LES TECHNIQUES DE CRYPTOGRAPHIE

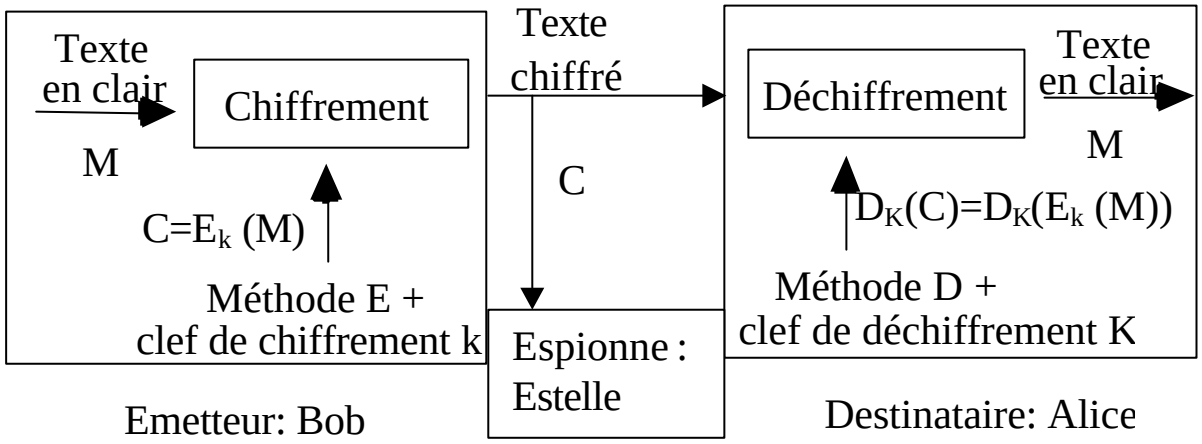
G. Florin

S. Natkin

Mars 2002

Généralités

Définition


Texte
en clair
M
Chiffrement
C=Ek (M)
Méthode E +
clef de chiffrement k
Emetteur: Bob
Texte
chiffré
C
Espionne :
Estelle
Déchiffrement
Texte
en clair
M
DK(C)=DK(Ek (M))
Méthode D +
clef de déchiffrement K
Destinataire: Alice

Chiffrement

Bob, doit transmettre à Alice, un message $M \in$ MESSAGES_A_ENVOYER.
M est dit “en clair“.

Estelle, une espionne, d’écouter la voie de communication pour connaître M.

Bob, construit un texte chiffré $C \in$ MESSAGES_CHIFFRES.

$$C = E_k(M). \quad \text{ou} \quad C = \{M\}_k^E$$

La fonction E_k dépend d’un paramètre k appelé clef de chiffrement.

Le **chiffrement** est donc une transformation d'un texte pour en cacher le sens

La possibilité de chiffrer repose donc sur la connaissance de l’algorithme de chiffrement E et de la clef k de chiffrement.

Déchiffrement

Le **déchiffrement** est l'opération inverse permettant de récupérer le texte en clair à partir du texte C chiffré.
Il repose sur la fonction D_K de MESSAGES_CHIFFRES dans MESSAGES_A_ENVOYER telle que

$$M= D_{K'}(C) \text{ ou } C = \{M\}^{D}_{K}$$

On doit avoir

$$D_K (E_k(M))=M$$

D_K est donc une fonction inverse à gauche de E_k.

Pour un couple cr = (E,D) donné de famille de fonction de chiffrement et de déchiffrement, l'ensemble des couples (k, K) vérifiant cette propriété est noté CLE(cr).

Crypto-systèmes

Pour que ces opérations assurent la confidentialité du transfert entre Alice et Bob, il est nécessaire qu'au moins une partie des informations E, D, k, K soit ignorée du reste du monde.

Décrypter ou casser un code c'est parvenir au texte en clair sans posséder au départ ces informations secrètes. C'est l'opération que doit réaliser Estelle pour retrouver M.

L'art de définir des codes est la cryptographie. Un spécialiste en cryptographie est appelé cryptographe.

L'art de casser des codes est appelé cryptanalyse ou cryptologie. Un spécialiste en cryptanalyse est appelé cryptanalyste.

Un crypto-système est l'ensemble des deux méthodes de chiffrement et de déchiffrement utilisable en sécurité.

Crypto-systèmes symétriques

Tels que soit k=K, soit la connaissance d'une des deux clefs permet d'en déduire facilement l'autre.

Conséquences :
Dichotomie du monde : les bons et les mauvais

Multiplication des clefs (un secret n'est partagé que par 2 interlocuteurs), donc pour N interlocuteurs N.(N-1)/2 couples

La qualité d'un crypto système symétrique s'analyse par rapport à des propriétés statistiques des textes chiffrés et la résistance aux classes d'attaques connues.

En pratique tant qu'un crypto système symétrique n'a pas été cassé, il est bon, après il est mauvais.

Crypto-systèmes asymétriques (a clefs publiques)

Tels que la connaissance de k (la clef de chiffrement) ne permet pas d'en déduire celle de K(la clef de déchiffrement).

Un tel crypto-système est dit asymétrique, la clef k est appelée la **clef publique**, la clef K est appelée la **clef privée**.

Fondement théorique : montrer que la recherche de K à partir de k revient à résoudre un problème mathématique notoirement très compliqué, c'est à dire demandant un grand nombre d'opérations et beaucoup de mémoire pour effectuer les calculs.

RSA (l'algorithme le plus utilisé à l'heure actuel) la déduction de K à partir de k revient à résoudre le problème de factorisation d'un grand nombre un problème sur lequel travaille les mathématiciens depuis plus de 2000 ans,

On estime que le plus rapide ordinateur que l'on puisse construire utilisant la meilleure méthode connue met plus de 1000 ans pour retrouver la clef privée d'un système RSA utilisant un modulo de 1024 bits (ordre de grandeur de la taille des clefs).

Asymétrie de l ’usage des clefs

BANQUE_MODERNE, désire autoriser ses clients à envoyer des ordres de virement chiffrés
Elle publie dans un annuaire infalsifiable

Nom = BANQUE_MODERNE, Algorithme de Chiffrement = E, Clef Publique = k

La banque conserve secrète la clef privée K.

Tout client peut calculer $C= E_k(M)$.

Seul la banque peut déchiffrer le message $M = D_K(C)$.

L ’algorithme d ’Estelle (Cryptanalyste)
Etape 1) Recherche des crypto -systèmes possibles

Hypothèses
Estelle veut décrypter C= E_k(M).
Estelle ne connaît ni D, ni E ni k, ni K.
Elle peut connaître des informations sur sa syntaxe et la sémantique de M.

Etape 1) Recherche des crypto systèmes possibles
CR={cr=(D,E)}

L ’algorithme d ’Estelle
Etape 2) Réduction de l ’espace des clefs

Pour tout cr déterminer le plus petit ensemble CLE_REDUIT⊂CLE(cr)
contenant la clef utilisée.
Si card (CLE_REDUIT={(k,K)})=1, M= D_K(C). Fin

A priori, tous les couples (k,K) sont équiprobable sur CLE(cr)
Estelle doit acquérir une connaissance soit déterministe (clefs impossibles) ou probabiliste (clefs improbables)qui facilite ses essais (réduit l ’entropie)

Exemples
Estelle possède M’ et C’ chiffrée avec le même cryptosystème et les mêmes clefs déduction de propriétés des clefs: **attaque à texte en clair**.
Estelle peut chiffrer des messages M avec E_k (sans connaître k) **attaque à texte en clair choisi**.

