Sécurité informatique
Clés secrètes

Bruno Martin

Université Côte d'Azur

M1 Informatique

Cryptologie = science du secret.
Comment : avec une **clé**,

- **chiffrer** un **clair** en un **chiffré** préserve sa **confidentialité**.
- Le destinataire **déchiffre** le chiffré pour recouvrer le clair.

Le **cryptanalyste** ne doit pas pouvoir **cryptanalyser**.
Attaques [6] : On suppose le mécanisme de chiffrement connu.

- **à chiffré connu (COA)** : seul le chiffré est connu ;
- **à couples clairs/chiffrés connus (KPA)** : des couples clairs/chiffrés sont connus, on cherche la clé ;
- **à clair choisi (CCA)** : on choisit des clairs, on calcule les chiffrés correspondants et on cherche la clé.

Bref historique

J. Stern [8] : 3 périodes :

- *âge artisanal* : hiéroglyphes, bible, antiquité, renaissance
- *âge technique* : (> WW2) machines chiffrantes complexes
- *âge paradoxal* : (> 1970) systèmes à clé publique

évolution parallèle avec la cryptanalyse (et les maths,...)

- manuelles
- electro-mécaniques
- informatiques
- quantique

Carré de Polybe

Polybe, écrivain grec : communication avec des torches :

	1	2	3	4	5
1	a	b	c	d	e
2	f	g	h	ij	k
3	l	m	n	o	p
4	q	r	s	t	u
5	v	w	x	y	z

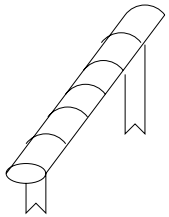
`TEXTE` changé en `44,15,53,44,15`. Caractéristiques :

- coder les lettres par des nombres
- réduire la taille de l'alphabet

transformation d'un caractère x sur A en y mot fini sur B.
Carré de Polybe : $\{a, \ldots, z\} \to \{1, \ldots, 5\}^2$.

Histoire – Grèce antique

500 av. J.-C : *scytale* des généraux Spartiates.



Clé secrète : diamètre du bâton.

Chiffre par transposition

Histoire – César

remplacer la lettre par celle située 3 positions plus loin.
Ainsi `A` devient `d`, `B` devient `e`...
Le clair `TOUTE LA GAULE` devient `wrxwh od jdxoh`.

Chiffre par substitution

Pourquoi chiffrer ?

- Hier :
  - raisons stratégiques
    (éviter que l'ennemi puisse lire un ordre de bataille)
  - l'église pour des raisons politiques
  - la diplomatie pour les rapports d'ambassades

- Aujourd'hui, avec le numérique :
  - confidentialité
  - intégrité
  - authentification

Buts de la cryptologie

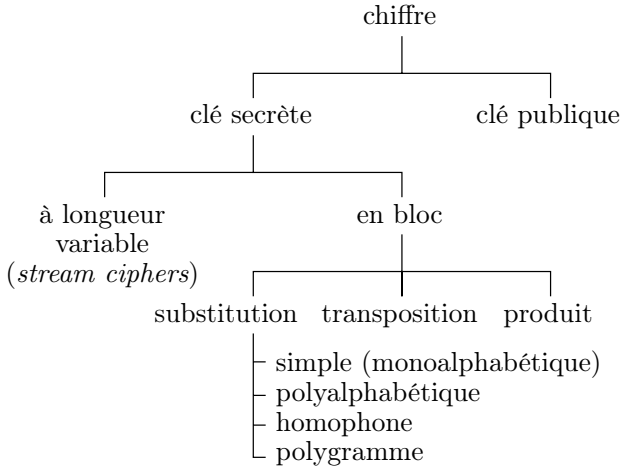
Nombre croissant de buts :

- *secret* : un ennemi ne peut rien apprendre d'intelligible
- *authentification* : garantie que le message provient bien de l'expéditeur prétendu
- *signature* : garantie que le message provient bien de l'expéditeur prétendu pour un tiers
- *minimalité* : on ne communique que ce qui est expressément spécifié.

Outils de la cryptologie

- *Théorie de l'information* : chiffre parfaitement sûr.
- *Complexité* : la plupart ne sont que calculatoirement sûrs.
- *Informatique* : algorithmique ; implémentation logicielle et/ou matérielle
- *Mathématiques* : théorie des nombres, probabilités, statistiques, algèbre, géométrie algébrique...
- *Physique* : quantique, cryptanalyse et distribution de clés

Classification des chiffres



Contenu

Principe des chiffres symétriques

Composés de [1] :

