Introduction à la cryptographie

Pierre-Louis Cayrel

Université de Limoges, XLIM-DMI,
123, Av. Albert Thomas
87060 Limoges Cedex France
05.55.45.73.10
pierre-louis.cayrel@xlim.fr

Licence professionnelle Administrateur de Réseaux
et de Bases de Données
IUT Limoges

Déroulement du cours

- 16 heures de cours/TD sur 4 semaines
  (2 séances de 2 heures par semaine)
- Objectifs du cours
  - Introduction et sensibilisation à la cryptographie (2h)
  - Notions d'arithmétique modulaire, théorie de l'information et corps finis (4h)
  - Théorie de la complexité (30min)
  - Cryptographie à clef secrète
    (chiffrement à flot, chiffrement par blocs) (3h30)
  - Cryptographie à clef publique (RSA, logarithme discret) (1h30)
  - Fonctions de hachage et signature électronique(2h)
  - Architectures PKI, SSL et Kerberos (2h)

Quelques références bibliographiques

- Menezes A. J., Vanstone S. A. and Oorschot P. C. V., **Handbook of Applied Cryptography**, Computer Sciences Applied Mathematics Engineering, CRC Press, Inc., 1st edition, 1996, `http://www.cacr.math.uwaterloo.ca/hac/`
- Schneier B., **Cryptographie Appliquée,** Vuibert, Wiley and International Thomson Publishing, NY, 2nd edition, 1997. `http://www.schneier.com/book-applied.html`
- Stinson D.R, **Cryptography : Theory and Practice,** Chapman & Hall/CRC Press, 2nd edition, 2002. `www.cacr.math.uwaterloo.ca/dstinson/CTAP2/CTAP2.html`

Sommaire

Principes fondateurs de la cryptographie

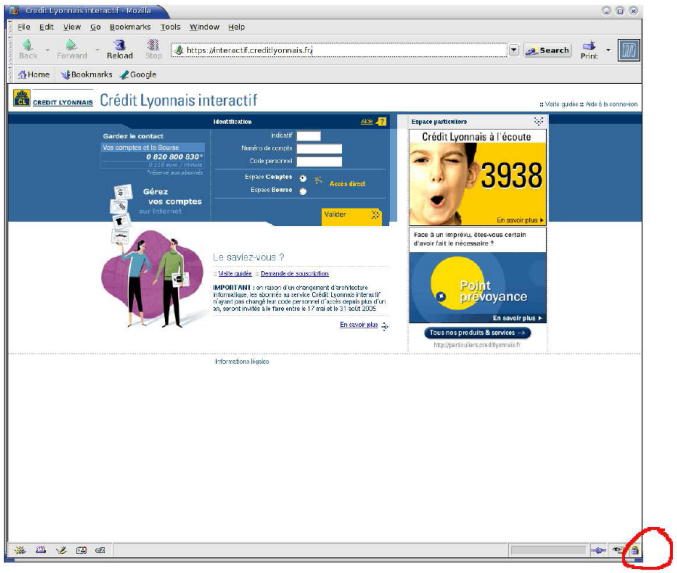
Cryptographie à clef secrète

Cryptographie à clef publique

Principes fondateurs de la cryptographie

Où utilise-t-on la cryptographie ? (1)

- **Internet** (confidentialité, anonymat, authentification (s'agit-il bien de ma banque ?))



Où utilise-t-on la cryptographie ? (2)

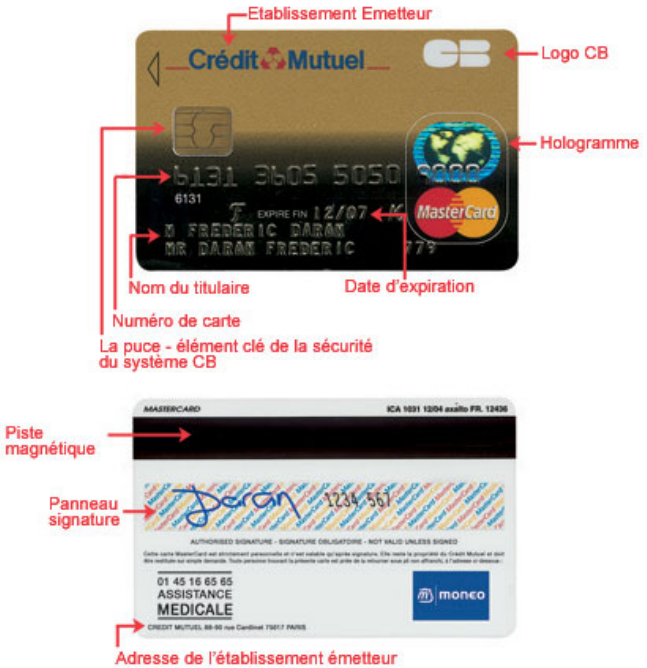
- **Signature électronique** (vérifiable, authentique, non-répudiation (je n'ai jamais signé ce texte ...))

Où utilise-t-on la cryptographie ? (3)

- **Vote électronique** (le résultat reflète le vote, chaque vote est confidentiel, on ne peut pas connaître des résultats partiels, seuls les électeurs peuvent voter et une seule fois)

Où utilise-t-on la cryptographie ? (4)

- **Paiement par carte bancaire** (Est-ce qu'il s'agit d'une vraie carte ? Est-ce que le montant débité sera égal au montant crédité ? Est-ce que le code secret est bien protégé ?)



Où utilise-t-on la cryptographie ? (5)

- **Décodeurs** (vérification de l'abonné, impossibilité de retransmettre les données décodées à une tierce personne, mise à jour de l'abonnement)

Où utilise-t-on la cryptographie ? (6)

- **Porte monnaie électronique** (pas de création de fausse monnaie, pas de création de faux porte-monnaie)

Où utilise-t-on la cryptographie ? (7)

- **Bases de données sécurisées** (ex : carte vitale.seules les personnes habilitées ont accès à la vue partielle à laquelle elles ont droit, les données peuvent être échangées entre un médecin, un laboratoire, un hôpital, mise à jour possible des données)

Cryptologie, cryptographie, cryptanalyse, c'est quoi la différence ?