Estelle connaît des propriétés de l ’algorithme de génération de (k,K).

L ’algorithme d ’Estelle
Etape 3) Analyse syntaxique

Déterminer le plus petit ensemble MESSAGES_SYNTAXIQUEMENT_CORRECTS⊃ MESSAGES_A_ENVOYER qui vérifie des propriétés de syntaxe connues d’Estelle

Objectif : Construire un test d’arrêt simple pour le calcul mené à l’étape 4
Une règle syntaxique est sous une forme ou une autre un invariant d’un langage. Elle implique donc une certaine redondance de l’information.
Exemples
Le plus grand mot de la langue française a 25 lettres (anticonstitutionnellement). Possibilité d’écrire 10^{34} mots de 25 lettres ou moins 80000 mots dans le dictionnaire Hachette
"le" est nécessairement suivi d’un nom masculin

- Règles logique classique (toutes les suites de huit bits à partir du début du texte appartiennent à l’alphabet ASCII)
- Règles résultant de l’application d’un test statistique permettant d’accepter ou de rejeter une hypothèse (la répartition des caractères ASCII dans le texte en clair suit la même loi que la répartition des lettres dans la langue française). Fréquences d'apparition (en anglais)

Lettres	Digrammes	Trigrammes
E 13,05	TH 3,16	THE 4,72
T9,02	IN 1,54	ING 1,42

L ’algorithme d ’Estelle
Etape 3) Analyse syntaxique 2

Deux cas possibles

Etape 3.1 Construction de l’espace des messages

Informations très précise sur la syntaxe de M (M est un mot de passe sur 8 caractères qui est très probablement composé d’un mot ou de deux mots français concatènes).

Etape 3.2 Construction d’une règle syntaxique

$\exists$SYN tel que alors $\forall$ M

$\in$ MESSAGES_SYNTAXIQUEMENT_CORRECTS SYN(M)=vrai.

L ’algorithme d ’Estelle
Etape 4) Recherche Exhaustive

Construire MESSAGES_POSSIBLES$\subset$ MESSAGES_SYNTAXIQUEMENT_CORRECTS tel que mes $\in$ MESSAGES_POSSIBLES

Soit Etape 4.1 : Recherche sur l’espace des clefs de chiffrement
mes $\in$ MESSAGES_SYNTAXIQUEMENT_CORRECTS et $\exists$ (k, K) $\in$ CLE_REDUIT(cr) et $E_k(mes)=C$

Soit Etape 4.2 : Recherche sur l’espace des clefs de déchiffrement
$\exists$(k, K) $\in$ CLE_REDUIT(cr)et $D_K(C)$=mes et SYN(mes).

Si card(MESSAGES_POSSIBLES)=1, M=mes, Fin

Attaque à texte chiffré en parcourant itérativement soit l’espace des clefs de chiffrement soit celui des clefs de déchiffrement.

L ’algorithme d ’Estelle
Etape 5) Analyse sémantique

Trouver une règle sémantique SEM
(le message porte sur la cocaïne ou les fausses factures)
telle que :
card ({X MESSAGES_POSSIBLES tel que SEM(X)})=1
Si une telle règle existe M=X, Fin

Sinon Estelle a échouée

Point de vue du cryptographe
Etape 1

Opération autrefois difficile,
devenue simple: standard de cryptographie, systèmes commercialisés.
la sécurité d'un crypto-système ne repose plus que sur le secret des clefs
(sauf dans le domaine militaire).

Point de vue du cryptographe
Etape 2

Choisir un crypto système cr dont l'espace des clefs est très grand.

Choix des clefs est le plus imprédictible possible
(éviter les mots d'un dictionnaire , nombres pseudo aléatoires à grain de génération difficile à deviner)

Limiter l'usage des clefs

Choisir un bon crypto système asymétrique tel que le calcul de k' à partir de k,
ou même de la réduction des k' possibles connaissant k est un problème reconnu scientifiquement comme très difficile.
Si par un hasard extraordinaire, Estelle arrive à résoudre ce problème,
elle devient célèbre, riche et par conséquent heureuse en amour.
Elle n'a donc plus aucune raison d'embêter Bob et Alice.

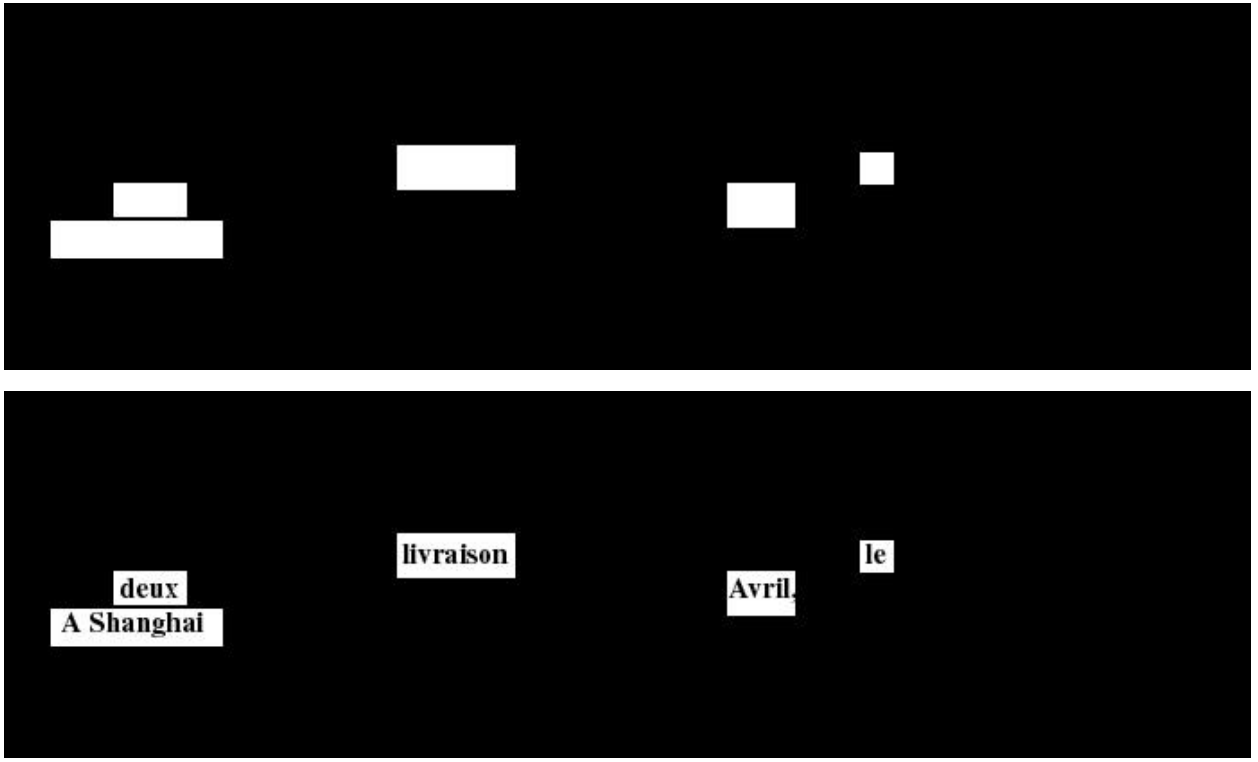
Point de vue du cryptographe
Etape 3

Deux stratégies :

Limiter la redondance (compression à un niveau syntaxique bas)

Augmenter la redondance en donnant plusieurs syntaxes possibles pour un même message (texte caché dans une image)

Masque classique



Cher ami
Je pense pouvoir assurer la livraison des 3O tonnes de blé prévue le 10 mars.
Mes deux assistants ne pourront venir vous voir avant Avril, mais je vous attends au Lotus Bleu
A Shanghai
Rastapopoulos

Point de vue du cryptographe
Etape 4
le masque jetable

Méthode imparable : le **chiffre parfait** ou masque jetable.

