

Cryptologie et signature électronique

GS15

Rémi Cogranne (& Nicolas Burger)

Université de Technologie de Troyes

Bureau : H109
remi.cogranne@utt.fr

Automne 2016-2017

Sommaire

- 1 Introduction
- 2 Terminologie
- 3 Qualités d'un cryptosystème
- 4 Historique
- 5 Définitions mathématiques d'un cryptosystème
- 6 Et après ?
- 7 Objectifs

Sommaire

- 1 Introduction
- 2 Terminologie
- 3 Qualités d'un cryptosystème
- 4 Historique
- 5 Définitions mathématiques d'un cryptosystème
- 6 Et après ?
- 7 Objectifs

Organisation de GS15

Planning

- 4h/semaine mardi 10h-12h et 14h-16h : Cours, TD
- plus 5 séances de TP sous Matlab (ou en C) en demi groupe (12-14h / 14h-16h).
- Enseignants : Rémi Cогranne (H109, “The Boss”) Nicolas Burger (“the sous-fifre”).

Évaluation de l'UV

- Final : (2h, seconde moitié de l'UV, moyenne 2014 = 13.9)
- Médian : (2h, première moitié de l'UV, moyenne 2014 = 13.4)
- Projet informatique : (seconde moitié, moyenne 2014 = 15.7)
- Pondération : $\max(30\% \text{ Médian} + 30\% \text{ Projet} + 40\% \text{ Final} ; 40\% \text{ Médian} + 10\% \text{ Projet} + 50\% \text{ Final})$

Plan

- 1 Introduction
- 2 Terminologie
- 3 Qualités d'un cryptosystème
- 4 Historique
- 5 Définitions mathématiques d'un cryptosystème
- 6 Et après ?
- 7 Objectifs

Introduction

Objectif du cours

Donner une introduction à la cryptographie moderne utilisée dans la transmission et le stockage sécurisé de données

La cryptologie est la science des messages secrets

Longtemps restreinte aux usages diplomatiques et militaires, elle est maintenant une discipline scientifique à part entière, dont l'objet est l'étude des méthodes permettant d'assurer les services d'intégrité, d'authenticité et de confidentialité dans les systèmes d'information et de communication

Domaines d'utilisation

- Internet : confidentialité, anonymat, authentification,...
- Signature électronique
- Vote électronique
- Paiement par carte bancaire
- Porte-monnaie électronique : fausse monnaie,...
- Décodeur : vérification de l'abonné,...
- Base de données sécurisé : carte vitale,...



Plan

- 1 Introduction
- 2 Terminologie**
- 3 Qualités d'un cryptosystème
- 4 Historique
- 5 Définitions mathématiques d'un cryptosystème
- 6 Et après ?
- 7 Objectifs

Quelques définitions

Définition (Cryptologie)

Étymologie : crypto= $\kappa\rho\upsilon\pi\tau\omicron\varsigma$ =caché, graphie= $\gamma\rho\alpha\phi\epsilon\iota\nu$ =Écrire ou logie= $\lambda\omicron\gamma\iota\alpha$ =Étude : science du secret. La cryptologie ne peut être vraiment considérée comme une science que depuis peu de temps. Cette science englobe la cryptographie et la cryptanalyse

Définition (Cryptographie)

Science de la dissimulation de messages assurant confidentialité, authenticité et intégrité.

Définition (Cryptanalyse)

Science qui consiste à tenter de comprendre un message ayant été chiffré sans posséder la clé de chiffrement. Le processus par lequel on tente de comprendre un message en particulier est appelé une attaque.

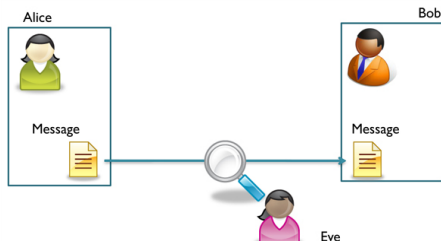
Terminologie

Protagonistes traditionnels

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

Objectif fondamental de la cryptographie

Alice et Bob peuvent communiquer sur un canal peu sûr. Ève ne doit pas comprendre ce qui est échangé.



Quelques définitions

Définition (Message en clair)

Information qu'Alice souhaite transmettre à Bob : texte, données chiffrées,...