- **Sécurité** se décompose en deux :
  sécurité informatique et **cryptologie**.
- **Cryptologie** :
  Science du secret avec deux composantes complémentaires :
  - **Cryptographie** : étude et conception des procédés de chiffrement des informations
  - **Cryptanalyse** : analyse des textes chiffrés pour retrouver les informations dissimulées

Bien distinguer, cryptographie et stéganographie

- **Cryptographie** : transforme un message clair en cryptogramme
- **Stéganographie** : dissimule l'existence même de l'information secrète (encre sympathique etc...)

Qui est cette femme ?

George Sand

Je suis très émue de vous dire que j'ai
bien compris, l'autre jour, que vous avez
toujours une envie folle de me faire
danser. Je garde un souvenir de votre
baiser et je voudrais que ce soit
là une preuve que je puisse être aimée
par vous.[...]

Illustration de l'utilisation de la stéganographie : extrait d'une lettre de George Sand.

Un autre exemple

Un mot sur la stéganographie

- Information non-chiffrée

  Connaissance de l'existence de l'information
  $=$
  Connaissance de l'information

- Exemples :
  - Message couvert : tablette couverte de cire, crâne du messager
  - Message invisible : encre sympathique (Pline 1er siècle av. JC)
  - Message illisible : Micro-film sous forme de point
  - Message subliminal : traitement de texte des ministres de M. Thatcher
- Théorie : Faible niveau de sécurité
- Pratique : ça marche ...(11/09/2001 ?)
- Utilisée également pour le Watermarking (JPEG, MP3-MPEG,etc)

- Laissons la stéganographie à Madame Sand et à Tintin, et intéressons nous à

LA CRYPTOGRAPHIE

Terminologie (1)

- Protagonistes traditionnels :
  - Alice et Bob : souhaitent se transmettre des informations
  - Oscar : un opposant qui souhaite espionner Alice et Bob
- Objectif fondamental de la cryptographie
  - permettre à Alice et Bob de communiquer sur un canal peu sûr
  - Oscar ne doit pas comprendre ce qui est échangé.

Terminologie (2)

- Texte clair : information qu'Alice souhaite transmettre à Bob
  - Ex : texte en français, donnée numérique etc...
- **Chiffrement :** processus de transformation d'un message M de telle manière à le rendre incompréhensible
  - Basé sur une fonction de chiffrement E
  - On génère ainsi un message chiffré $C = E(M)$
- **Déchiffrement :** processus de reconstruction du message clair à partir du message chiffré
  - Basé sur une fonction de déchiffrement D
  - On a donc $D(C) = D(E(M)) = M$ (D et E sont injectives)

A quoi sert la cryptographie ?

CAIN
(Confidentialité - Authentification - Intégrité - Non-répudiation)

- **C**onfidentialité des informations stockées/manipulées
  - utilisation d'un algorithme de chiffrement.
  - empêcher l'accès aux infos pour ceux qui ne sont pas autorisés.
- **A**uthentification d'utilisateurs/de ressources
  - utilisation d'algorithmes d'authentification.
  - Alice s'identifie à Bob en prouvant qu'elle connaît un secret S, (ex : un mot de passe).
- **I**ntégrité des informations stockées/manipulées
  - vérifier que les infos transmises n'ont pas subie d'altérations
- **N**on-répudiation des informations
  - utilisation d'algorithmes de signatures
  - empêcher un utilisateur de se dédire

Algorithmes de cryptographie

- Propriétés théoriques nécessaires :
  1. **Confusion :** Aucune propriété statistique ne peut être déduite du message chiffré
  2. **Diffusion :** Toute modification du message en clair se traduit par une modification complète du chiffré

Relation fondamentale

- En pratique : E et D sont paramétrées par des clés K_e et K_d : $E_{K_e}(M) = C$ et $D_{K_d}(C) = M$
- $K_e, K_d \in$ espace des clés.
- Définit deux catégories de systèmes cryptographiques :
  - Systèmes à **clé secrète** (ou **symétriques**) ($K_e = K_d = K$)
  - Systèmes à **clé publique** (ou **asymétriques**) ($K_e \neq K_d$)

Les grands types de menaces : menaces passives

- Oscar ne fait qu'écouter le message.
- menace la confidentialité
- une information sensible parvient également à une autre personne que son destinataire légitime.

Les grands types de menaces : menaces actives

- Oscar peut modifier le contenu des messages échangés.
- menace l'intégrité de l'information.
- Exemple d'attaques actives :
  - l'usurpation d'identité (de l'émetteur ou du recepteur)
  - l'altération / modification du contenu des messages ;
  - la destruction de messages/ le retardement de la transmission ;
  - la répétition de messages (jusqu'à engorgement)
  - la répudiation de message : l'émetteur nie avoir envoyé le message.

Modélisation de l'adversaire

On veut modéliser un attaquant :

- le plus intelligent possible $\longrightarrow$ il peut faire toutes les opérations qu'il souhaite
- qui dispose d'un temps limité.
  - on ne souhaite pas considérer les attaques faisables en 2^{80} ans
  - sinon, l'adversaire peut toujours énumérer toutes les clefs (temps exponentiel en $2^{taille(clefs)}$)