M sous forme d'une suite de n bits. Clef k_M de n bits, parfaitement aléatoire (suite uniforme de bits) utilisée qu'une seule fois (l'étape de réduction de l'espace des clefs n'a apportée aucune information)
$\Rightarrow$ Essai de toutes les clefs de CLE(cr) qui est l'ensemble des suites de n bits.

Chiffrement: $C=E_{k_M}(M)=M \oplus k_M$
Ou $\oplus$ représente le ou exclusif

Déchiffrement: $M=D_{k_M}(C)=C \oplus k_M$

très rapide et sans faille.

Point de vue du cryptographe
Etape 4
le masque jetable 2

$\forall$Mess $\in$ MESSAGES_SYNTAXIQUEMENT_CORRECTS $\exists$X $\in$ CLE(cr) tel que

$$C=E_X(Mess)$$

$X=C\oplus Mess \Rightarrow$

$$C= X\oplus Mess = C\oplus Mess\oplus Mess = C$$

En balayant tout l'espace des clefs on trouvera tous les messages de MESSAGES_SYNTAXIQUEMENT_CORRECTS.
Le fait d'avoir espionné pour connaître C n' a apporté aucune information.

Point de vue du cryptographe
Etape 4
le masque jetable 3

Notons :
A l'événement : C a été reçu par Estelle
B l' événement : M a été émis par Bob

Information apportée par la réception de :

$$I=-\log_2(\text{Probabilité(B sachant A)}/\text{Probabilité(B)})$$

Or comme toutes les clefs sont équiprobables, C a pu être construit avec à partir de n'importe quel message possible M'.Donc A et B sont indépendants.

$$\text{Probabilité(B sachant A)}=$$
$$\text{Probabilité(A).Probabilité(B)/Probabilité(A)=Probabilité(B)}$$

$$I=-\log_2(\text{Probabilité(B)}/\text{Probabilité(B)})=-\log_2(1)=0$$

Crypto-systèmes symétriques

Chiffrement par substitution

Principe général

A chaque lettre ou groupe de lettres on substitue une autre lettre ou un autre groupe de lettres.

substitution mono alphabétique

Pour chaque lettre de l'alphabet de base on se donne une autre lettre utilisée dans le texte chiffré.

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

Exemple historique: Le chiffre de César On décale les lettres de 3 positions

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
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

Forme générale des chiffre par décalage sur l'alphabet à 26 letres :

$$E_k(x)=x+k \bmod 26$$

$$D_k(y)=y-k \bmod 26$$

Chiffre de Vigenère

	0	1	2	3
	c	l	e	f
CL	2	11	4	5

$$E_{CL}(x_n)=(x_n+CL\ (n \bmod 4)) \bmod 26$$

t	e	x	t	e	s	e	c	r	e	t
19	4	23	19	4	18	4	2	17	4	19
2	11	4	5	2	11	4	5	2	11	4
21	15	1	24	6	3	8	7	19	15	23
v	p	b	y	g	d	i	h	t	p	x

Autres chiffres par substitution

Les substitutions homophoniques

Au lieu d'associer un seul caractère crypté à un caractère en clair on dispose d'un ensemble de possibilités de substitution de caractères dans laquelle on choisit aléatoirement.

Les substitutions de polygrammes

Au lieu de substituer des caractères on substitue par exemple des digrammes (groupes de deux caractères)

- Au moyen d'une table (système de Playfair)
- Au moyen d'une transformation mathématique (système de Hill).

Le masque pseudo aléatoire

Principe du masque jetable mais en utilisant un masque pseudo aléatoire. Le grain est la clef

Les chiffres par transposition

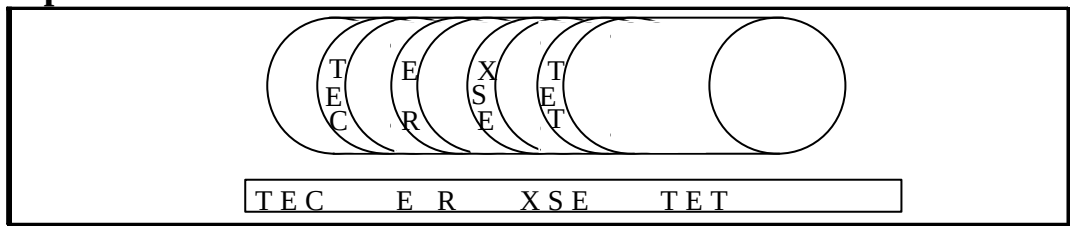
Principe général

On procède à un réarrangement de l'ensemble des caractères (une transposition) qui cache le sens initial.

La technique est très peu résistante aux attaques statistiques.

Le plus souvent on utilise deux visions géométriquement différentes du texte.

Exemple



- On enroule une fine langue de papyrus ou de peau sur un tambour d'un diamètre donné (technique assyrienne 400 av JC).

- On écrit horizontalement un texte sur la lamelle enroulée.

- Quand la lamelle est déroulée les lettres sont incompréhensibles.

- Pour décrypter le message il faut un cylindre du bon diamètre.

Transposition matricielle

- Le message en clair est écrit dans une matrice.

- La clé une permutation de [1..n] ou n est le nombre de colonne

- La technique de transposition consiste à lire la matrice en colonne selon un ordre donné par la clef.