Définition (Chiffrement)

Processus de transformation d'un message en clair en un message chiffré qui n'est pas compréhensible. Ce processus dépend souvent d'une clé de chiffrement.

Définition (Dechiffrement)

Processus de reconstruction du message clair à partir du message chiffré. Ce processus dépend souvent d'une clé de déchiffrement.

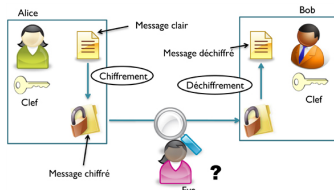
Plan

- 1 Introduction
- 2 Terminologie
- 3 Qualités d'un cryptosystème**
- 4 Historique
- 5 Définitions mathématiques d'un cryptosystème
- 6 Et après ?
- 7 Objectifs

Qualités d'un cryptosystème

Alice veut être certaine

- qu'une personne non autorisée (Ève) ne peut pas prendre connaissance de ses messages
- que ses messages ne sont pas falsifiés par un attaquant malveillant (Martin)
- que le destinataire (Bob) a bien pris connaissance de ses messages et ne pourra pas nier l'avoir reçu (non répudiation)
- que son message n'est pas brouillé par les imperfections du canal de transmission



Qualités d'un cryptosystème

Bob veut être certain

- que le message reçu est authentique c'est à dire que le message n'a pas été falsifié par un attaquant malveillant (Martin) et que le messages vient bien d'Alice (autrement dit qu'un attaquant (Oscar) ne se fait pas passer pour Alice, mascarade)
- que l'expéditeur (Alice) ne pourra pas nier avoir envoyé le message (non-répudiation)
- que le message n'est pas brouillé (par les imperfections du canal de transmission ou par un brouillage intentionnel), autrement dit qu'il est identique á l'original que lui a envoyé Alice.

Qualités d'un cryptosystème

Intégrité des données

Le message ne peut pas être falsifié sans qu'on s'en aperçoive

Identité des interlocuteurs du message

- L'émetteur est sûr de l'identité du destinataire c'est à dire que seul le destinataire pourra prendre connaissance du message car il est le seul à disposer de la clef de déchiffrement.
- Authentification, le receveur est sûr de l'identité de l'émetteur grâce à une signature

Non répudiation se décompose en 3

- D'origine : l'émetteur ne peut nier avoir écrit le message
- De reception : le receveur ne peut nier avoir reçu le message
- De transmission : l'émetteur du message ne peut nier avoir envoyé le message.

Services d'un cryptosystème

Service d'intégrité

Garantir que le contenu d'une communication ou d'un fichier n'a pas été modifié. Par exemple, on peut souhaiter vérifier qu'aucun changement du contenu d'un disque dur n'a eu lieu

Service d'authenticité

Garantir l'identité d'une entité donnée ou l'origine d'une communication ou d'un fichier. Le service de non-répudiation est réalisé par une signature numérique

Service de confidentialité

Garantir que le contenu d'une communication ou d'un fichier n'est pas accessible aux tiers. Des services de confidentialité sont offerts dans de nombreux contextes (téléphonie mobile, navigateurs, télévision à péage, ..)

Attaques passives d'un cryptosystème

Attaque brutale

Enumérer toutes les valeurs possibles de clés

Attaque par séquences connues

Deviner la clé si une partie du message est connue

Attaque par séquences forcées

Faire chiffrer par la victime un bloc dont l'attaquant connaît le contenu, puis on applique l'attaque précédente ...

Attaque par analyse différentielle

Utiliser les faibles différences entre plusieurs messages pour deviner la clé

Attaques actives d'un cryptosystème

Principe

- Martin peut modifier le contenu des messages échangés.
- Menace l'intégrité de l'information.

Exemples

- Usurpation d'identité (de l'émetteur ou du récepteur).
- Altération/modification du contenu des messages.
- Destruction de messages et/ou retardement de la transmission.
- Répétition de messages (jusqu'à engorgement).
- Répudiation de message : l'émetteur nie avoir envoyé le message.