- alphabet des clairs $\mathcal{A}_\mathcal{M}$
- alphabet des chiffrés $\mathcal{A}_\mathcal{C}$
- alphabet des clés $\mathcal{A}_\mathcal{K}$
- chiffrement ; application $E : \mathcal{A}_\mathcal{K}^\star \times \mathcal{A}_\mathcal{M}^\star \to \mathcal{A}_\mathcal{C}^\star$;
- déchiffrement ; application $D : \mathcal{A}_\mathcal{K}^\star \times \mathcal{A}_\mathcal{C}^\star \to \mathcal{A}_\mathcal{M}^\star$

E et D vérifient $\forall K \in \mathcal{A}_\mathcal{K}^\star$, $\forall M \in \mathcal{A}_\mathcal{M}^\star$:

$$D(K, E(K, M)) = M = \{\{M\}_K\}_K$$

Notation entre accolades appelée *notation Alice et Bob* :

`https://en.wikipedia.org/wiki/Security_protocol_notation`

Chiffres monoalphabétiques

Chiffre monoalphabétique : bijection des lettres de $\mathcal{A}_M$ sur $\mathcal{A}_C$. Permutation si $\mathcal{A}_M = \mathcal{A}_C$

Chiffre additif

Exemple : César. {a,...,z}≡{A,...,Z} $\equiv \{0, \ldots, 25\} = \mathbb{Z}_{26}$

Chiffrement : $\forall x \in \mathbb{Z}_{26}$, $x \mapsto x + 3 \mod 26$

Déchiffrement : $\forall y \in \mathbb{Z}_{26}$ $y \mapsto y - 3 \mod 26$

Chiffre multiplicatif

On étudie : $x \mapsto t \cdot x \mod 26$ pour $t \in \mathbb{N}$.

Valeurs de t acceptables tq pgcd$(t, 26) = 1 \Leftrightarrow t \nmid 26$.

$\varphi(26)$ valeurs de t : $\{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\}$.

Les autres n'assurent pas l'unicité du déchiffrement (p.e. 2).

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12
n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25
0	2	4	6	8	10	12	14	16	18	20	22	24

Déchiffrement

Pour déchiffrer, il faut t^{-1} modulo 26.

Utiliser Euclide étendu fournit les coefficients de Bézout, i.e. $x, y \in \mathbb{N}$ t.q. $d = \gcd(a, b) = ax + by$.

A partir des coefficients de Bézout, on déduit t^{-1} modulo 26 :

$$\gcd(t, 26) = 1 \Leftrightarrow \exists x, y \in \mathbb{N} : tx + 26y = 1 \Leftrightarrow x \equiv t^{-1} \mod 26$$

Calcul manuel itératif

Euclide étendu(q, r) avec $q < r$

Q,R$\leftarrow (1, 0), (0, 1)$;

tantque $r \neq 0$ **faire**

$t \leftarrow q \mod r$;

$T \leftarrow Q - \lfloor q/r \rfloor R$;

$(q, r) \leftarrow (r, t)$;

$(Q, R) \leftarrow (R, T)$;

retourne (q, Q) ; q est le pgcd et Q donne les coeffs.

Euclide étendu de $(11, 26)$

q	r	t	Q	$\lfloor q/r \rfloor$	R	T
11	26	11	$(1, 0)$	0	$(0, 1)$	$(1, 0)$
26	11	4	$(0, 1)$	2	$(1, 0)$	$(-2, 1)$
11	4	3	$(1, 0)$	2	$(-2, 1)$	$(5, -2)$
4	3	1	$(-2, 1)$	1	$(5, -2)$	$(-7, 3)$
3	1	0	$(5, -2)$	3	$(-7, 3)$	$(26, -11)$
1	0		$(-7, 3)$		$(26, -11)$	

pgcd$(11, 26) = 1$ de coefficients de Bézout $(-7, 3)$.

L'inverse de 11 $\mod 26 = -7 = 19$.

Euclide étendu(q, r) avec $q < r$
Q$\leftarrow (1, 0)$;
R$\leftarrow (0, 1)$;
tantque $r \neq 0$ **faire**
$t \leftarrow q \mod r$;
$T \leftarrow Q - \lfloor q/r \rfloor R$;
$(q, r) \leftarrow (r, t)$;
$(Q, R) \leftarrow (R, T)$;
ftq
retourne (q, Q) ; q est le pgc
fin

Chiffres affines

Avec 26 chiffres additifs et 12 multiplicatifs, on obtient les chiffres **affines** : étant donnés s et $t \in \mathbb{N}$, pour chiffrer :

$$x \mapsto (x + s) \cdot t \mod 26$$

La clé est (s, t) ; on déchiffre en appliquant successivement les méthodes précédentes.

26.12=312 chiffres affines possibles. Nous sommes loin des 26 !=403.291.461.126.605.635.584.000.000 chiffres monoalphabétiques.

Chiffres définis par mot clé

Définir tous les chiffres monoalphabétiques possibles, par :

- un mot clé, par exemple `CRYPTANALYSE` ;
- une lettre clé, par exemple `e`.