Exemple

1	6	4	3	2	5
M	E	S	S	A	G
E	S	E	C	R	E
T	A	C	H	I	F
F	R	E	R	P	A
R	T	R	A	N	S
P	O	S	I	T	I
O	N				

Le message crypté est donc:
METFRPO ARIPNT SCHRAI SECERS GEFASI ESARTON

Chiffre symétrique moderne

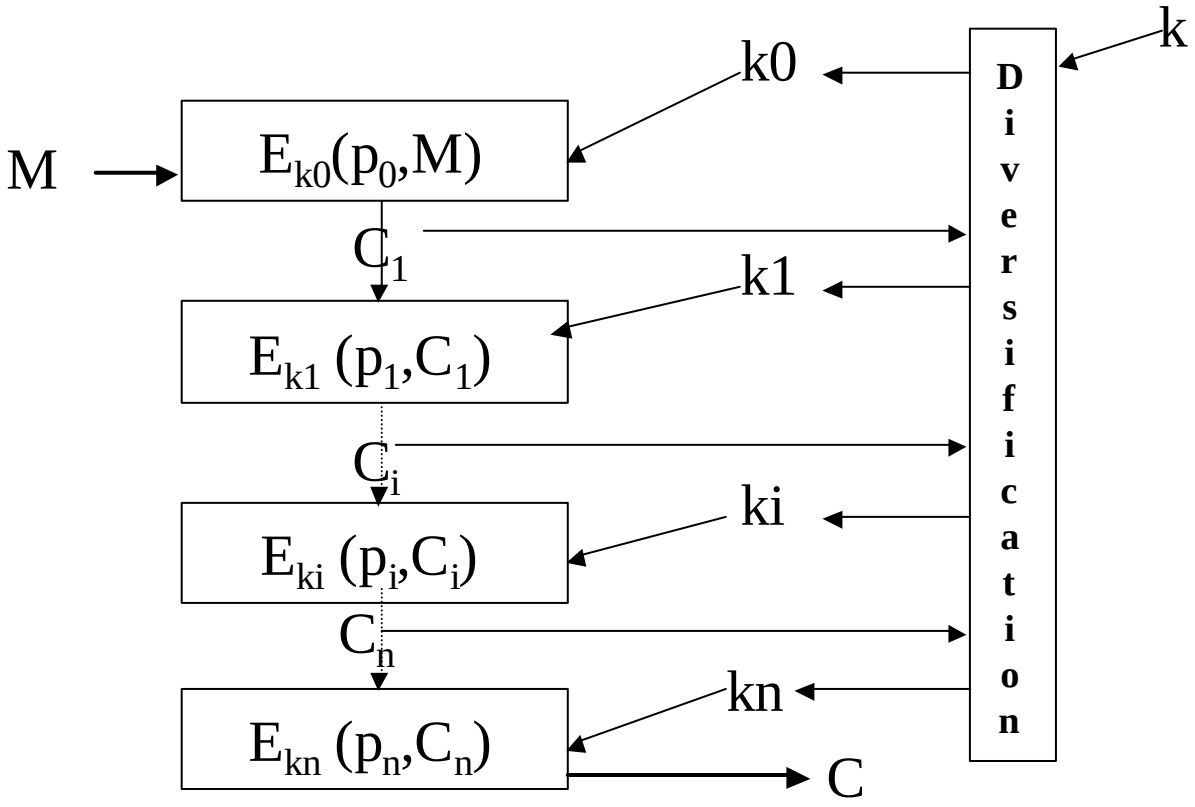
Prrincipes de confusion et de diffusion

Combinaison complexe d ’opérations de transposition et de substitution portant sur des chaînes de bits longues

Opérateurs booléens ou arithmétiques selon l ’implantation visée

Suite itérative d ’une fonction dépendant du calcul à l ’étage précédent, d ’une clef dérivée calculée en fonction de l ’itération et de la clef initiale (principe des système cryptographiques produits de Shannon et du chiffrement en chaîne)

Systèmes cryptographiques produits et chiffrement en chaîne



Réseaux de Feistel

Soit F(i ,B) une fonction de chiffrement qui utilise les mêmes clefs et paramètres que E mais porte sur des blocs B de longueur égale à la moitié de M.

E est donné par :

- On permute les deux blocs ce qui donne (R,L),
- C=E(M)=(LC, RC)

avec LC=R et RC=L⊕ F_{ki}(i,R).

E est son propre inverse.

- la première permutation donne (RC,LC)=(RC,R),
- l'ajout de la fonction donne (RC⊕ F_{ki}(i,R),R)= (L⊕F_{ki}(i,R) ⊕ F_{ki}(i,R),R)=(L,R)

Modes de chiffrement

$M=O_0,O_1,..., O_n,O_{n+1},..., O_{2n},....$

Par blocs (ECB: Electronic CodeBook)
$C=E(O_0,O_1,..., O_n),E(O_{n+1},..., O_{2n})....$

En chaîne (CBC: Cipher Block Chaining)
$C=E(S_0=(I_0,I_1,..., I_n)\oplus(O_0,O_1,..., O_n)),$
$E(S_1 = S_0 \oplus (O_{n+1},..., O_{2n})),....$
Fournit un meilleur brouillage et un contrôle d ’intégrité

Cryptanalyse différentielle

Nouvelles techniques d ’attaque à texte chiffré choisi:

$$A \longrightarrow A \oplus K \longrightarrow E(A \oplus K)$$

$$B \longrightarrow B \oplus K \longrightarrow E(B \oplus K)$$

$$A \oplus B \longrightarrow A \oplus B \oplus K \longrightarrow E(A \oplus B \oplus K)$$

Analyse pour tout A des sorties

$$\Delta(A)=\{E(B \oplus K) \oplus E(A \oplus B \oplus K)\}$$

Le DES: historique

-Dès le début des années 1960 la technologie des circuits intégrés permet de travailler à des circuits combinatoires complexes permettant d'automatiser:

la méthode de substitution.

la méthode de transposition.

=> Idée d'appliquer ces techniques en cascade dans un produit de chiffres.

- Mise au point à partir de 1968 d'une méthode de chiffrement basée sur 16 étages de substitutions et transpositions basés sur des clés (IBM)

- Appel d'offre NBS (1973) pour la mise au point d'un système de cryptographie

- Proposition IBM (1975)

- Adoption définitive et normalisation du DES d'IBM (1978) par le NBS ("National Bureau of Standards").

-Normalisation ANSI X3.92 connue sous le nom de DEA ("Data Encryption Algorithm").

Le DES: Principes (1)

Choix possibles pour la sécurité

- Méthodes simples de chiffrement et des clés très longues .

Le DES

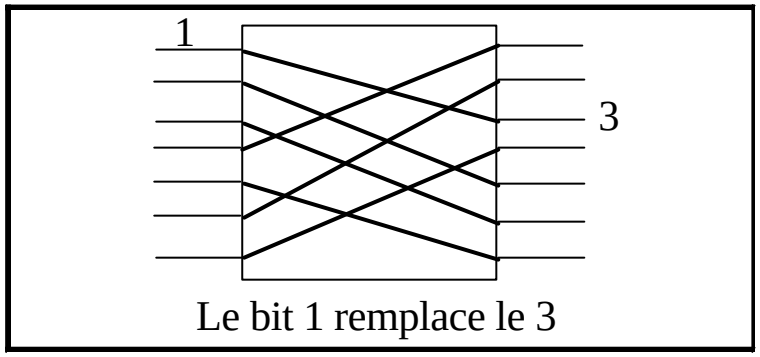
- Produit de transpositions et substitutions nombreuses et compliquées pour une clé relativement courte
  => facilité de transport.

- Les chiffres à substitution et à transposition sont faciles à réaliser en matériel.

Les boîtes de transposition "P-Box"
Les boites de substitution "S-Box"

Le DES: P-box

Exemple pour 8 bits (solution matérielle)



Facile à réaliser par simple câblage

Autre solution (logicielle) par des tables

Exemple de transposition sur 64 bits : permutation initiale du DES

58 50 42 34 26 18 10 2 60 52 44 36 28 20 12 4
62 54 46 38 30 22 14 6 64 56 48 40 32 24 16 8
57 49 41 33 25 17 9 1 59 51 43 35 27 19 11 3
61 53 45 37 29 21 13 5 63 55 47 39 31 23 15 7

Le bit 1 remplace le 58

Le DES: S_Box

Fonction d'expansion E

32	1	2	3	4	5	4	5	6	7	8	9	8	9	10	11	12	13	12	13	14	15	16	17
16	17	18	19	20	21	20	21	22	23	24	25	24	25	26	27	28	29	28	29	30	31	32	1

S-Box

2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

Le codage de 100101, conduit à choisir l'élément (2,5) de valeur 13, soit en binaire 1101.