Plan

- 1 Introduction
- 2 Terminologie
- 3 Qualités d'un cryptosystème
- 4 Historique**
- 5 Définitions mathématiques d'un cryptosystème
- 6 Et après ?
- 7 Objectifs

Un bref historique

Quelques grandes dates

- -600 : Utilisation de la cire pour cacher un message.
- -500 : Spartiates (cryptographie par permutation).
- -50 : chiffrement de César (cryptographie par substitution monoalphabétique).
- 1586 : chiffrement de Vigenère (cryptographie par substitution polyalphabétique).
- 1914-1945 : machine Enigma (polyalphabétique mécanique).
- 1970 : DES (algorithme sur système informatique).
- 1977: RSA (Rivest Shamir Adleman): cryptographie asymétrique.
- 1985: chiffrement El Gamal.
- 2000: AES (Advanced Encryption Standard soit standard de chiffrement avancé).

Codes de 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).
- Un exemple historique dont le principe est encore utilisé dans les codes à clef secrète (DES, AES) est la méthode de la grille (principe utilisé par les spartiates).

Exemples

On veut envoyer le message suivant: RENDEZ VOUS DEMAIN
MIDI VILLETANEUSE

Codes de permutation

- 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)
- 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□TEC

Codes de permutation

- Pour augmenter la sécurité, on ajoute une clé.
- Pour cela on rajoute une clé secrète constituée par l'ordre de lecture des colonnes.

On choisit la clé: CAPTER

On numérote les colonne en fonction du rang des lettres du mot CAPTER dans l'alphabet 2, 1, 4, 6, 3, 5 et on lit les colonnes dans l'ordre indiqué.

EVEMINR□D□DADUADLUZ□N□TENOMILEESIIES

On a 6! codes différents.

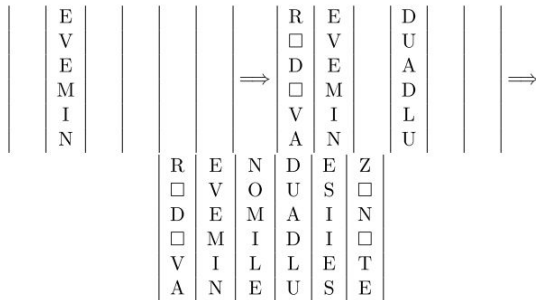
Exemples

Crypter le message suivant: LA CRYPTOGRAPHIE EST BIEN
avec la clé SUPER

Codes de permutation

Déchiffrement

Pour décoder le message précédent on range en colonne sur la grille en suivant l'ordre des colonnes donné par le mot de code



On a affaire à un code à clé secrète ou code symétrique car la clé de décodage est la même que la clé de codage.

Codes de substitution (monoalphabétique)

Dans les codes de substitution l'ordre des lettres est conservé mais on les remplace par des symboles d'un nouvel alphabet suivant un algorithme précis.

Exemple (Code de César)

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
Jules César pendant la guerre des Gaules a utilisé ce code de substitution suivant :

lettre codée = lettre claire + 3 modulo 26

Le message en clair RENDEZ VOUS DEMAIN MIDI
VILLETANEUSE devient UHQGHC YRXV GHPDLQ PLGL
YLOOHWDQHXVH

Codes de substitution (monoalphabétique)

Chiffrement

On peut considérer toute la famille des codes
lettre codée = lettre claire + n modulo 26 où n est un entier entre 0 et 25 appelé la clé du code.

Avec la clé $n = 7$ le texte codé du message précédent devient:
YLUKLG CVBZ KLTHPU TPKP CPSSLAHULBZLBZL

Déchiffrement

Le décodage se fait en utilisant la relation
lettre claire = lettre codée - n mod 26
Ccode symétrique ou à clé secrète.

Codes de substitution (décodage)

Décodage par analyse de fréquence

On considère un message codé avec une substitution monoalphabétique: JTVMNKKTVLDEVVTLWTWITKTXUTLW-JERUTVTWTHDXATLIUNEWV.

JTVIEWWELOWENLVVNOEDJJTVLTPTXYTLWTWUT
SNLITTVQXTVXUJXWEJEWTONKKXLT.