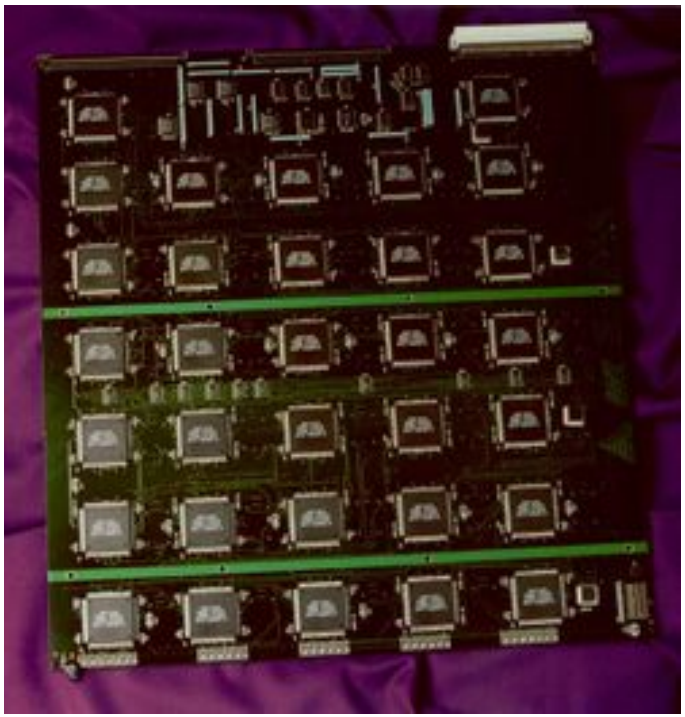
Les attaques sur un chiffrement

- Cryptanalyse : étude de la sécurité des procédés de chiffrement utilisés en cryptographie
- Niveaux d'attaques possibles :
  - Texte chiffré connu : seul C est connu d'Oscar
  - Texte clair connu : Oscar connaît C et M correspondant
  - Texte clair choisi : $\forall M$, Oscar peut obtenir C
  - Texte chiffré choisi : $\forall C$, Oscar peut obtenir M
- garantir la confidentialité $\Rightarrow$ Oscar ne peut pas :
  - trouver M à partir de $E(M)$
  - trouver la méthode de déchiffrement D à partir d'une séquence $\{M_i, E(M_i)\}$.

Algorithmes d'attaques

- Attaque brutale
  - Enumérer toutes les valeurs possibles de clefs
  - 64 bits $\Rightarrow 2^{64}$ clefs $= 1.844 \times 10^{19}$ combinaisons
    Un milliard de combinaisons/s $\Rightarrow$ 1 an sur 584 machines
- Attaque par séquences connues
  - Deviner la clef si une partie du message est connue
    ex : en-têtes de standard de courriels
- 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 (ex : logs) pour deviner la clef

Deep Crack, circuit dédié à l'attaque par force brute de DES.



Bref historique des codes secrets...

- Cryptographie Ancienne
  - Transposition Sparte (5ème siècle av JC)
  - Substitution César : décalage des lettres (1er siècle av JC),

Bref historique des codes secrets...

- Vigenère (XVI ème)
  - $\longrightarrow$ sujet à des analyses statistiques

Bref historique des codes secrets...

- Cryptanalyse des codes mono et poly alphabétiques
  - El Kindi (IXème siècle)
  - Babbage/Kasiski (XIXème siècle)
- Mécanisation de la cryptographie et de la cryptanalyse
  - Enigma (1918) (Niveau de sécurité qui dépend du nombre de rotors)

Enigma

Bref historique des codes secrets...

- Vers un chiffrement parfait : Vernam, théorie de l'information
- Standard de chiffrement à clé secrète : DES (1977), AES(2000)
- Cryptographie à clé publique (1976)

Cryptographie à clef secrète

Cryptographie symétrique

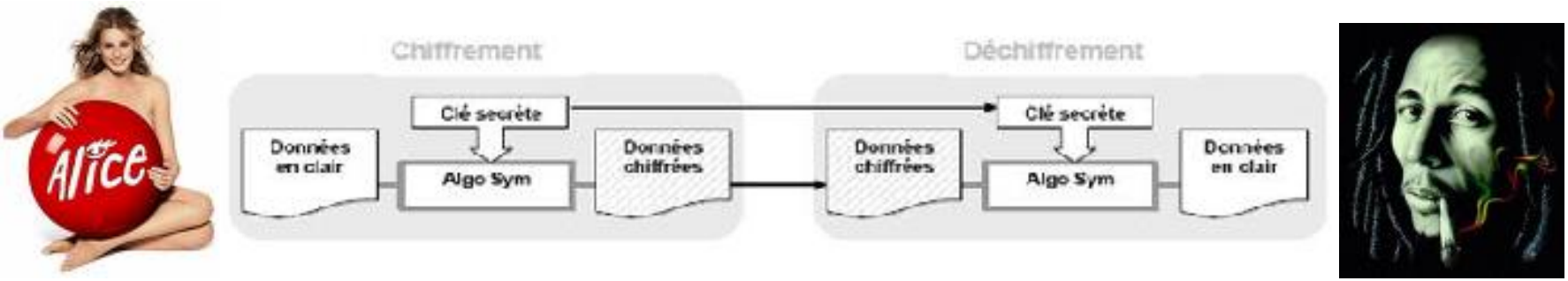


Fig.: La cryptographie symétrique

Concept fondamental en cryptographie symétrique : la clé

Principe de Kerckhoffs : l'algorithme doit pouvoir être divulgué.

De plus, la clef prend suffisamment de valeurs contre une attaque exhaustive.

Principe

- $K_e = K_d = K$ (clé privée convenue secrètement par Alice et Bob)
  - En pratique : grande efficacité en terme de temps de calculs
  - Inconvénient : la clé K doit rester secrète.
- Analogie : coffre-fort !
- Historiquement le premier type de chiffrement utilisé.
- Fourni le seul chiffrement théoriquement indéchiffrable
  - Chiffrement de Vernam (ou one-time password)
  - Démonstration du mathématicien Claude Shannon (1949)

Chiffrement symétrique : outils de base utilisés (1)

A la base des chiffrements à clé secrète :

- Substitution : remplacer chaque élément par un autre.
- Transposition (ou permutation) : changer l'ordre des éléments

Chiffrement symétrique : outils de base utilisés (2)

Autres opérations utiles :

- Arithmétique modulaire dans $\mathbb{Z}_n$, $a, b, n \in \mathbb{N}$, avec $n \geq 2$.

$$a = b \mod n \equiv n \text{ divise } a - b$$

En pratique : $b =$ reste de la division euclidienne de a par n.