Le DES architecture générale (1)

Deux modes

- Mode cryptage par bloc de 64 bits
- Mode cryptage à la volée ("stream")
(octets par octets avec des registres à décalage)

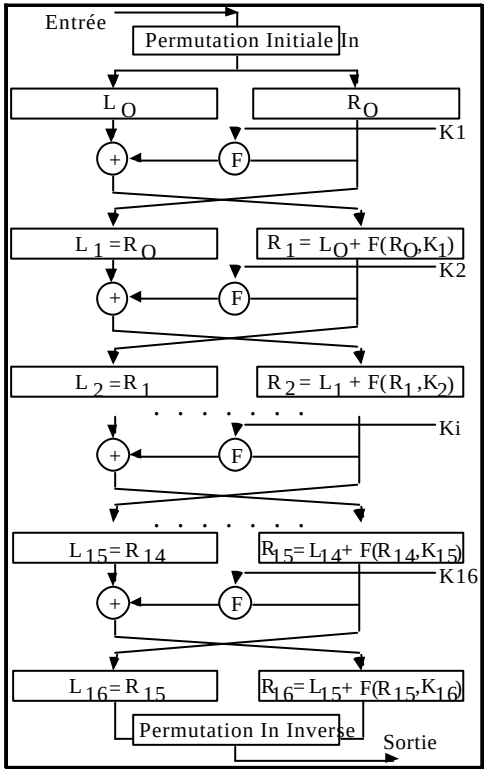
Utilisation d'une clé sur 56 bits

En fait 8 fois 7 bits avec une parité
(initialement 128 bits)

19 étages de logique combinatoire

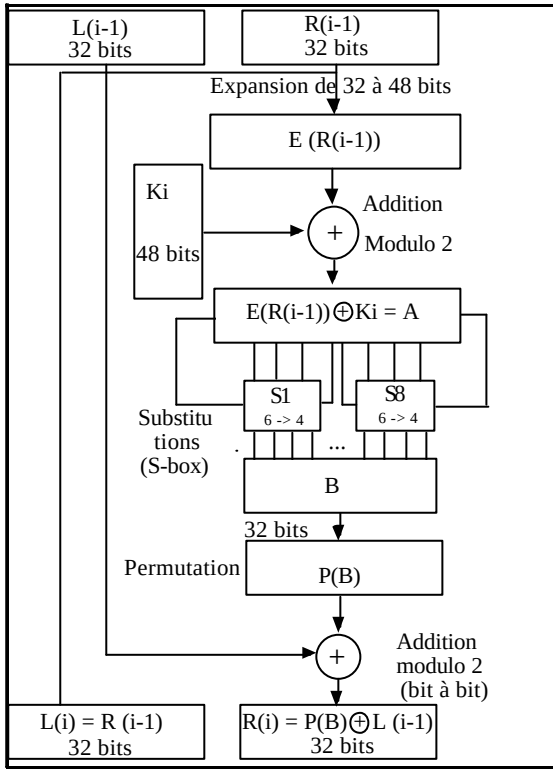
Appliquent des transpositions substitutions sur des blocs de 2 x 32 bits
- 1 étage amont, 2 en aval sont des transpositions simples fixes
- 16 étages intermédiaires dépendent de la clé de façon complexe.

Le DES architecture générale (2)

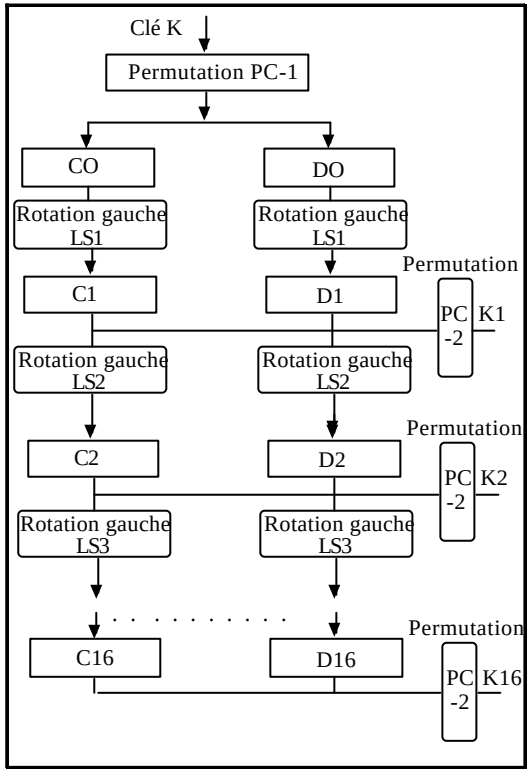


Réseau de Feistel: Chaque ronde est son propre inverse

Le DES architecture générale (3)



DES: Diversification des clefs



DES: Controverse

- Performances Excellentes - cryptage à la volée à débits potentiellement très élevés (dizaine/ centaine de Mégabits/seconde).

- Utilisation multiples : Transmission de données informatiques, Cryptage de chaînes de télévision à péage.

Controverse sur la sécurité du DES
Problème de longueur des clés

Des puces spéciales permettant l'essai de 10^6 clés par seconde ont été construites Elles peuvent être organisées en processeurs spéciaux massivement Le DES 56 est attaquable par des moyens informatiques plus ou moins lourds à la portée des états.

Problème du choix des substitutions

Les principes de choix des S-box n'ont complètement été rendus publique:

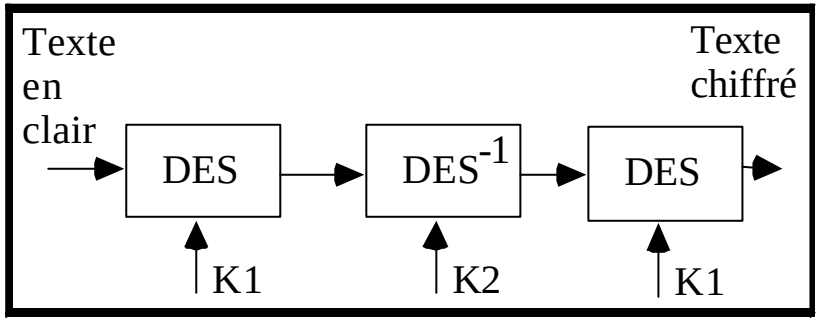
- Aucune S-Box n'est une fonction linéaire ou affine des entrées.
- Une différence d'un bit sur deux entrées d'une S-Box produit au moins deux bits différents sur les sorties
- Si un bit d'une entrée est donné et que l'on fait varier les autres bits, pour un bit de sortie donné, le nombre de cas ou il prend la valeur 0 est voisin du nombre de cas ou il prend la valeur1.

Elles sont conçues pour résister à la cryptanalyse différentielle.
Personne n'a jamais rien trouvé concernant d'éventuelles propriétés cachées des boites de substitution.

Triple DES

Utilisation de DES en cascade

Avec deux clés K1, K2 (128 bits).