Lettre	% français	% texte	Lettre	% français	% texte
A	9,4	1	N	7,2	5
B	1,0	0	O	5,1	2,5
C	2,6	0	P	2,9	1
D	3,4	2,5	Q	1,1	1
E	15,9	8	R	6,5	1
F	1	0	S	7,9	1
G	1	0	T	7,3	20
H	0,8	1	U	6,2	4,5
I	8,4	3,8	V	2,1	12
J	0,9	5,1	W	0	9,9
K	0	4,7	X	0,3	6
L	5,3	9	Y	0,2	1
M	3,2	1	Z	0,3	0

Codes de substitution (décodage)

On peut donc faire l'hypothèse que $T=E$ puis que $V=S$ (à cause des lettres doublées) puis que les voyelles A, I, O, U correspondent à D, E, N, X et finalement on obtient la correspondance

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

Codes de substitution (polyalphabétique)

Code de Vigenère

- On se fixe une longueur de bloc m .
- On découpe le message en blocs de m -lettres.
- On chiffre par blocs de m lettres. On décide par exemple que la première lettre d'un bloc de m est codée avec un code de César de clé n_1 , la deuxième avec un code de César de clé n_2 et la m -ième par un code de César de clé n_m .

Exemple

$m = 5, n_1 = 3, n_2 = 14, n_3 = 7, n_4 = 22, n_5 = 19$

Codes de substitution (Vigenère)

		Lettre en 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
C l é	A	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
	B	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	A
	C	C	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
	D	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
	E	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	D
	F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
	G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
	H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
	I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
	J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
u t i l i s é e	K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
	L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
	M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
	N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
	O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
	P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
	Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
	R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
	S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
	T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
C o d e	U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
	V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
	W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
	X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
	Y	Z	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	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

Codes de substitution

Exemple (Un exemple pratique)

Message en clair	U	N	I	V	E	R	S	I	T	E
Clé	U	T	T	U	T	T	U	T	T	U
Cryptogramme	O	G	B	P	X	K	M	B	M	Y

Question

Chiffrer la phrase "LA VIE EST BELLE" avec la clé "CLE".

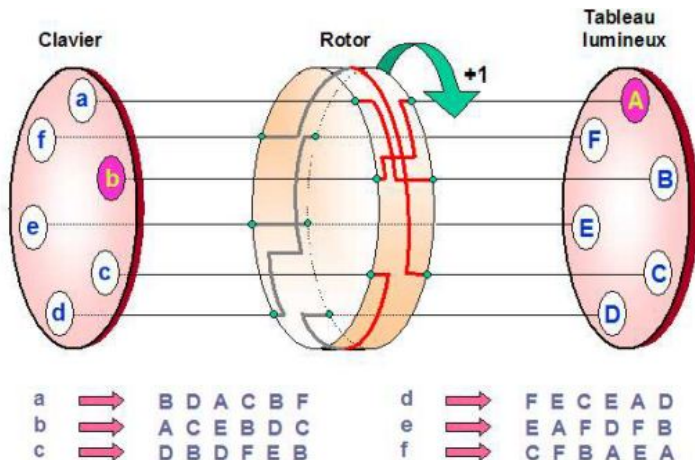
Codes de substitution

Enigma

La cryptologie connut une véritable avancée en 1918 grâce à l'invention de l'Allemand Arthur Scherbius : la machine Enigma.



Codes de substitution (Emigma simplifiée)



Codes de substitution (Emigma simplifiée)

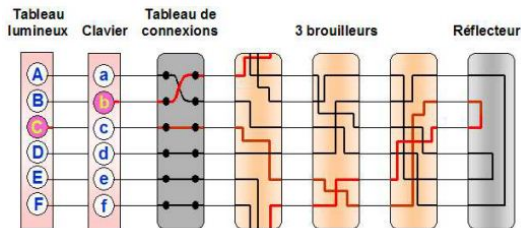
Pivotement du rotor

En faisant pivoter d'un cran le rotor, chaque fois qu'une lettre est saisie au clavier, cela revient à procéder à un changement automatique d'alphabet chiffré à chaque frappe clavier.
Le système de substitution polyalphabétique de Vigenère en action, et sans effort !

Question

Si un utilisateur entre le message clair "bbbbbb", quel est le message chiffré ?

Codes de substitution (Emigma complète)



Nombre de façons différentes de chiffrer un même message avec Enigma supérieur à 10 millions de milliards avec 3 rotors

- Orientation des brouilleurs : $26 \times 26 \times 26$ positions = 17 576 alphabets chiffrés différents
- Disposition des brouilleurs : 123, 132, 213, 231, 312, 321 = 6 positions possibles
- Tableau de connexions : 100 391 791 500 nombre de branchements possibles en appariant 6 fois 2 lettres parmi 26.

