

Th 1 info

Cryptographie symétrique

La sécurité parfaite est-elle possible ?

asymétrique (à clé publique) E_K (publique)

$$\begin{array}{l} m \rightarrow c = E_K(m) \\ m \xrightarrow{K} D_K(c) = m \end{array}$$

On a besoin de la longueur de la clé aussi grand que $H(m) =$ nombre de bits du message.

Ex. $K \in \mathbb{F}_2^m$, $p(K) = \frac{1}{2^m}$ alors $H(K) = m$ $\rightarrow H(K)$ car K a une proba uniforme

masque jetable (One-time pad)

- Chiffrement de Vigenère (16^{si}) $\leftarrow$ 19^{si} Kasiski casse le point faible

- Chiffrement de Vernam (20^{si})

$\rightarrow$ idée que la clé doit être aussi longue que le message

On suppose $M = m_1 \dots m_n$ est un message et $K = k_1 \dots k_n$ une clé aussi longue que le message.

On peut supposer (pas nécessaire pour la sécurité) que $m_i \in \mathbb{F}_2$ et $k_i \in \mathbb{F}_2$

Chiffrement:

$$\begin{array}{c} m_1 m_2 \dots m_n \\ \oplus k_1 k_2 \dots k_n \\ \hline \end{array} \quad \left. \begin{array}{l} \oplus = \text{add dans } \mathbb{F}_2 \text{ ou } \mathbb{Z}/q\mathbb{Z} \text{ en général} \end{array} \right\}$$

Dechiffrement:

$$\begin{array}{c} c_1 c_2 \dots c_n \\ \oplus k_1 k_2 \dots k_n \\ \hline \end{array} \quad \left. \begin{array}{l} \text{NB } \ominus = \oplus \text{ si } q=2; q=26 \text{ était le crypte} \\ \text{seul de Vigenère} \end{array} \right\}$$

Pour le masque jetable, on a la sécurité parfaite

(le masque jetable est parfaitement sûr) ss.:

- Les bits de la clé $K = k_1 \dots k_n$ sont choisis de manière aléatoire et indépendantes

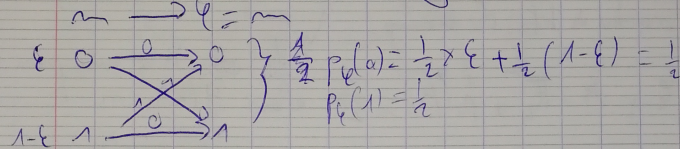
- or ne utilise jamais la clé.

Preuve (idic):

On peut supposer que $K = m = A^m = (\mathbb{Z}/q\mathbb{Z})^m = \mathbb{F}$

On peut réduire au cas $m=1$

$(K) \times m \xrightarrow{\oplus} \mathbb{F}$
 (uniforme) $(p,q=2)$ XOR $\rightarrow$ uniforme aussi $\mathbb{F}$
 Propriété de Shannon



Vigenère: $A = \{A, B, \dots, Z\} = \mathbb{Z}/26\mathbb{Z}$

(16/2)

Table d'addition: décalages

	A	B	C	...	Z
0 = A	A	B	C	...	Z
1 = B	B	C	D	...	A
2 = C	C	D	E	...	B
...	...	...	...	...	...
25 = Z	Z	A	B	...	Y

	P	E	A	C	E
0	L	O	V	E	L
1	Z	S	V	G	P

Algorithme / cryptosystème AES (2001?)

(a remplace DES (1976))

AES = itération plusieurs fois (~ 16) de quatre fonctions:
 Pour un message de 128 bits $\in \mathbb{F}_2^{128}$ écrit en forme de matrice des octets

$A \in \mathbb{F}_2^8 \times \mathbb{F}_2^8$

$$A = \begin{pmatrix} a_{00} & \dots & a_{05} \\ \vdots & & \vdots \\ a_{50} & \dots & a_{55} \end{pmatrix}$$

a) Shift Rows:

$$A \rightarrow \begin{pmatrix} a_{00} & a_{01} & a_{02} & a_{03} \\ a_{10} & a_{11} & a_{12} & a_{13} \\ a_{20} & a_{21} & a_{22} & a_{23} \\ a_{30} & a_{31} & a_{32} & a_{33} \end{pmatrix}$$

Chiffre et classique par transposition

b) Sub Bytes

On applique une substitution $(A \rightarrow A)$
 $b_{ij} = S(a_{ij})$ $S(a) = a^{-1}$ dans $\mathbb{F}_2^8$
 0 si $a = 0 \dots 0$

c) Mix columns

$$A = (v_0, v_1, v_2, v_3) \rightarrow T(v_0, v_1, v_2, v_3)$$

où $v_j = \begin{pmatrix} a_{0j} \\ a_{1j} \\ a_{2j} \\ a_{3j} \end{pmatrix}$ et T est une matrice

avec coordonnées:

$$\begin{matrix} 1_0 & 1 = 1 \\ 1_1 & 2 = x \\ 1_2 & 3 = 1+x \end{matrix} \left. \vphantom{\begin{matrix} 1_0 \\ 1_1 \\ 1_2 \end{matrix}} \right\} \in \mathbb{F}_2[x] / (p(x))$$

Transformation linéaire

Généralisation $A = \mathbb{F}_2^8$ au lieu de $\mathbb{Z}/4\mathbb{Z}$ du chiffrement de Hill (2^8)

2 Add Round Key (Round)

Chiffrement de Vigenère/Vernam

$$A \rightarrow A \oplus K_i$$

Remarque: AES: $K \times m \rightarrow \mathcal{C}$

avec $(K) = \mathbb{F}_2^{128}$ (variable)