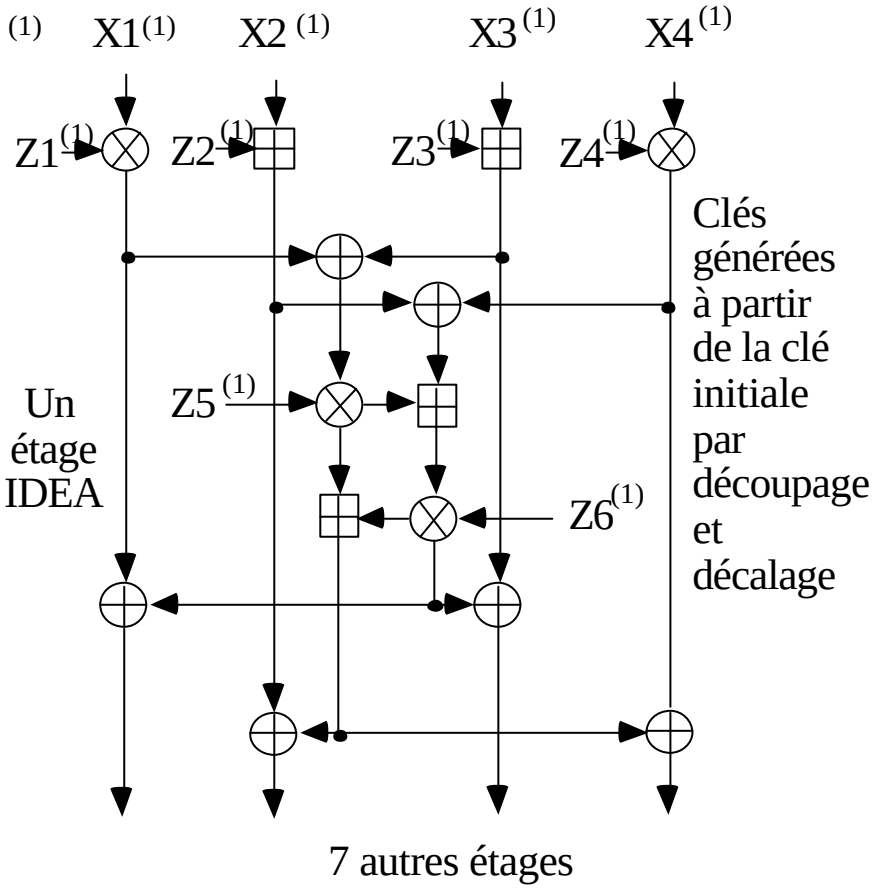
IDEA: Principes (1)

Autre solution de chiffrement par blocs de 64 bits basé sur huit étages facilement réalisable en matériel ou en logiciel.

Les opérations utilisées sont des opérations arithmétiques:

- ou exclusif $\oplus$
- addition modulo 2^{16} $\boxplus$
- multiplication modulo $2^{16}+1$ $\otimes$

IDEA: Schéma


(1) X1(1) X2 (1) X3 (1) X4 (1)
Z1(1) Z2(1) Z3(1) Z4(1)
Clés générées à partir de la clé initiale par découpage et décalage
Un étage IDEA
Z5 (1)
Z6(1)
7 autres étages

IDEA:Conclusions

- IDEA est considéré par les spécialistes comme l'un des meilleurs cryptosystème à clé privée.

- La longueur de clé est élevée (128 bits).

- La vitesse de chiffrement et de déchiffrement peut-être élevée au moyen de circuits spéciaux.
  Circuits à 55 Mb/s et 177 Mb/s
  En logiciel sur 386 33Mhz: 880 Kb/s

- Les attaques semblent difficile mais le système est assez récent

Les chiffres asymétriques

RSA: Chiffrement et déchiffrement

Chiffrement (publique)

- La clé publique est un couple d'entiers:

$$\mathbf{K = (e, n)}$$

- Le chiffrement se fait au moyen de l'élévation à la puissance e modulo n:

$$\mathbf{E_K\ (M) = M^e\ mod\ n}$$

Déchiffrement (secrète)

- La clé secrète est un couple d'entiers:

$$\mathbf{k = (d, n)}$$

- Le déchiffrement se fait au moyen de l'élévation à la puissance d modulo n:

$$\mathbf{D_k\ (M) = M^d\ mod\ n}$$

RSA :Détermination des clefs

1. Détermination de n

Trouver **deux entiers premiers** p et q très grands: **Calculer n = p q**
p et q doivent rester secrets:La sécurité du système repose sur la difficulté de factoriser
un grand entier n en deux entiers premiers p et q.
n doit avoir un longueur supérieure à 512 bits. p et q doivent vérifier diverses autres conditions.

2. Détermination de e

Calculer **z = (p-1) (q-1)**
Choisir un entier **e premier avec z.**
La clé publique est (e , n)

3. Détermination de d

Choisir un entier d tel que : **e d =1 mod z** (d inverse de e dans l'arithmétique mod z)
La clé privée est (d , n)

RSA: Inversibilité

Fonction d'Euler

Pour n entier $z = \phi(n)$ est le nombre d'entiers premiers avec n.

- si n est premier $\phi(n) = n-1$
- si $n = p.q$ avec p et q premiers

$$\phi(n) = (p-1)(q-1)$$

Théorème d'Euler

Si a et n sont premiers entre eux

$$a^{\phi(n)} \bmod n = 1$$

Pourquoi RSA marche

$$D_k(E_K(M)) = ((M)^e \bmod n)^d \bmod n$$
$$= (M^e)^d \bmod n = M^{e.d} \bmod n$$

Mais on a choisi $e.d = 1 \bmod z$

Donc il existe un entier j tel que $e.d = j\ z + 1$

$M^{e.d} = M^{j.z}\ M \bmod n = M \bmod n$

En effet d'après le théorème d'Euler:

$M^{j.z} \bmod n = (M^z)^j \bmod n = (1)^j = 1$

Exemple (B. Schneier)

1) Soit deux entiers premiers p =47,q =71

$n = p.q = 3337$

2) $z= (p-1)(q-1)= 46 . 70 = 3220$

Choisissons e = 79 (premier avec n)

3) Calcul de l'inverse de e modulo z

Une solution possible: le théorème d'Euler

$e^{\phi(n)} = e\, e^{\phi(n)-1} \bmod z = 1 \bmod z$

Donc $d = e^{-1} = e^{\phi(n)-1} \bmod z$

Numériquement $79^{78} \pmod{3220} = 1019$

4) Pour chiffrer M = 6882326879666683

Décomposons M en blocs dont la valeur est inférieure à n= 3337

=> Des blocs de 3 chiffres

M= 688 232 687 966 668 3

Chiffrer 688: $688^{79} \bmod 3337 = 1570$

E(M) = 1570 2756 2091 2276 2423 158

Déchiffrer 1570:$1570^{1019} \bmod 3337 = 688$

RSA: Calcul des nombres premiers: Algorithmes probabilistes de Miller Rabin

Tirer aléatoirement un nombre p impair; Soit m impair tel que $p=2^k m+1$,
Soit a un nombre aléatoire tel que $1 \leq a \leq p-1$; $b:=a^m \bmod m$;
Si $b \equiv 1 \bmod p$ alors test:=faux fsi
Sinon
    i:=1;test:=vrai;
    tant que $i \leq k-1$ et test:=faux
        Si $b \equiv -1 \bmod p$ alors test:=faux fsi
        Sinon
        $b:=b^2 \bmod p$
        fsi
    ftq
si test=vrai réponds p est premier sinon réponds p est décomposable fsi