Plan

- 1 Introduction
- 2 Terminologie
- 3 Qualités d'un cryptosystème
- 4 Historique
- 5 Définitions mathématiques d'un cryptosystème**
- 6 Et après ?
- 7 Objectifs

Petit rappel sur les bijections

Définition (Fonction Bijective)

Une fonction f de \mathcal{A} dans \mathcal{B} est bijective ssi tout élément $b \in \mathcal{B}$ admet un unique antécédent par f , i.e. $\forall b \in \mathcal{B}, \exists! a \in \mathcal{A} : f(a) = b$.

Définition (Fonction inverse)

On appelle fonction inverse d'une fonction bijective f la fonction de \mathcal{B} dans \mathcal{A} qui à tout élément $b \in \mathcal{B}$ associe l'antécédent de b par f , i.e. $f^{-1}(b) = a$ lorsque $f(a) = b$.

On a : $f^{-1}(f(a)) = a$ pour tout $a \in \mathcal{A}$.

Petit rappel sur les bijections

Définition (Permutation)

Soit S un ensemble fini. Une permutation p sur S est une fonction bijective de S dans S .

Exemple (Permutation)

Soit $S = 1, 2, 3, 4, 5$ et soit la fonction p définie par $p(1) = 3$, $p(2) = 5$, $p(3) = 4$, $p(4) = 2$, $p(5) = 1$.

On représente aussi cette fonction sous la forme

$$p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 2 & 1 \end{pmatrix}$$

Question

Montrer que p est une permutation.

Domaine de définitions des variables

Définition (Alphabet)

Soit \mathcal{A} un ensemble fini de symboles appelé l'alphabet. Par exemple, $\mathcal{A} = \{0, 1\}$ ou $\mathcal{A} = \{A, B, C, \dots, X, Y, Z\}$. Tous les alphabets peuvent être codés à partir de l'alphabet binaire.

Définition (Espace de messages)

On note \mathcal{M} l'ensemble des messages en clair, i.e. l'ensemble des chaînes de caractères $m_1m_2\dots$ composé de caractères $m_i \in \mathcal{A}$ où \mathcal{A} est l'alphabet d'entrée. On note \mathcal{A}^n l'ensemble des messages de longueurs n .

Définition (Espace de chiffrement)

On note \mathcal{C} l'ensemble des messages chiffrés, i.e. l'ensemble des chaînes de caractères $m_1m_2 \dots$ composé de caractères $m_i \in \mathcal{A}$ où \mathcal{A} est l'alphabet de sortie.

Définitions des fonctions

Définition (Espace de clés)

On note \mathcal{K} l'ensemble des clés.

Définition (Fonction de chiffrement)

Chaque élément $e \in \mathcal{K}$ détermine de façon unique une fonction bijective E_e de \mathcal{M} dans \mathcal{C} . E_e est appelée une fonction de chiffrement. C'est une fonction bijective car il faut pouvoir déchiffrer le message produit par la fonction E_e .

Définition (Fonction de déchiffrement)

Chaque élément $d \in \mathcal{K}$ détermine de façon unique une fonction bijective D_d de \mathcal{C} dans \mathcal{M} . D_d est appelé une fonction de déchiffrement.

Définitions d'un système de chiffrement

Définition (Système de chiffrement)

Un système de chiffrement consiste en un ensemble $\mathcal{E} = \{E_e : e \in \mathcal{K}\}$ et un ensemble $\mathcal{D} = \{D_d : d \in \mathcal{K}\}$ avec la propriété : pour toute clé $e \in \mathcal{K}$, il existe une unique clé $d \in \mathcal{K}$ telle que $D_d = E_e^{-1}$, soit encore $D_d(E_e(m)) = m$ pour tout message $m \in \mathcal{M}$.

Remarque

Concevoir un système de chiffrement revient à définir les 5 ensembles \mathcal{M} , \mathcal{C} , \mathcal{K} , \mathcal{E} , \mathcal{D} . Ces ensembles sont généralement connus du public.

Remarque

La paire de clés $(e; d)$ définit une procédure de chiffrement. Tout le secret de la procédure réside dans la clé. En cas de doute dans la sécurité, il suffit de changer de paire de clés.