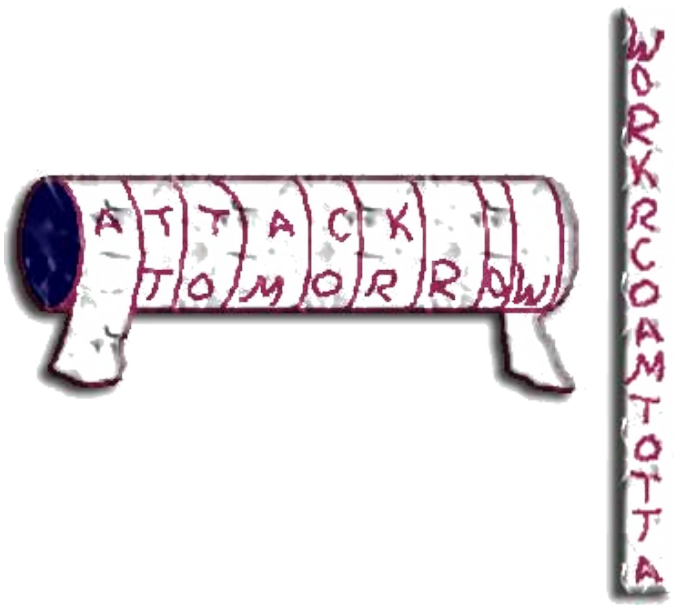
$$5 = 1 \mod 4 \text{ et } -3 = 125 \mod 128$$

- Notions associées : Primalité, Euclide, Th. des restes chinois, Gauss, Euler...
- opération XOR (ou exclusif $\oplus$)
  - Opération bijective (bijection inverse : $\oplus$)
  - correspond à une addition bit-à-bit modulo 2.

Les premiers procédés

Initialement, le secret échangé était la technique mise en oeuvre

- 400 av JC : esclave envoyé à Aristogoras par Histaïus
- Ve av JC : premières transpositions monoalphabétiques
  - Chiffrement de type anagramme : mélange les lettres du message
  - Confusion sur la syntaxe mais chaque lettre conserve sa valeur
  - Clé de chiffrement complexe
  - Principe des scytales spartiate (coms entre chefs des armées)

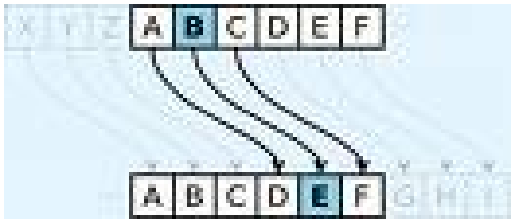


Les premiers procédés (2)

- IVe : premières substitution
  - Chiffrement par changement d'alphabet
  - Ex : Kama-sutra : recommande aux femmes de maîtriser le mlecchita-vikalpà (art de l'écriture secrète)
- 150 avant JC : carré de Polybe
  - alphabet de 25 lettres (pas de 'w' ou i et j regroupés)
  - remplace les lettres par des chiffres
  - codage d'une lettre = coordonnée dans le tableau : $A \rightarrow 11, B \rightarrow 12...$

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

Le chiffrement de César...



- Chiffrement par décalage avec $K = 3$.
- $E_K(M) = M + K \mod n$ et $D_K(C) = C - K \mod n$
- Seulement n façons différentes de chiffrer un message
  - code très peu sûr (recherche exhaustive facile)
  - avantage de la simplicité
    - employé par les officiers sudistes (guerre de Sécession)
    - réemployé sur les forums de News : $ROT - 13(K = 13)$
  - Généralisation : chiffrement affine

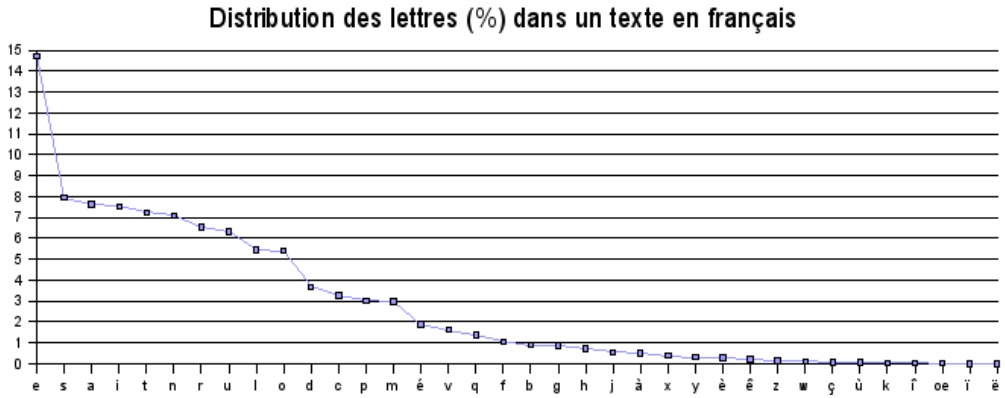
$$E_{(a,b)}(M) = a \times M + b \mod n(\text{ pour } a \in Z_n^{\times})$$

Cryptanalyse des substitutions mono-alphabétique

- Rappel : substitution mono-aphabétique : on remplace chaque lettre par une lettre différente.
- Nombre de possibilités (alphabet de 26 lettres) ?
  - chiffrement de A : 26 possibilités
  - chiffrement de B : 25 possibilités
  - ... $\longrightarrow 26! \approx 4 \times 10^{26}$ *possibilits*
  - Ordre de grandeur de comparaison : plier 50 fois sur elle-même une feuille de papier (épaisseur : 1 dixième de mm)
    $\longrightarrow$ épaisseur de la feuille :
    2^{50} dixième de millimètre $\approx 1,1 \times 10^8$ km
    (110 millions de km $\approx$ 300 fois distance Terre/Lune)

Cryptanalyse des substitutions mono-alphabétique

- MAIS ne cache pas la fréquence d'apparition des symboles !



