob la valeur $y_1 = a^{x1}$ [mod *p*] = 5^6 [23] = 8

4.Bob choisit à son tour un nombre secret x_2=15

5.Bob envoie à Alice la valeur $y_2 = a^{x2}$ [mod p] = 5^{15} [23] = 19

6.Alice peut maintenant calculer la clé secrète : y_2^{x1} [mod p] = 19^6 [23] = 2

7.Bob fait de même et obtient la même clé qu'Alice :

$$y_1^{x2} \text{ [mod p]} = 8^{15} \text{ [23]} = 2$$

La clé secrète est donc K=2

161

Exercice

Alice et Bob utilisent le protocole de Diffie-Hellman pour échanger la clé. Ils choisissent un nombre premier p = 233 et un générateur a = 45.

Alice choisit un nombre secret x_1 = 11 et Bob choisit à son tour un nombre secret x_2 = 20.

Quelle est la clé d'échange ?

162

Confidentialité

La confidentialité est garantie par le fait qu'un éventuel attaquant, qui intercepterait les communications entre Alice et Bob, n'aurait aucun moyen de retrouver la clé privée à partir des informations transmises publiquement.

À la fin du protocole, Alice et Bob sont donc en possession d'une même clé secrète K, qu'ils n'ont pas échangé directement. Si quelqu'un a espionné leurs conversations, il connait p,a,y1 et y2. Il ne peut pas retrouver K comme le font Alice ou Bob. x1 et x2 étant de très grands nombres, il est en effet extrêmement complexe de retrouver leurs valeurs à partir des informations transmises en clair (problème du logarithme discret).

163

Applications

L'algorithme Diffie-Hellman est un algorithme d'échange de clés, utilisé notamment lors de l'ouverture d'une connexion à un site sécurisé via le protocole SSL/TLS.

Il est également utilisé pour les problèmes d'appariement de deux objets dans la technologie Bluetooth.

164

Cryptographie symétrique

VS

Cryptographie asymétrique

Chiffrement à clé publique *VS* chiffrement à clé privée

- Le problème majeur avec un **chiffrement symétrique** (AES par exemple) est la nécessité de partager la clé. On doit transmettre les clés de manière sécurisée (sur un canal authentifié).
- Le problème majeur avec un **chiffrement asymétrique** (RSA par exemple) est sa lenteur à cause des calculs complexes qui y sont associés, alors que la cryptographie symétrique brille par sa rapidité. Ceci rend l'utilisation d'un chiffrement asymétrique coûteuse , puisqu'un tel chiffrement ne peut pas être appliqué sur un grand débit de données à transmettre.

166

Cryptographie hybride : Compromis entre les deux chiffrements

Pour pallier ce défaut, on recourt à la cryptographie hybride qui combine les deux systèmes afin de bénéficier des avantages (rapidité de la cryptographie symétrique pour le contenu du message) et utilisation de la cryptographie « lente » uniquement pour la clé.

Dans de nombreux environnements de communication modernes, y compris Internet, l'essentiel des données échangées est crypté par l'algorithme symétrique rapide AES. Sa clé privée, dite clé de session, est cryptée avec l'algorithme asymétrique RSA.

Code à clé privée: Chiffrement et déchiffrement du message

Code à clé public: Chiffrement et déchiffrement de la clé

167

FONCTION DE HACHAGE

Fonction de hachage

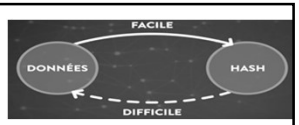
Une **fonction de hachage h** est une fonction permettant d'associer à chaque donnée d'entrée une **donnée de sortie**, appelée **résumé**.

La donnée d'entrée de ces fonctions est souvent appelée ***message*** (en anglais **Input**) ;

La valeur de sortie est souvent appelée **résumé, valeur de hachage**, **empreinte numérique**, **empreinte** ou encore **haché** (en anglais, ***message digest*** ou ***digest***, ***hash***).

Cette fonction doit posséder certaines propriétés.

Propriétés d'une fonction de hachage



La fonction de hachage doit être:

— **déterministe**: elle associe un et un seul résumé à un texte en clair.

— **à sens unique** (one-way function) : càd qu'il soit impossible de retrouver le message original à partir du résumé. On dit que h est **résistante à la préimage**.

y = h(x), mais il est impossible de retrouver x à partir de y !

— **résistante aux collisions:** c'est-à-dire que deux messages distincts doivent avoir très peu de chances de produire le même résumé. Cela signifie que la moindre modification du document entraine la modification de son résumé. L'idéal est que h soit injective mais c'est loin d'être vrai. On dit que h est **résistante à la seconde préimage.**

Difficile de trouver m1 et m2 différents tels que h(m1)=h(m2)

Propriétés d'une fonction de hachage

Une fonction de hachage h transforme une entrée de données (Input) d'une dimension variable "m" et donne comme résultat une sortie de données (Digest) inférieure et fixe h(m).

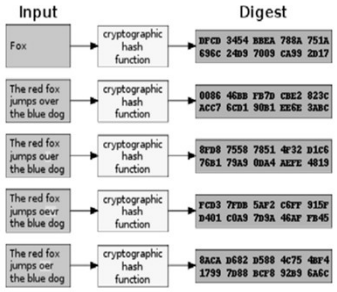
— l'entrée peut être de dimension variable ;

la sortie doit être de dimension fixe ;

— h(m) doit être relativement facile à calculer ;

— h doit être une fonction à sens unique ;

— h doit être presque « sans collision ».



Authentification et intégrité

Les algorithmes de hachage sont utilisés dans la génération des signatures numériques. Le hachage assure:

— **L'intégrité**: càd vérifier si un document a été modifié (le changement d'une partie du document change son empreinte) ;

— **L'authenticité**: le destinataire est sûr de l'identité de l'émetteur, et réciproquement.

Les fonctions de hachage les plus utilisées de nos jours sont les SHA-2 (*Secure Hash Algorithm*). C'est une famille de fonctions de hachage qui comporte les fonctions **SHA-256** (32 bits) et **SHA-512** (64 bits).

Signature numérique

La **signature numérique** (ou **signature électronique**) est un mécanisme permettant de garantir l'intégrité d'un document électronique et d'en authentifier l'auteur, par analogie avec la signature manuscrite d'un document papier.

La signature est obtenue en appliquant d'abord une fonction de hachage au document puis en chiffrant le résumé à l'aide d'une clé (privée ou publique).

Hachage Chiffrement

Document ----------> Résumé ----------> Signature

173