$m = \mathbb{F}_2^{128} \rightarrow k_1, k_2, \dots, k_6 = \text{clés de rounds}$

$\mathcal{C} = \mathbb{F}_2^{128}$

LFSR (Linear feedback shift register)

= manière de produire une est à une suite de bits infinis, avec une période très haute.

motivation:

$$\mathbb{F}_2^m \rightarrow \mathbb{F}_2^n$$

$$K \rightarrow k_1 \dots k_n \text{ bits}$$

($k_1, \dots, k_n$) peut être utilisée dans un chiffrement de Vernam:

$$\begin{array}{r} m_1 \dots m_N \\ k_1 \dots k_N \\ \hline c_1 \dots c_N \end{array}$$

Def: Un registre à décalage à rétroaction (LFSR) est une suite de bits $s_0, \dots, s_{L-1}$ qui est définie par une fct. de rétroaction linéaire:

$$\mathbb{F}_2^L \rightarrow \mathbb{F}_2$$

$$S_i = (s_0, \dots, s_{i-1}) \rightarrow s_{i+L}$$

Le LFSR est donc la fct. $S_i = (s_0, \dots, s_{i-1}) \rightarrow S_{i+L} = (s_{i+L}, \dots, s_{i+L+L-1})$ de laquelle on peut extraire la suite $(s_0, \dots, s_L, \dots)$ et $\mathbb{F}_2^L$ à partir de $S_0 \in \mathbb{F}_2^L$.

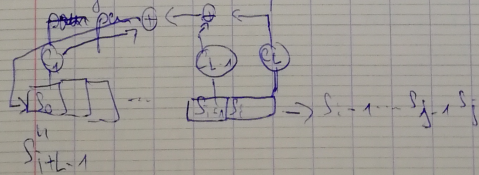
Remarque:

Une fct. (non linéaire) $g: \mathbb{F}_2^L \rightarrow \mathbb{F}_2$ peut être utilisée pour définir une suite $k_i = g(S_i)$ de bits.

Fonctionnement d'un LFSR

$$\text{Soit } S_{i+L} = \sum_{j=0}^{L-1} c_j s_{i+L-j}$$

⊗ la fct. de rétroaction pour $(c_1, \dots, c_L)$ donne à décaler le LFSR



LFSR

Def: Les ~~coefficients~~ $S_0 = (s_0, \dots, s_{L-1}) \in \mathbb{F}_2^L$, qui déterminent la suite (s_i) produite par le LFSR, s'appelle l'état initial du registre.

On va identifier $(s_0, s_1, s_2, \dots)$ avec $s(x) = s_0 + s_1x + s_2x^2 + \dots \in \mathbb{F}_2[[x]]$ et la fct de rétroaction (en mettant $c_0 = 1$) $(c_1, \dots, c_L)$ avec $g(x) = c_1x + \dots + c_Lx^L + c_0 \in \mathbb{F}_2[x]$, qui s'appelle la fct de connexion (ou de rétroaction).

La récurrence est donc équivalente à $g(x)s(x) = f(x) \in \mathbb{F}_2[[x]]$

$$C_0 \quad s(x) = s_0 + s_1x + s_2x^2 + \dots + s_{L-1}x^{L-1} \quad \text{de degré } < L$$

$$C_L \quad \frac{s(x) \cdot x^L}{\left(\sum_{j=1}^L c_j x^{L-j}\right) x^L} = \frac{s_0 x^L}{\text{polynôme de degré } < L}$$

Analogie:

$$\mathbb{Z} \longleftrightarrow \mathbb{F}_2[x]$$

$$Q \longleftrightarrow \mathbb{F}_2[x] = \left\{ \frac{f(x)}{g(x)} \mid f, g \in \mathbb{F}_2[x], g \neq 0 \right\}$$

$$R \longleftrightarrow \mathbb{F}_2[x] \supseteq \mathbb{F}_2[x]_{(x)} = \left\{ \sum_{j=0}^{\infty} s_j x^j \mid s_j \in \mathbb{F}_2 \right\}$$

On remarque que la suite (s_i) est ultimement périodique c-à-d $\exists$ une pré-période m_0 $(s_i)_{i \geq m_0}$ est périodique.
 Prop: La suite est ultimement périodique avec période $N \leq 2^L - 1$.
 Si de plus $c_L = 1$ la suite est périodique.

Def: On dit qu'un LFSR est non-dégénéré si $c_L = 1$.

Preuve: Soit $S_i = (s_0, \dots, s_{L-1}) \in \mathbb{F}_2^L$.

Comme $\mathbb{B}$ détermine S_i donc S_i a $2^L - 1$ valeurs possibles pour la suite $S_i \neq (0, 0, \dots, 0)$.

Si on a $S_i = (0, \dots, 0)$ on a $S_{i+1} = S_{i+2} = \dots = (0, \dots, 0)$ si on a
 $S_i = S_{i+T}$ pour $T \leq 2^L - 1$ et on entre dans un cycle de longueur
 T . $\square$

Pourquoi est-ce que $S_i \neq (0, \dots, 0)$
 et $S_0 \neq (0, \dots, 0)$ et $C_L = 1$?

Preuve (#2 Idée)

Soit $g(x) = x^N - 1$, alors

$\Delta(x) = \frac{f(x)}{g(x)}$ satisfait

$$(x^N - 1) \Delta(x) = \frac{f(x)(x^N - 1)}{g(x)}$$

$$= f(x)h(x) \text{ où } g(x)h(x) = x^N - 1$$

$$a = 0,514$$

$$(10^3 - 1)a = 514$$

$$\Rightarrow a = \frac{514}{10^3 - 1}$$