  En français, la lettre e apparaît le plus souvent etc...

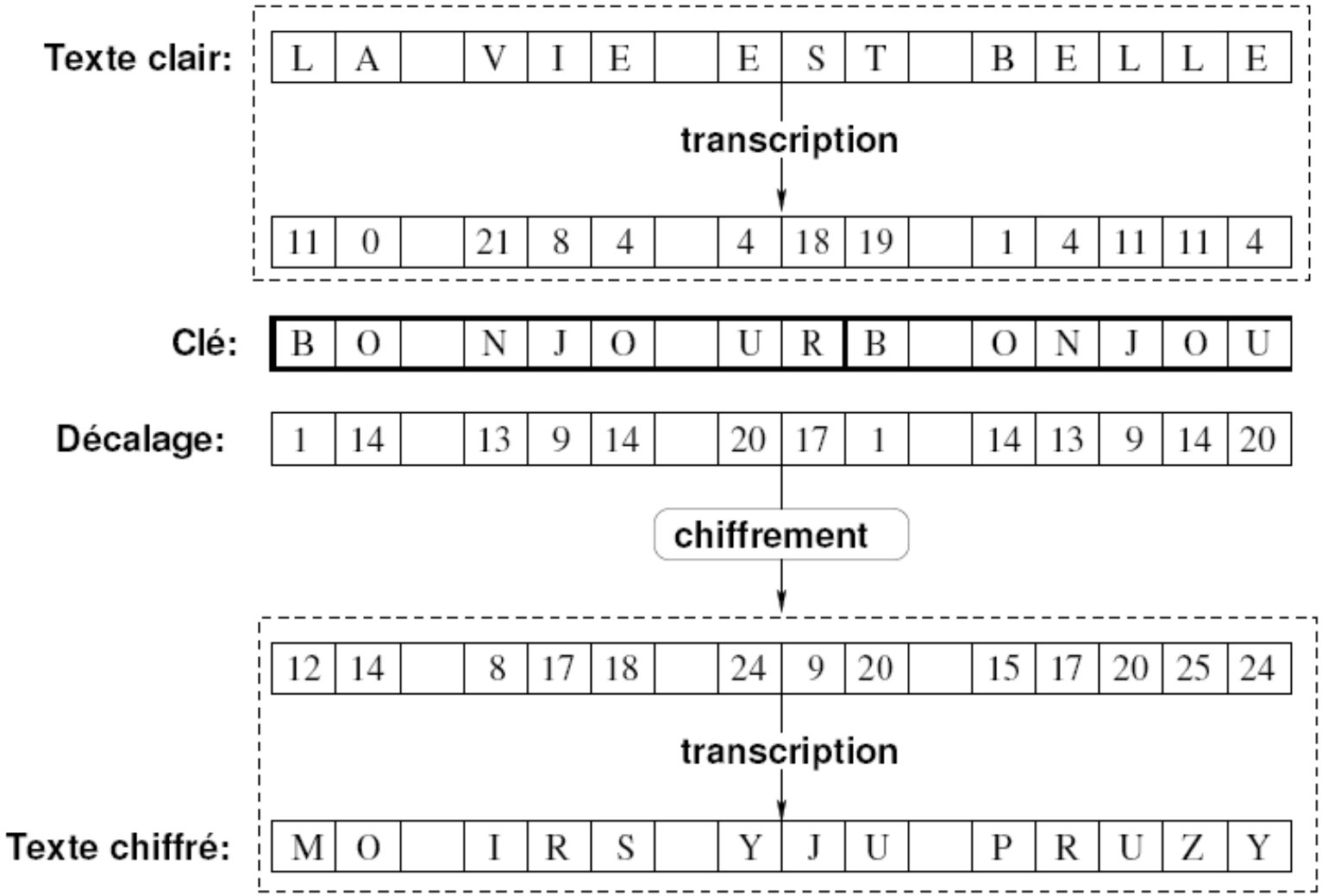
- Exemple : cryptanalyse du texte suivant : HQYRBHU GX UHQIRUW DYHF GHV DUPHV

  Réponse : envoyer du renfort avec des armes

- cryptanalyse proposée par Al Kindi (un savant arabe) au IXe s.

La cryptographie par substitution polyalphabétique (1)

- Méthode utilisée par Vigenère (1586)
  - la clef définit le décalage pour chaque lettre du message
    A : décalage de 0
    B : décalage de 1
    Z : décalage de 25
    Ex : chiffrement de *La vie est belle* avec la clé *bonjour*.


Texte clair:
L A V I E E S T B E L L E
transcription
11 0 21 8 4 4 18 19 1 4 11 11 4
Clé:
B O N J O U R B O N J O U
Décalage:
1 14 13 9 14 20 17 1 14 13 9 14 20
chiffrement
12 14 8 17 18 24 9 20 15 17 20 25 24
transcription
Texte chiffré:
M O I R S Y J U P R U Z Y

La cryptographie par substitution polyalphabétique (2)

- Procédé de Vigenère résistera jusqu'au milieu du XIXe s.
  - Cryptanalyse de Babbage (1854) et Kasiski (1863)
  - But : se ramener à la cryptanalyse de substitution simple
  - Exemple :

ENVOYER LA CAVALERIE
CLEFCLE FC LEFCLEFCL
$\longrightarrow$ GYZTAPD QC NEACWIWKP

1. Déterminer la taille de la clé (méthode de Kasiski) : 4
2. On réarrange le cryptogramme par groupe de 4 lettres :
   GYZT
   APDQ
   CNEA
   CWIW
   KP
3. Pour chaque colonne, cryptanalyse de substitution simple

