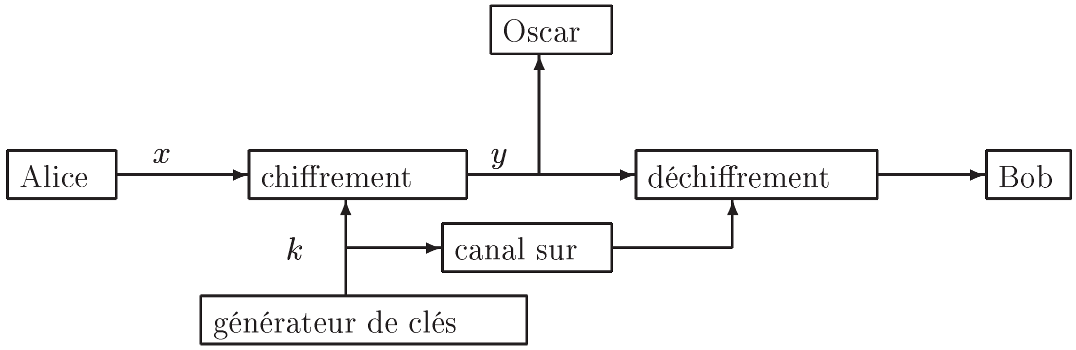
Définition d'un système cryptographique



Le tuple $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ est un système cryptographique si :

$\mathcal{P}$:	Ensemble des textes clairs ;
$\mathcal{K}$:	Ensemble des clés ;
$\mathcal{C}$:	Ensemble des textes chiffrés ;
$\mathcal{E}$:	Ensemble des règles de chiffrement pour les clés de $\mathcal{K}$;
$\mathcal{D}$:	Ensemble des règles de déchiffrement pour les clés de $\mathcal{K}$;
Et :	$\forall k \in \mathcal{K}, \exists e_k \in \mathcal{E}, \exists d_k \in \mathcal{D}, \forall x \in \mathcal{P}$, $d_k(e_k(x)) = x$.

La cryptanalyse

principe de Kerckhoff : Oscar connait le système cryptographique utilisé.

but : Déterminer la clé utilisée.

Les attaques :
- Texte chiffré connu : Oscar ne connait que la chaine du message chiffré.
- Texte clair connu : Oscar dispose d'un texte clair et du texte chiffré correspondant.
- Texte clair choisi : Oscar a accès à une machine chiffrante.
- Texte chiffré choisi : Oscar a temporairement accès à une machine déchiffante.

Typologie des systèmes

Clé privée/clé publique :
- clé privée : la totalité de la clé est communiqué en secret (Chiffrement par substitution, de Hill, de Vigénère, le DES,...) ;
- clé publique : une partie de la clé est communiquée en secret tandis que l'autre est communiquée en publique (RSA, chiffrement de Rabin,...).

Chiffrement par bloc/en chaine :
- par bloc : la clé ne varie pas au cours du chiffrement ;
- en chaine : la clé varie au cours du chiffrement.

Monoalphabétique/polyalphabétique :
- monoalphabétique : pour un caractère clair, un caractère chiffré ;
- polyalphabétique : pour un caractère clair, plusieurs caractères chiffrés ;

Système idempotent ou non

Chiffrement en chaine

Le tuple $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{L}, \mathcal{F}, \mathcal{E}, \mathcal{D})$ est un système cryptographique en chaine si :

$\mathcal{P}$:	Ensemble des textes clairs ;
$\mathcal{K}$:	Ensemble des clés ;
$\mathcal{C}$:	Ensemble des textes chiffrés ;
$\mathcal{L}$:	Alphabet de séquence de clés ;
$\mathcal{F}$:	$(f_1, f_2, \ldots)$ générateur de séquence : $\forall i \leq 1, f_i : \mathcal{K} * \mathcal{P}^{i-1} \to \mathcal{L}$;
$\mathcal{E}$:	Ensemble des règles de chiffrement pour les clés de $\mathcal{L}$;
$\mathcal{D}$:	Ensemble des règles de déchiffrement pour les clés de $\mathcal{L}$;
Et :	$\forall z \in \mathcal{L}, \exists e_z \in \mathcal{E}, \exists d_z \in \mathcal{D}, \forall x \in \mathcal{P}$, $d_z(e_z(x)) = x$.

Si la séquence ne dépend que de la clé : système synchrone.

Si $\forall i \geq 1, z_i = z_{i+d}$: système périodique.

rem.: Si $\forall i \geq 1, z_i = K$: chiffrement par bloc.

Système cryptographique produit

Principe : combiner les systèmes cryptographiques.

but : augmenté la sécurité des systèmes.