Prob (p décomposable et réponds premier) £ 1/4

RSA calcul des puissances modulo n

Calcul de $z = M^e \bmod n$
On note e(i) le ième bit dans la décomposition binaire de e

$$e = \sum_{i=0}^{t-1} e(i).2^i$$

z:=1;
Pour i=t-1 à 0 faire
    z:=z^2 mod n;
    si e(i)=1 alors z:=z.M mod n fsi
fpour

Exemple

calcul de 1570^{1019} mod 3220
La représentation binaire de 1019 est 1111111011 d'ou t=10

i	e(i)	z	z^2 mod n	$z^2.M^{e(i)}$ mod n
9	1	1	1	1570
8	1	1570	2194	796
7	1	796	2923	735
6	1	735	2968	1308
5	1	1308	2320	1733
4	1	1733	3326	2752
3	1	2752	1851	2880
2	0	2880	1955	1955
1	1	1955	1160	2535
0	1	2535	2500	688

RSA: performances

L ’algorithme précédent est en O(3t) multiplications.
Multiplications sur 512 Bits= 64 multiplication en moyenne sur 32 bits. 192 multiplication pour l ’élévation à la puissance.

Utiliser des longueurs de clés de plus en plus importantes
Valeurs utilisées 512 bits, 640 bits, 1024 bits (considéré comme assez sûr pour plusieurs années)
2048 bits
Utiliser des circuits intégrés de cryptage de plus en plus performants
Actuellement une dizaine de circuits disponibles.
Vitesse de cryptage de base pour 512 bits:
de 10 à 100 Kb/s
Évolution en cours de l'ordre de 1 Mb/s

Remarque: Compte tenu de la complexité des traitements le DES est environ toujours 100 fois à 1000 fois plus rapide que le RSA.

RSA: faiblesses d ’implantation

- Ne jamais utiliser une valeur de n trop petite,
- Ne pas utiliser une clef secrète trop courte
- N'utiliser que des clefs fortes, c'est à dire telles que p-1 et q-1 ont un grand facteur premier
- Ne pas chiffrer des blocs trop courts (les compléter toujours a n-1 bits), de façon à détruire toute structure syntaxique
- Ne pas utiliser un n commun à plusieurs clefs, si ces clefs peuvent être utilisées pour chiffrer un même message.
- Si une clef secrète (d,n) est compromise, ne plus utiliser les autres clefs utilisant n comme modulo
- Ne jamais chiffrer ou authentifier un message provenant d'un tiers sans le modifier (ajouter quelques octets aléatoires par exemple)

La nécessité des clefs fortes est un point discuté.

RSA: Cryptanalyse

On montre que le calcul d ’une des clefs à partir de l ’autre est équivalent au problème de la factorisation de n

On n ’a pas encore montré que la cryptanalyse du RSA est équivalente au problème de la factorisation

Complexité temporelle du meilleur algorithme séquentiel de factorisation (crypte algébrique)

$$O(e^{1,92+o(1)(\log(n)^{1/3}(\log\log(n))^{2/3}})$$

Actuellement un calcul en parallèle utilisant quelques milliers d'ordinateurs pendant quelques mois permet de factoriser des nombres d'une centaine de chiffres (400 bits)
Utiliser des n=1024 ou 2048 bits selon protection cherchée est de moins ou plus de cinq ans.
Prévoir un moyen pour augmenter cette valeur par sur chiffrement ou déchiffrement suivi d'un rechiffrement.

RSA cartes bancaires

Limitation des calculs du fait de la puissance de calcul disponible.

n sur 320 bits (de l'ordre de 95 chiffres)

clé publique 3 pour tout le monde

RSA: Conclusions

Solution assez générale.

Utiliser le RSA brièvement au début d'un échange
pour échanger des clés symétriques de session
d'un algorithme efficace

Efficacité en sécurité
La méthode est officiellement sûre si l'on respecte
certaines contraintes de longueur de clés et d'usage.
Personne depuis 2500 ans n'a trouvé de solution rapide
au problème de la factorisation ...

Bases théoriques de la cryptographie asymétriques

La cryptographie asymétrique n ’est jamais inconditionellement sûre (chiffre parfait): Estelle peut toujours faire une attaque exhaustive en utilisant la clef publique.

Théorie de la complexité calulatoire de la cryptanalyse

Complexité algorithmique

Nom du problème	Enoncé	Complexité
Factorisation	Soit n=p.q ou p et q sont deux entiers premiers et très grands, vérifiant quelques propriétés qui sont précisées dans la présentation du RSA. Trouver p et q connaissant n	NP Super polynomial
Extraction des racines dans un anneau non intègre	Soit n=p.q ou p et q sont deux entiers premiers et très grands, vérifiant quelques propriétés qui sont précisées dans la présentation du RSA. Soit $b \in (0..n-1)$, Trouver $x \in (0..n-1)$ tel que $b=x^t \bmod n$	NP Super polynomial
Logarithme discret	Soit p un nombre premier très grand tel que p-1 a un grand facteur premier soit $g \in (0..p-1)$ tel que $\forall y \in (1,..p-2)\ g^y \neq 1 \bmod p$, soit $b \in (0..p-1)$ Trouver $x \in (1,..p-2)$ tel que $g^x=b \bmod p$ n. b. On montre que g est un élément primitif du groupe multiplicatif Z/Zp, c'est à dire que les puissances de g modulo p engendrent (1,..p-1). Donc le problème précédent a une solution.	NP Super polynomial
Isomorphie de deux graphes	Soit G(X,U) et G'(X,U') deux graphes isomorphes. Trouver la permutation permettant de passer de G à G'. n. b. X est un ensemble d'entier (sommets du graphe). Un élément de U ou de U' (arc du graphe) est un couple (a,b) d'éléments de X. Le problème consiste à trouver une permutation π de X tel que la fonction qui a $(a,b) \in U$ fait correspondre $(\pi(a),\pi(b))$ soit une bijection de U dans U'.	NP-complet Exponentiel
Problème du sac à dos	Soit x un nombre et $X=\{x_1, x_2,..x_n\}$ un ensemble de nombres. Trouver un sous-ensemble S de X tel que $x = \sum_S x_i$	NP-complet Exponentiel

Fonctions à sens unique

C'est une fonction f(M) facile à calculer
mais telle qu'il est extrêmement difficile de déduire M de f(M).

Exemple:

Calcul modulo n (dans un anneau fini)
M^2 est facile à calculer modulo n (M^e).
$\sqrt{M}$ est difficile à calculer (log M).

Fonction à sens unique avec brèche secrète

C'est une fonction f(M) facile à calculer telle qu'il est extrêmement difficile de déduire M sauf si l'on connaît un secret K.
Deux exemples utilisés en pratique:
• Problème de la factorisation (RSA),
n=pxq, p et q sont premier, e est défini comme dans le RSA et public
$f(M)= M^e \bmod n$,
brèche connaissance de p ou q
• Problème du logarithme discret (El Gammal)
p est premier, a est un élément primitif de Z^p, $b= a^x \bmod p$, k est quelconque,
p, a, b sont publics, $a^k \bmod p$ est connu
$f(M)= M. b^k \bmod p$,
brèche connaissance de x
En effet $1/b^k = 1/(a^k)^x$

Fonctions basées sur la théorie de la complexité

Algorithme basé sur le sac à dos
Cassé car la brèche montrait que le problème de
l ’inversion de f était un cas polynomial d ’un problème
NP complet.