Calculer la longueur d'une clé de Vigenère

- Considérons par exemple le message codé suivant :
  CS AZZMEQM, CO XRWF, CS DZRM GFMJECV. X'IMOQJ JC LB NLFMK CC LBM WCCZBM KFIMSZJSZ CS URQIUOU. CS ZLPIE ECZ RMWWTV, SB KCCJ QMJ FCSOVJ GCI ZI ICCKS...
- Idée : une séquence se répète $\longrightarrow$ la distance entre 2 séquences est probablement un multiple de la taille de la clef

Séquence	Position	Distance	Décomposition
COX	11-140	129	3.43
FCS	16-99	83	83
ZRM	20-83	63	$3^2 7$
FMJ	24-162	138	2.3.23
CLB	37-46	9	3^2
KCC	44-92	48	$2^3 3$
WTV	87-133	46	2.23
CCJ	93-126	33	3.11
ICC	110-155	45	$3^2.5$
MJI	136-163	27	3^3

pgcd pour les triplets pertinents : 3

- Cryptanalyse classique par analyse de fréquence en regroupant par paquet de 3

  LE SILENCE, LA PAIX, LE VIDE PRESQUE. J'AVAIS VU UN FURET OU UNE FOUINE TRAVERSER LE MACADAM. LE RUBAN QUI DEFILE, ET TOUS CES RUBANS SUR LA ROUTE...
- Méthode moderne (Friedman 1920) : calcul d'indices de coincidences.

Enjeux de la cryptanalyse : le télégramme de Zimmermann

- 1917 : la guerre s'enlise
- Les Etats-Unis de Wilson sont restés neutre
- L'état-major allemand veut lancer la guerre sous-marine totale
  - Pb : peut déclencher entrée en guerre des USA
  - Idée de Zimmermann (ministre aff. étr.) : occuper les USA avec le Mexique et le Japon $\Rightarrow$ soutien financier alld à ces insurrections.
  - Z. envoit un télégramme chiffré à l'ambassade d'allemagne aux USA
- Télégramme déchiffré par le bureau 40 (Montgomery et al.)
- Permet l'entrée en guerre des USA contre l'Allemagne.

Mécanisation de la cryptographie : Enigma

- Machine Enigma (Scherbius 1918)
  - Substitution polyalphabétique
    - 26 orientations pour 3 rotors : $26^3 = 17576$ alphabets
  - Réflécteur : cryptage/décryptage : même config
    - Connector/Reflector : substitution
- Brisé par l'équipe polonaise (Marian Rejewski) en 1933.
- Renforcé par les allemands pdt la 2eme guerre (avec 5 rotors)
- Cassé par les bombes de Turing (Bletchley) (dico...)

Notion de sécurité inconditionnelle

- Cryptanalyses précédentes utilisent la répétition de la clé
- Définition (Sécurité inconditionnelle) :

  la connaissance du message chiffré n'apporte aucune information sur le message clair.
  - seule attaque possible : recherche exhaustive de clé secrète
  - la clé secrète doit être au moins aussi longue que le texte clair
- Existe-t-il un sytème cryptographique inconditionnellement sûr ?

Alice et Bob veulent s'échanger des données à l'aide de la méthode du masque jetable appelée aussi One Time Pad.

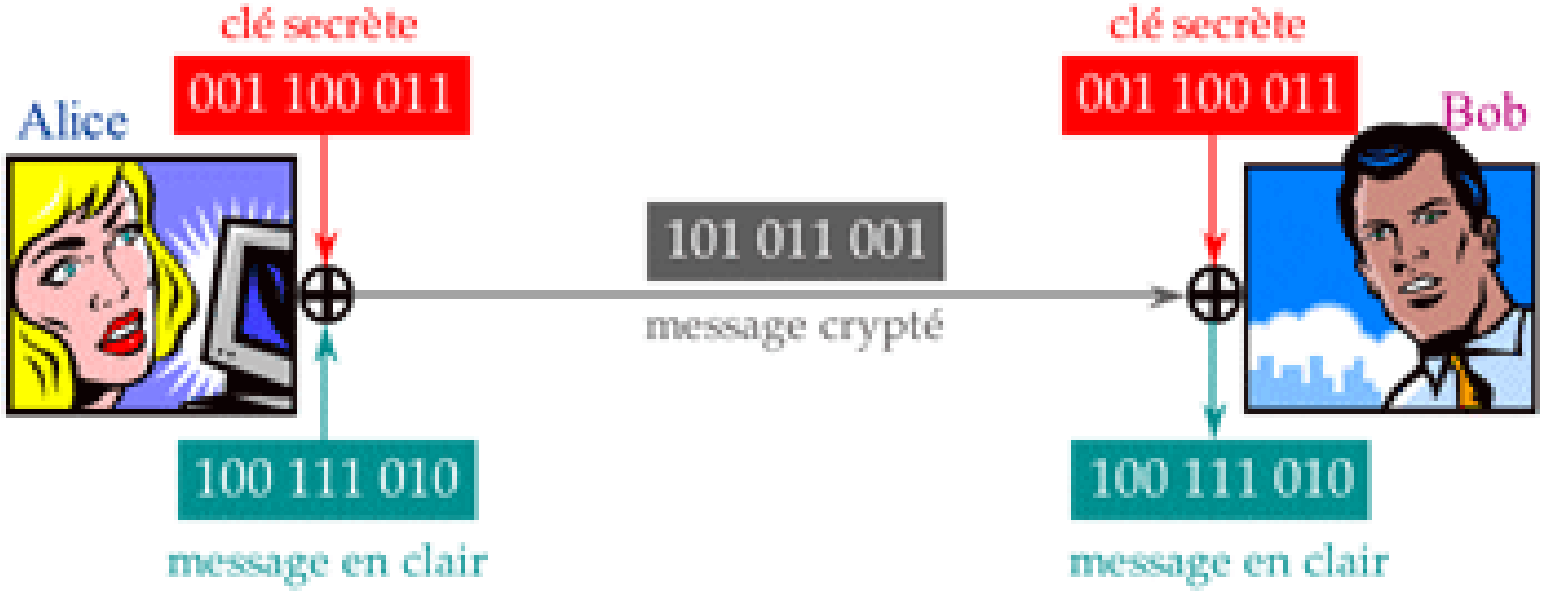
One Time Pad : *Xor* entre une suite de bits aléatoires et le texte à chiffrer.