Soient $S_1 = (\mathcal{P}, \mathcal{P}, \mathcal{K}_1, \mathcal{E}_1, \mathcal{D}_1)$ et $S_2 = (\mathcal{P}, \mathcal{P}, \mathcal{K}_2, \mathcal{E}_2, \mathcal{D}_2)$ deux systèmes cryptographiques. Le système $S = (\mathcal{P}, \mathcal{P}, \mathcal{K}_1 * \mathcal{K}_2, \mathcal{E}, \mathcal{D})$ défini par

$$\begin{array}{l} \forall k = (k_1, k_2) \in \mathcal{K}_1 * \mathcal{K}_2, \forall x, y \in \mathcal{P} \\ e_{(k_1,k_2)}(x) = e_{k_2}(e_{k_1}(x)), \\ d_{(k_1,k_2)}(y) = d_{k_1}(d_{k_2}(y)) \end{array}$$

est le système produit (noté $S_1 * S_2$).

S^n est le système cryptographique itéré.

Un système S est idempotent si $S^2 = S$.

Notions d'arithmétique modulaire

$a \; mod \; m$ est le reste de la division entière de a par m ($0 \leq a \; mod \; m \leq m-1$).

$a \equiv b (mod \; m)$ si m divise $(b-a)$.

lem.: $a \equiv b (mod \; m)$ ssi $a \; mod \; m = b \; mod \; m$.

Exemple : $143 \; mod \; 5$? $-18 \; mod \; 7$?

pgcd est le plus grand commun diviseur.

$\mathbb{Z}_m = \{0, \ldots, m-1\}$
$x \; op_m \; y : x \; op \; y \; mod \; m$ avec $op \in \{+, -, *\}$

La fonction indicatrice d'Euler $\phi(m)$ est définie par le nombre d'entiers de $\mathbb{Z}_m$ qui sont premiers avec m.

Soit $a \in \mathbb{Z}_m$, $a^{-1} \in \mathbb{Z}_m$ est l'inverse de a si $a *_m a^{-1} \equiv a^{-1} *_m a \equiv 1 (mod\ m)$.

Th.: Un nombre a admet un inverse dans $\mathbb{Z}_m$ si et seulement si $pgcd(a, m) = 1$ (i.e. a et m sont premiers entre-eux).

Algo. d'Euclide : Le plus grand commun diviseur de deux nombres b et a ($b > a$) est donné par la définition récursive suivante :

$$pgcd(a, b) = \begin{cases} a \text{ si } b\ mod\ a = 0 \\ pgcd(b\ mod\ a, a) \text{ sinon} \end{cases}$$

Algo. d'Euclide étendu : L'inverse de x dans $\mathbb{Z}_m$ si il existe est $x_m^{-1} = inverse(x, m, 0, 1, m)$ avec :

$$inverse(u, v, t, t', m)$$
$$\begin{cases} t' \text{ si } v\ mod\ u = 0 \text{ et } u = 1 \\ \perp \text{ si } v\ mod\ u = 0 \text{ et } u \neq 1 \\ inverse(v\ mod\ u, u, t', (t - (v\ div\ u) * t')\ mod\ m, m) \end{cases}$$

Notions de probabilité

Notation : $\mathcal{X}$ un espace d'événements, X une distribution de probabilités sur $\mathcal{X}$ et $Pr_{\mathcal{X}}(x)$ la probabilité d'un événement x suivant X.

Soient X et Y deux ensembles d'événements différents.
La probabilité mutuelle $Pr_{(\mathcal{X},\mathcal{Y})}(x, y)$: probabilité que x et y soient réalisés simultanément.
La probabilité conditionnelle $Pr_{\mathcal{X}}(x|y)$: probabilité de x sachant que y est réalisé.

$$Pr(x, y)_{(\mathcal{X},\mathcal{Y})} = Pr_{\mathcal{X}}(x|y)Pr_{\mathcal{Y}}(y)$$

Th.: (Théorème de Bayes) Si $Pr_{\mathcal{Y}}(y) > 0$ alors

$$Pr_{\mathcal{X}}(x|y) = \frac{Pr_{\mathcal{X}}(x)Pr_{\mathcal{Y}}(y|x)}{Pr_{\mathcal{Y}}(y)}$$

cor.: Deux distributions X et Y sont indépendantes si et seulement si

$$Pr_{\mathcal{X}}(x|y) = Pr_{\mathcal{X}}(x), \forall x \in \mathcal{X}, \forall y \in \mathcal{Y}$$