Exemple sur un cas d'école

Exemple (Sur un exemple)

- Soit $\mathcal{M} = \{m1, m2, m3\}$ et $\mathcal{C} = \{c1, c2, c3\}$.
- Il y a $3! = 6$ fonctions bijectives de \mathcal{M} dans \mathcal{C} . Ces fonctions bijectives constituent l'ensemble \mathcal{E} et on choisit $\mathcal{E} = \mathcal{D}$.
- Notons $\mathcal{K} = \{1, 2, 3, 4, 5, 6\}$, chaque clé spécifie une bijection.
- Alice et Bob choisissent une clé commune $e = d \in \mathcal{K}$ qui définit une fonction bijective.

Remarque

En pratique, les ensembles \mathcal{E} et \mathcal{D} sont tellement grands qu'il devient très difficile pour un adversaire de trouver la fonction de déchiffrement.

Algorithme cassable

Définition (Système de chiffrement cassable)

Un système de chiffrement est dit cassable si un adversaire, sans aucune information a priori sur $(e; d)$, peut systématiquement retrouver le message original à partir du message chiffré dans un temps raisonnable.

Remarque

Un temps raisonnable correspond à un temps "petit" devant la durée de vie de l'information contenue dans le message chiffré.

Définition (Recherche exhaustive)

Tout système de chiffrement peut être cassé en essayant toutes les clés possibles! C'est la recherche exhaustive. Lorsque l'espace des clés est de taille très important, cette recherche devient infaisable numériquement.

Ordre de grandeurs

Pour se faire une idée sur la recherche exhaustive

Supposons que le système informatique utilisé teste 10^{12} clés par seconde (ce n'est pas encore possible de nos jours, plutôt 10^6).

Taille de la clé (bits)	Nombre de clés	Temps requis
32	$2^{32} \approx 10^9$	$\approx 10^{-3}$ secondes
56	$2^{56} \approx 10^{16}$	≈ 10 heures
128	$2^{128} \approx 10^{38}$	$\approx 10^{18}$ années
168	$2^{168} \approx 10^{50}$	$\approx 10^{30}$ années

Remarque

L'âge de l'univers est estimé à $6 \cdot 10^9$ années.

Lois de Kerckhoffs (1883)

Les 7 "lois"

- Une information codée ne doit en aucun cas pouvoir être déchiffrée sans la connaissance de sa clé.
- Les interlocuteurs ne doivent pas subir de dégâts au cas où le système de codage serait dévoilé.
- La clé doit être simple et modifiable à souhait.
- Les cryptogrammes doivent être transportables, c'est-à-dire télégraphiables.
- L'appareil de codage et les documents doivent être transportables.
- Le système doit être simple d'utilisation.
- Le système de chiffrage doit être au préalable examiné par des experts.

Lois de Kerckhoffs

Le principe de Kerckhoffs à retenir

La sécurité d'un cryptosystème ne doit reposer que sur le secret de la clé. Par conséquent, l'algorithme peut être divulgué.

Cryptosystème symétrique

Définition (Cryptosystème symétrique)

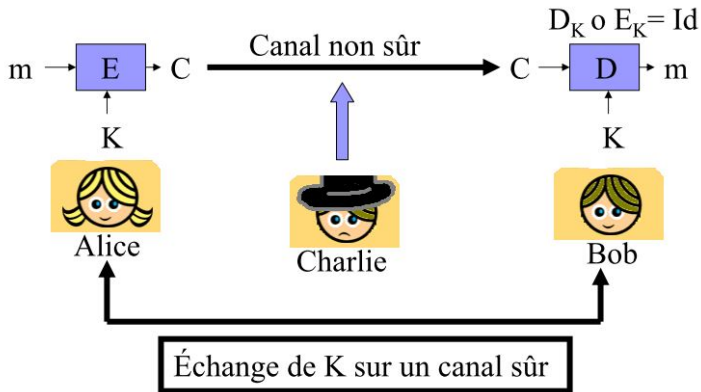
Considérons un système de chiffrement avec les ensembles de chiffrement et de déchiffrement $\mathcal{E} = E_e : e \in \mathcal{K}$ et $\mathcal{D} = D_d : d \in \mathcal{K}$ où \mathcal{K} est l'espace des clés.

Le système de chiffrement est dit à clé privée ou symétrique si pour chaque pair de clés $(e; d)$, il est "numériquement facile" de déterminer d connaissant e et de déterminer e à partir de d .

Remarque

En pratique, on a souvent $e = d$, d'où le terme de cryptographie symétrique.