$$chiffre_t := clair_t \oplus alea_t$$

Pb : Alice et Bob doivent posséder la même suite de bits aléatoires pour pouvoir décoder.

$$clair_t := chiffre_t \oplus alea_t$$

One Time Pad



Opération « ou exclusif » :

⊕	0	1
0	0	1
1	1	0

Systèmes cryptographiques pratiquement sûr

- Vernam : seul système prouvé inconditionnellement sûr
  - MAIS problème du caractère aléatoire et du stockage de K
  - tous les autres systèmes sont théoriquement cassables
- Définition (chiffrement pratiquement sûr) :

  un message chiffré ne permet de retrouver ni la clé secrète ni le message clair en un temps humainement raisonnable.

$\Rightarrow$ permet d'utiliser des clés plus petites (56, 128 bits...)

Systèmes cryptographiques pratiquement sûr

- **Question :** Pourquoi ne pas tester toutes les clés possibles ?

Systèmes cryptographiques pratiquement sûr

- **Réponse :** ce serait trop long a tester sur ordinateur !

  Ex : portable 1Ghz $\longrightarrow 10^9$ op/s ; clé : 128 bits soit

  $2^{128} \approx 3,4 \times 10^{38}$ possibilités $\Rightarrow 3,4 \times 10^{29}$ s

  10^{22} ordi pdt 1 an (il y a $\approx 10^9$ PC ds le monde en 2007)

  Age de l'univers : 15 milliards $\times 365 \times 24 \times 3600 \approx 4,7 \times 10^{17}$s

Système pratiquement sûrs utilisés aujourd'hui

- 1977 : standard de chiffrement D.E.S (56 bits)
  - basé sur des opérations facilement implantables
  - résultat du chiffrement statistiquement plat
  - utilisé dans les cartes à puces etc...
  - problème : clé devenu trop petite
    - cassable en 8h avec 100 PCs ($2^{56} \approx 7,2 \times 10^{16}$)

$$\frac{7,2 \times 10^{16}}{10^9 \times 3600 \times 24 \times 100} \approx 8 \text{ heures}$$

- depuis 2000 : nouveau standard A.E.S. (128, 192 ou 256 bits)
- Autres exemples de systèmes de chiffrement à clé secrète :
  - IDEA (1992) : blocs de 64 bits, clef de 128 bits ;
  - Triple DES à deux clefs : blocs de 64 bits, clef de 112 bits :

$$C = E_{K_1}(D_{K_2}(E_{K_1}(M)))$$
$$M = D_{K_1}(E_{K_2}(D_{K_1}(C)))$$

Cryptographie à clef publique

Motivations

- Systèmes cryptographiques à clé secrètes
  - pratiquement sûrs
  - efficaces en termes de temps de calcul.
- Mais nouvelles interrogations :
  - Avant d'utiliser un système de chiffrement à clé secrète, comment convenir d'une clé ?
  - Comment établir une communication sécurisée entre deux entités sans échange préalable de clef ?

  $\Rightarrow$ Solution apportée par Diffie et Hellman (1976)
  - systèmes cryptographiques à clé publique