Probabilité et cryptographie

$C(k) = \{e_k(x), x \in \mathcal{P}\}$

Probabilité d'avoir un texte chiffré y :

$$Pr_{\mathcal{C}}(y) = \Sigma_{k/y \in C(k)} Pr_{\mathcal{K}}(k) Pr_{\mathcal{P}}(d_k(y))$$

Probabilité d'avoir un texte chiffré y sachant que le texte clair est x :

$$Pr_{\mathcal{C}}(y|x) = \Sigma_{k/x \in d_k(y)} Pr_{\mathcal{K}}(k)$$

Probabilité d'avoir un texte clair x sachant que le texte chiffré est y :

$$Pr_{\mathcal{P}}(x|y) = \frac{Pr_{\mathcal{P}}(x) Pr_{\mathcal{C}}(y|x)}{Pr_{\mathcal{C}}(y)}$$

Un système cryptographique assure une confidentialité parfaite si

$$\forall x \in \mathcal{P}, \forall y \in \mathcal{C}, Pr_{\mathcal{P}}(x|y) = Pr_{\mathcal{P}}(x)$$

Probabilité et cryptographie (suite)

Th.: Soit le système cryptographique $S = \{\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D}\}$, $|\mathcal{P}|=|\mathcal{C}|=|\mathcal{K}|$. S assure une confidentialité parfaite si et seulement si
$\forall k \in \mathcal{K}, Pr_{\mathcal{K}}(k) = \frac{1}{|\mathcal{K}|}$ et
$\forall x \in \mathcal{P}, \forall y \in \mathcal{C}, \exists! k \in \mathcal{K} / e_k(x) = y$.

Exemple : Soient $\mathcal{P} = \{a, b\}$ avec $Pr_{\mathcal{P}}(a) = \frac{1}{4}$ et $Pr_{\mathcal{P}}(b) = \frac{3}{4}$; $\mathcal{K} = \{k_1, k_2, k_3\}$ et $Pr_{\mathcal{K}}(k_1) = \frac{1}{2}$, $Pr_{\mathcal{K}}(k_2) = \frac{1}{4}$, $Pr_{\mathcal{K}}(k_3) = \frac{1}{4}$; $\mathcal{C} = \{1, 2, 3, 4\}$.

$e_k(x)$	k_1	k_2	k_3
a	1	2	3
b	2	3	4

Calculer $\forall x \in \mathcal{P}, \forall y \in \mathcal{C}, Pr(x|y)$?

Chiffrement par substitution

Algo. de chiffrement par substitution :

$$\begin{array}{l} \mathcal{P} = \mathcal{C} = \mathbb{Z}, \mathcal{K} = \{\pi/\pi \text{ permutation sur } \mathbb{Z}\}, \\ \forall \pi \in \mathcal{K}, x, y \in \mathbb{Z}, (\pi^{-1} \circ \pi = \pi \circ \pi^{-1} = id), \\ e_\pi(x) = \pi(x), \\ d_\pi(y) = \pi^{-1}(y). \end{array}$$

Propriétés : par bloc, monoalphabétique, à clé privée, idempotent et $|\mathcal{K}| = 26! > 4 * 10^{26}$.

Attaque : fréquence des lettres.

Exemple : Déchiffrement de

$$\begin{array}{rl} y = & RUZVFSMLXCMZVQFDHUJLF \\ & UCAHVYFUCVHVBFZSMXZSHV \end{array}$$

par la substitution :

$$\begin{array}{ccccccccccccc} a & b & c & d & e & f & g & h & i & j & k & l & m \\ X & N & Y & A & H & P & O & G & Z & Q & W & B & T \\ n & o & p & q & r & s & t & u & v & w & x & y & z \\ S & F & L & R & C & V & M & U & E & K & J & D & I \end{array}$$

Chiffrement par substitution (suite)

lem.: Le système de chiffrement par substitution offre une confidentialité parfaite.

Algo. de chiffrement affine :

$$\mathcal{P} = \mathcal{C} = \mathcal{K} = \{(a,b) \in \mathbb{Z} * \mathbb{Z} / pgcd(a, 26) = 1\},$$
$$\forall k = (a,b) \in \mathcal{K}, x, y \in \mathbb{Z},$$
$$e_k(x) = ax + b \; mod \; 26,$$
$$d_k(y) = a^{-1}(y - b) \; mod \; 26.$$

Attaque : recherche exhaustive de la clé ($|\mathcal{K}| = 26 * \phi(26) = 312$).

Chiffrement par décalage : $a = 1$.