Echec sauf sur les algorithmes probabilistes (A apport nul de connaissances)

Fonction de hachage

Une fonction de hachage h est une fonction qui à un message M
de longueur quelconque fait correspondre un message H(M)
(notée aussi $\{M\}^H$) de longueur constante.
L'intérêt d'une fonction de hachage est que M peut être arbitrairement grand alors que H(M) a une longueur donnée.
Terminologie: Résumé, fonction de contraction,
digest, empreinte digitale, …

Exemple: Hasch codes des systèmes de fichiers, codes détecteurs d 'erreurs

Fonction de hachage sécuritaire

f(M) telle que f est une fonction de hachage par rapport à M

f est à collision faible difficile: il est calculatoirement difficile de trouver M significatif tel que f(M)=K

f est à collision forte difficile:il est calculatoirement difficile de trouver M et M’ tel que f(M)=f(M ’)

Elle est avec clef si son calcul dépend d ’une information secrète la clef K

MD5: Principes (1)

Une fonction de hachage à sens unique.qui génère une signature sur 128 bits.

Le message est décomposé en blocs de 512 bits soient 16 sous-blocs
Mj de 32 bits.
Pour chaque bloc de 512 bits on réalise 4 séries de 16 applications
successives des fonctions de base FF, GG , HH, II qui dépendent des sous-blocs Mj
et de constantes a, b, c, d,

$$FF(a,b,c,d,Mj,s,ti) \longrightarrow a = b + ((a = F(b,c,d) + Mj + ti) \lhd s)$$

$$GG(a,b,c,d,Mj,s,ti) \longrightarrow a = b + ((a = G(b,c,d) + Mj + ti) \lhd s)$$

$$HH(a,b,c,d,Mj,s,ti) \longrightarrow a = b + ((a = H(b,c,d) + Mj + ti) \lhd s)$$

$$II(a,b,c,d,Mj,s,ti) \longrightarrow a = b + ((a = I(b,c,d) + Mj + ti) \lhd s)$$

Dans les formules précédentes $\angle$s désigne un décalage à gauche de s positions

MD5 Principes (2)

Les fonctions F,G,H,I sont données par:

$$F(X,Y,Z)=(X \wedge Y) \vee (\neg X \wedge Z)$$
$$G(X,Y,Z)=(X \wedge Z) \vee (Y \wedge \neg Z)$$
$$H(X,Y,Z)=(X \oplus Y \oplus Z)$$
$$I(X,Y,Z)=Y \oplus (X \vee \neg Z)$$

Signature

Une signature manuscrite idéale est réputée posséder les propriétés suivantes:

- La signature **ne peut-être imitée.**
Elle prouve que le signataire a délibérément signé le document.

- La signature **authentifie** le signataire.
Seul le signataire peut avoir signé.

- La signature appartient à un seul document (elle **n'est pas réutilisable**).

- Le document signé ne peut être partiellement ou totalement **modifié**.

- La signature ne peut-être **reniée**.

-La signature peut être **contrôlée**

Signature Numérique

Base de la signature numérique:une fonctions de hachage H sécuritaire et d ’une fonction à sens unique f avec brèche.

La signature est composée de $f^{-1}(H(M))$

Seul le signataire sait calculer f^{-1}
Tout le monde peut calculer H et f et donc pour M donné vérifier la signature

Si H est a collision faible, on ne pourra pas coller une signature sur un document à créer

Signature El Gamal

Clef publique d ’Alice:
p premier, $g<p$, $y=g^x \bmod p$

Clef privée d ’Alice
$x<p$

Signature de M par Alice
choisir k tel que k et p-1 soient premiers entre eux
calculez $a=g^k \bmod p$ et b tel que $M=(xa+kb) \bmod p-1$
a,b sont la signature de M par Alice

Vérification par Bob
$y^a a^b \bmod p=g^M \bmod p$

Exemple (Schneier)

Clef publique, p=11, g=2
Clef privée x=8<11
Publique $y=2^8 \bmod 11=3$

Signature de M=5
Choix de k=9 aléatoire et premier avec 10=11-1
$a=2^9 \bmod 11=6$
Recherche de b tel que $M=5=(8 \times 6+9 \times b) \bmod 10$
soit b=3 ($48+27=75 \equiv 5 \bmod 10$)
contrôle $3^6 6^3 \bmod 11=2^5 \bmod 11=10$

Validité de la signature

Pour signer à la place d ’Alice il faut trouver x tel que
$y=g^x \bmod p$ donc résoudre le problème du logarithme discret

Pour signer M ’ de tel façon que signature(M)=signature (M ’)
On doit avoir:
$y^a a^b \bmod p = g^{M'} \bmod p$
donc résoudre le problème du logarithme discret

Validité du contrôle

$y^a \bmod p = (g^x)^a \bmod p = g^{xa} \bmod p$

$a^b \bmod p = g^{kb} \bmod p$

$y^a . a^b \bmod p = g^{(xa+kb)} \bmod p$

Or

$g^M \bmod p = g^{(s(p-1)+xa+kb)} \bmod p = g^{(s(p-1)+xa+kb)} \bmod p$

$= g^{(s(p-1))} \bmod p \cdot g^{(xa+kb)} \bmod p = g^{(xa+kb)} \bmod p$

(théorème d ’Euler)

Génération de nombres pseudo aléatoires sécuritaires

Problème important:
Pour créer des nonces
Pour générer des clefs

Propriété attendue

Quelque soit l ’observation du pirate il ne peut
acquérir de l ’information sur le nombre qui va être généré

Formalisation

Suite Pseudo aléatoire:
Il s ’agit d ’une suite de nombres $X_0,X_1,...$
X_0 , S_0 grain
$0<X_i<N$
$X_n=f(X_{n-1},S_{n-1})$
$S_n=g(X_{n-1}, S_{n-1})$

Tout test statistique fait accepter l ’hypothèse
« X est une suite de nombres uniformément répartis dans 0,N »
ou
« $Prob(X_n/X_0, X_1, \ldots X_{n-1})=Prob(X_n) =1/N$ »

Suite Pseudo aléatoire sécuritaire

Propriété pas suffisante pour la sécurité:
Les X sont transmis, éventuellement en clair, les S restent cachés
il faut qu ’un pirate qui a observé $X_0,….,X_{n-1}$ ne puisse en déduire X_n
Deux solutions:
1) La suite est aléatoire (bruit thermique d ’une résistance)
2) Le grain est le plus aléatoire possible (fonction de la vitesse de frappe au clavier, d ’un nombre d ’interruption…) et
la fonction de s donnée par a=f(b,s) doit être à sens unique

Exemple ANSI X9.17

Choisir une clef K pour le DES et X_0 imprévisibles et secrets,
T_n est la date courante
$S_n=E_k(E_k(T_n)+X_{n-1})$
$X_n=E_k(E_k(T_n)+S_n)$

Bibliographie

S.Natkin Les protocoles de sécurité de l'Internet, Dunod 2002

J. Stern- La science du secret Ed Odile Jacob 1998

A.S. Tannenbaum - Computer Networks Prentice Hall

D. Stinson - Cryptographie, Théorie et pratique, Thomson Publishing International France

B. Schneier - Cryptographie appliquée Thomson Publishing International France

D.E. Denning - Cryptography and data security Addison Wesley 1982