Cryptographie à clef publique

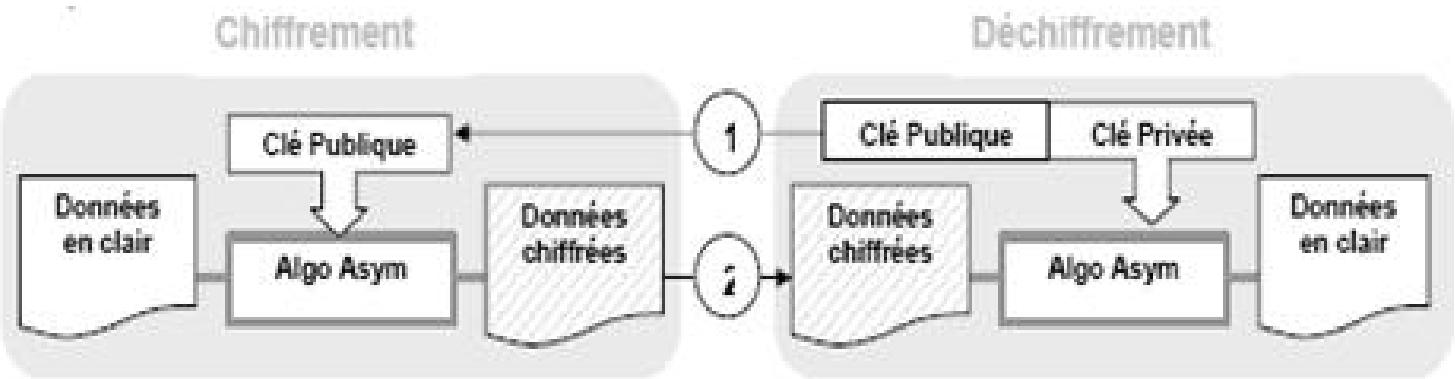


Fig.: La cryptographie asymétrique

Cryptographie asymétrique

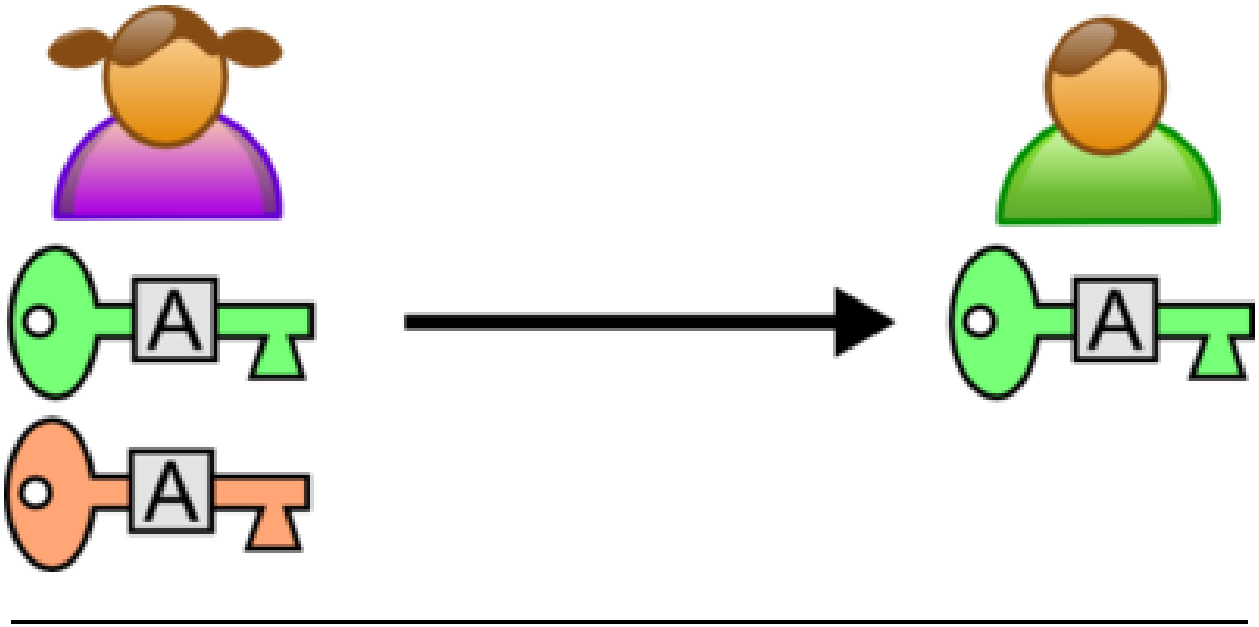


Fig.: La cryptographie asymétrique : Première Étape

Alice génère deux clés. La clé publique (verte) qu'elle envoie à Bob et la clé privée (rouge) qu'elle conserve précieusement sans la divulguer à quiconque.

Cryptographie asymétrique

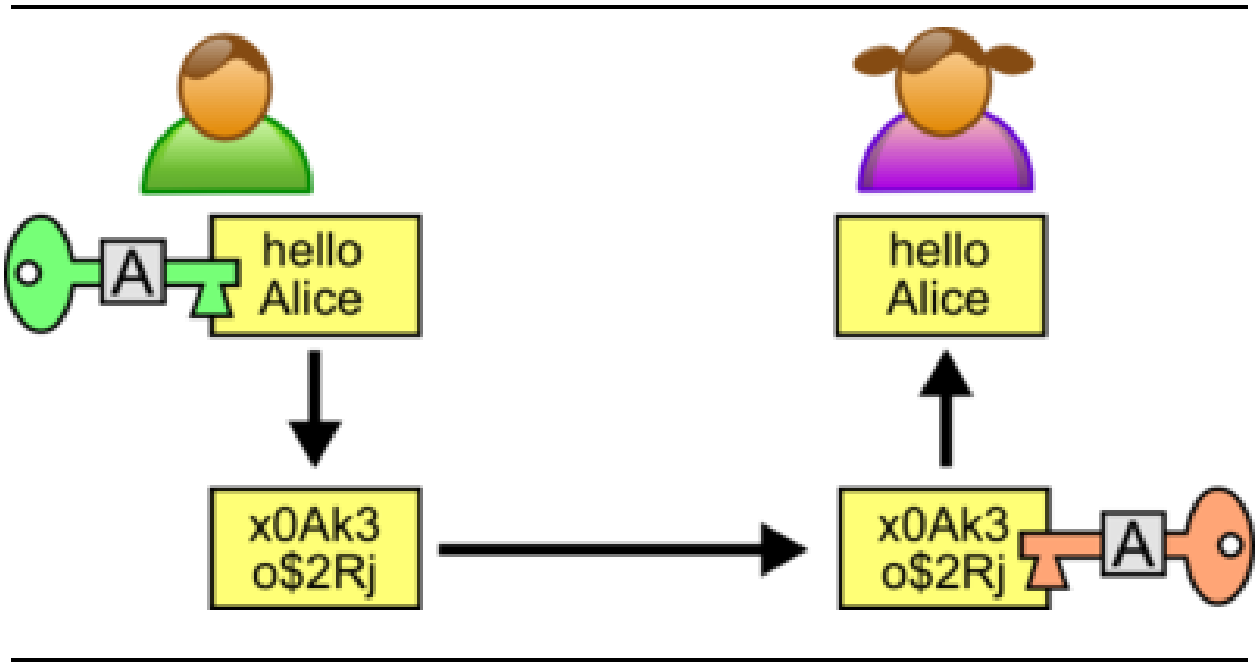


Fig.: La cryptographie asymétrique : Deuxième et Troisième Étape

Bob chiffre le message avec la clé publique d'Alice et envoie le texte chiffré. Alice déchiffre le message grâce à sa clé privée.

Cryptographie asymétrique

Fondée 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.

Déroulement

Bob souhaite pouvoir recevoir des messages chiffrés de n'importe qui.

- Il génère une valeur (clef publique) à partir d'une fonction à sens unique.
- Il diffuse la clef publique, mais garde secrète l'information permettant d'inverser cette fonction (clef secrète).

Ce qu'il reste à développer

- Des **maths** pour la crypto ...
- Description des schémas de chiffrement à clef privée : LFSR, DES, AES
- Description du système à clé publique le plus connu : RSA (1978)
- Protocole d'échange de clés de Diffie-Hellmann
- Fonction de hachage et signature
- Gestion des clés publiques (PKI,SSL,Kerberos)...
- ... A SUIVRE DANS LE RESTE DU COURS !