Cryptosystème symétrique



Cryptosystème asymétrique

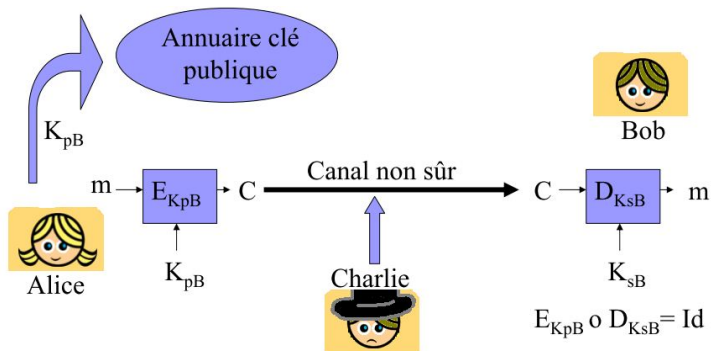
Définition (Cryptosystème asymétrique ou à clé publique)

Considérons un système de chiffrement avec les ensembles de chiffrement et de déchiffrement $\mathcal{E} = \{E_e : e \in \mathcal{K}\}$ et $\mathcal{D} = \{D_d : d \in \mathcal{K}\}$ où \mathcal{K} est l'espace des clés.

Supposons que chaque pair $(E_e; D_d)$ vérifie la propriété suivante : connaissant E_e , il est numériquement infaisable, connaissant un message chiffré $c \in \mathcal{C}$, de trouver le message en clair $m \in \mathcal{M}$ tel que $E_e(m) = c$.

Cette propriété implique que, connaissant e , appelé la clé publique, il est numériquement infaisable de déterminer la clé d , dite clé privée. Le système de chiffrement est dit alors à clé publique.

Cryptosystème asymétrique



Comparaison symétrique/assymétrique

Symétrique

- Avantages
 - Rapidité
- Inconvénients
 - Nombre de clés à gérer
 - Distribution des clés (authentification, confidentialité)

Assymétrique

- Avantages
 - Nombre de clés à distribuer est réduit par rapport aux clés symétriques,
 - Distributions des clés facilités : pas besoin de l'authentification
- Inconvénients
 - Vitesse de chiffrement (environ un facteur 1000 entre les deux)

Comparaison symétrique/assymétrique

Problèmes propres aux deux systèmes




- Auparavant la sécurité reposait sur le fait que l'algorithme utilisé était secret
Exemple : Alphabet de César. Décalage de trois positions des lettres de l'alphabet
Le mot CESAR devient FHVDU
- Aujourd'hui les algorithmes sont connus de tous. La sécurité repose uniquement sur le secret d'une clé (principe de Kerckhoffs).
La gestion des clés "secrètes" reste le maillon faible.

Plan

- 1 Introduction
- 2 Terminologie
- 3 Qualités d'un cryptosystème
- 4 Historique
- 5 Définitions mathématiques d'un cryptosystème
- 6 Et après ?
- 7 Objectifs

Et après ?

Au programme


- Les mathématiques pour la cryptographie (arithmétique, théorie des corps finis; complexité algorithmique,...)
-  Génération de nombres aléatoires, chiffrement de flux
- Description des schémas de chiffrement à clé privée : DES, AES, ...
- Description des systèmes à clé publique: RSA, El-Gamal, ...
- Protocoles d'échange de clés
- Fonctions de hachage et signature
-  Des TPs avec Matlab ou en C et un mini-projet.
-  Un recueil d'exo (et d'examens des années précédentes).

Plan

- 1 Introduction
- 2 Terminologie
- 3 Qualités d'un cryptosystème
- 4 Historique
- 5 Définitions mathématiques d'un cryptosystème
- 6 Et après ?
- 7 Objectifs**

Objectifs de l'UV

Clarifions les choses

- Cette UV comporte une partie mathématique importante ...
- Il n'est pas attendu de votre part que vous connaissiez les démonstrations sur le bout des doigts.
- Cest éléments mathématiques sont là pour que vous compreniez le fonctionnement des méthodes de chiffrement, comment on mesure certains quantités.
- Il est donc attendu que vous connaissiez les résultats principaux et que vous sachiez les utiliser POUR LA CRYPTO.
-  Un recueil d'exo (et d'examens des années précédentes) pour que vous sachiez mieux ce qui est attendu de vous