Exemple : Déchiffrement par décalage ($b = 11$) :

$$y = \begin{array}{l} ZSNZXMTPYOPXLCTYDN \\ ZXMTPYOPNLATELTYPD \end{array}$$

Chiffrement de Hill

Algo. de chiffrement de Hill :

$$\mathcal{P} = \mathcal{C} = (\mathbb{Z})^m,$$
$$\mathcal{K} = \{\text{matrices } m * m \text{ inversibles dans } \mathbb{Z}\},$$
$$\forall K \in \mathcal{K}, x, y \in (\mathbb{Z})^m,$$
$$e_K(x) = xK,$$
$$d_K(y) = yK^{-1}$$

Remarque : une matrice de $\mathbb{Z}_m$ est inversible si $pgcd(det\ K, m) = 1$.

Propriétés : par bloc, polyalphabétique, idempotent et à clé privée.

Exemple : Chiffrer puis déchiffrer $x = et$ avec $K = \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}$, $K^{-1} = \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix}$

Chiffrement de Hill (suite)

Chiffrement par permutation :

$$\mathcal{K} = \{\pi/\pi \text{ permutation sur } \mathbb{Z}_m\},$$
$$\forall \pi \in \mathcal{K}, x = x_1 \dots x_m, y = y_1 \dots y_m \in \mathbb{Z}^m,$$
$$(\pi^{-1} \circ \pi = \pi \circ \pi^{-1} = id),$$
$$e_\pi(x) = x_{\pi(1)} \cdots x_{\pi(m)},$$
$$d_\pi(y) = y_{\pi^{-1}(1)} \cdots y_{\pi^{-1}(m)}.$$

$$K_\pi = (k_{ij})/k_{ij} = \begin{cases} 1 & \text{si } i = \pi(j) \\ 0 & \text{sinon} \end{cases}$$

Chiffrement de Vigénère ($XVI^{ème}$) et de Vernam (1917)

Algo. de chiffrement de Vigénère :

$$\begin{aligned}
&\mathcal{P} = \mathcal{C} = \mathcal{K} = (\mathbb{Z})^m, \\
&\forall K, x, y \in (\mathbb{Z})^m, \\
&K = k_1 \ldots k_m, x = x_1 \ldots x_m, y = y_1 \ldots y_m, \\
&e_K(x) = (x_1 +_{26} k_1) \ldots (x_m +_{26} k_m) \ (\ mod\ m), \\
&d_K(y) = (y_1 -_{26} k_1) \ldots (y_m -_{26} k_m) \ (\ mod\ m).
\end{aligned}$$

Propriétés : en chaine périodique de période m, polyalphabétique, à clé privée, idempotent et $|\mathcal{K}| = 26^m$.

Algo. de chiffrement de Vernam :

$$\begin{aligned}
&\mathcal{P} = \mathcal{C} = \mathcal{K} = (\mathbb{Z}_2)^m, \\
&\forall x, y, k \in (\mathbb{Z}_2)^m, e_k(x) = x \oplus k, d_k(y) = y \oplus k,
\end{aligned}$$

lem.: Les systèmes de chiffrement de Vigénère et de Vernam offrent une confidentialité parfaite.

Standard de Chiffrement de Données : DES

DES : Data Encryption Standard
- 1973 : appel d'offre du National Bureau of Standards ;
- 1975 : publication du DES (modification de LUCIFER d'IBM) ;
- 1977 : adoption comme standard.
- révisé tous les 5 ans.
- fin probable : 1998

Algorithme du DES L'algorithme du DES prend en entrée un texte clair de 64 bits, une clé de 64 bits (dont les bits terminaux de chaques octets sont des bits de parité pour le contrôle des erreurs) et calcule un texte crypté sur 64 bits.

Algorithme général du DES

$DES(x : texte\ 64 bits, K : clé\ 64 bits) : 64 bits$
$L_0 R_0 = IP(x), (|L_0| = |R_0| = 32)$
Pour $i = 1$ à 16
$L_i = R_{i-1}$
$R_i = L_{i-1} \oplus f(R_{i-1}, T_i(K))$
finPour
résultat $IP^{-1}(R_{16} L_{16})$

$f(r : 32 bits, k : 48 bits) : 32 bits$
$B = Exp(r) \oplus k = B_1 \ldots B_8, (|B_i| = 6)$
Pour $i = 1$ à 8
$B_i = b_1 \ldots b_6$
$C_i = S_i(b_1 b_6, b_2 b_3 b_4 b_5)$
finPour
résultat $P(C_1 \ldots C_8)$

Diversification de la clé

Principe : la clé subit une permutation, une série de rotations circulaires “par partie” puis une permutation inverse.

Algo. de diversification de la clé Les fonctions LS_j, $1 \leq j \leq 16$ sont des rotations circulaires vers la gauche d'un bit pour les indices 3, 4, 5, 6, 7, 8, 10, 11, 12, 13, 14 et 15, et de deux bits pour les indices 1, 2, 9 et 16.

$T_i(k : 64bits) : 48bits$
  $k' = ote\_bits\_de\_parite(k)$
  $C_0D_0 = PC\text{–}1(k'), (|C_0|{=}|D_0|{=}\ 28)$
  Pour $j = 1$ à i
    $C_j = LS_j(C_{j-1})$
    $D_j = LS_j(D_{j-1})$
  finPour
  résultat $PC\text{–}2(C_i, D_i)$

rem.: Les fonctions de permutation $T_i(K), 1 \leq i \leq 16$ sont calculables à l'avance.

Modes d'utilisation du DES

ECB (electronic codebook mode) :
mode courant ;

IV : une valeur initiale arbitraire.

CBC (cipher block chaining mode) :

$CBC(x_1, x_2, \ldots : 64 bits)$
bloc initial $y_0 = IV$
Tantqu'il y a des blocs de texte clair x_i
$y_i = DES(y_{i-1} \oplus x_i)$
finTantque

$CBC^{-1}(y_1, y_2, \ldots : 64 bits)$
bloc initial $y_0 = IV$
Tantqu'il y a des blocs de texte chiffré y_i
$x_i = y_{i-1} \oplus DES^{-1}(y_i)$
finTantque

Modes d'utilisation du DES (suite)

OFB (output feedback mode) :
Chiffrement en chaîne synchrone

$OFB = (x_1, x_2, \ldots : 64bits)$
bloc initial $z_0 = IV$
Tantqu'il y a des blocs de texte clair x_i
$z_i = DES(z_{i-1})$
$y_i = z_i \oplus x_i$
finTantque

$OFB^{-1}(y_1, y_2, \ldots : 64bits)$
bloc initial $z_0 = IV$
Tantqu'il y a des blocs de texte chiffré y_i
$z_i = DES(z_{i-1})$
$x_i = z_i \oplus y_i$
finTantque

Modes d'utilisation du DES (suite)

CFB (cipher feedback mode) :

$CFB = (x_1, x_2, \ldots : 64 bits)$
initial bloc $y_0 = IV$
Tantqu'il y a des blocs de texte clair x_i
$z_i = DES(y_{i-1})$
$y_i = z_i \oplus x_i$
finTantque

$CFB^{-1}(y_1, y_2, \ldots : 64 bits)$
bloc initial $y_0 = IV$
Tantqu'il y a des blocs de texte chiffré y_i
$z_i = DES(y_{i-1})$
$x_i = z_i \oplus y_i$
finTantque

Systèmes à clés publiques

Pr.: Rendre impossible la construction de la clé de déchiffrement à partir de la clé de chiffrement.
- clé publique de chiffrement,
- clé privé de déchiffrement.

Rivest, Shamir et Adleman :(1977) factorisation des grands nombres ;

Rabin : factorisation des grands nombres ;

Merkle-Hellman : problème du sac-à-dos ;

McEliece : théorie algébrique des codes ;

ElGamal : logarithme discret dans un corps fini ;

Chor-Rivest : problème du sac-à-dos.

Le système RSA

Construction du système par Bob :
- Choix de 2 grands nombres premiers p et q ;
- calcul de $n = pq$ et de $\phi(n) = (p-1)(q-1)$;
- choix d'un b tel que $pgcd(b, \phi(n)) = 1$;
- calcule de $a = b^{-1}\ mod\ \phi(n)$;
- publication de b et n.

Chiffrement de x par Alice :
$e_K(x) = x^b\ mod\ n$

Déchiffrement de $y = e_K(x)$ par Bob :
$d_K(y) = y^a\ mod\ n$

Clé : (n, p, q, a, b)
- clés publiques : n et b,
- clés privées : p, q et a.

Le système RSA

Algo. $square - and - multiply$ pour le calcul de y dans $y = x^c \ mod \ n = sm(x, c, n, |c|, 1)$ avec $|c| = l$ le nombre de bits de la représentation binare de c et $bin(c, i)$ le $i^{ème}$ bit de c.

$$sm(x, c, n, l, z)$$
$$\begin{cases} z \text{ si } l = 0 \\ sm(x, c, n, l-1, (z2 * x \ mod \ n)) \text{ si } bin(c, l) = 1 \\ sm(x, c, n, l-1, z2) \text{ sinon} \end{cases}$$

sachant que $z2 = z^2 \ mod \ n$.

Exemple : $p = 101$, $q = 113$, $x = 9726$.