Eliminer toutes les occurrences multiples de lettres dans le mot clé -ici `CRYPTANLSE`- puis

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


Cryptanalyse

Shannon : une petite proportion de lettres fournit plus d'informations que les deux tiers du texte.

Faire une analyse statistique des fréquences d'apparition des lettres ou des bigrammes dans le chiffré.

Résolution de $ax \equiv b \mod n$

On utilise la méthode de résolution de l'équation $ax \equiv b \mod n$ pour les chiffres multiplicatifs. On distingue deux cas :

- $\gcd(a, n) = 1$: $ax \equiv b \mod n \Leftrightarrow x \equiv a^{-1}b \mod n$ avec a^{-1} donné par Euclide étendu.
- $\gcd(a, n) = d \neq 1$ de nouveau deux cas :
  - $d \nmid b$, l'équation n'a pas de solution ;
  - $d|b$: $ax \equiv b \mod n \Leftrightarrow da'x \equiv db' \mod dn'$. On divise tout par d et on résout $a'x \equiv b' \mod n'$. On a alors l'ensemble de solutions : $\{x = a'^{-1}b' + kn' : 0 \leq k < d\}$.

Conclusion

Chiffres monoalphabétiques pas résistants à une analyse statistique.

Besoin de chiffres pour lesquels la distribution statistique des fréquences des lettres tend vers une loi uniforme.

1re idée : utiliser une transformation cryptographique qui associe à chaque lettre du clair un ensemble de lettres du chiffré.

On obtient ainsi les **chiffres polyalphabétiques**

Chiffre de Vigenère (1586)

Dans un **chiffre polyalphabétique**, les caractères du clair sont transformés au moyen d'une clé $K = k_0, \ldots, k_{j-1}$ qui définit j fonctions différentes $f_0, \ldots, f_{j-1}$ telles que

$$\forall i,\ 0 < j \leq n \quad \begin{array}{l} f_{k_l} : \mathcal{A}_M \mapsto \mathcal{A}_C, \forall l,\ 0 \leq l < j \\ c_i = f_{k_i \mod j}(m_i) \end{array}$$

Idée : utiliser plusieurs systèmes monoalphabétiques différents.

Carré de Vigenère

```
abcdefghijklmnopqrstuvwxyz abcdefghijklmnopqrstuvwxyz
ABCDEFGHIJKLMNOPQRSTUVWXYZ NOPQRSTUVWXYZABCDEFGHIJKLM
BCDEFGHIJKLMNOPQRSTUVWXYZA OPQRSTUVWXYZABCDEFGHIJKLMN
CDEFGHIJKLMNOPQRSTUVWXYZAB PQRSTUVWXYZABCDEFGHIJKLMNO
DEFGHIJKLMNOPQRSTUVWXYZABC QRSTUVWXYZABCDEFGHIJKLMNOP
EFGHIJKLMNOPQRSTUVWXYZABCD RSTUVWXYZABCDEFGHIJKLMNOPQ
FGHIJKLMNOPQRSTUVWXYZABCDE STUVWXYZABCDEFGHIJKLMNOPQR
GHIJKLMNOPQRSTUVWXYZABCDEF TUVWXYZABCDEFGHIJKLMNOPQRS
HIJKLMNOPQRSTUVWXYZABCDEFG UVWXYZABCDEFGHIJKLMNOPQRST
IJKLMNOPQRSTUVWXYZABCDEFGH VWXYZABCDEFGHIJKLMNOPQRSTU
JKLMNOPQRSTUVWXYZABCDEFGHI WXYZABCDEFGHIJKLMNOPQRSTUV
KLMNOPQRSTUVWXYZABCDEFGHIJ XYZABCDEFGHIJKLMNOPQRSTUVW
LMNOPQRSTUVWXYZABCDEFGHIJK YZABCDEFGHIJKLMNOPQRSTUVWX
MNOPQRSTUVWXYZABCDEFGHIJKL ZABCDEFGHIJKLMNOPQRSTUVWXY
```

```
polyalphabetique KSYSSGTUUTZXVKMZ
VENUSVENUSVENUSV
```


Cryptanalyse...

... plus difficile : on tend vers une distribution uniforme.

Mais, en réarrangeant le chiffré en une matrice qui a autant de colonnes que la longueur de la clé, toutes les lettres d'une même colonne proviennent du même chiffre monoalphabétique.

Travail du cryptanalyste :
(1) déterminer la longueur de la clé
(2) appliquer les méthodes précédentes.

2 tests pour trouver la longueur de la clé : Kasiski et Friedman.

Chiffres homophones

But : lisser la distribution des fréquences des lettres.
L'alphabet cryptographique contient plusieurs équivalents pour une même lettre du clair.
On définit une substitution à représentations multiples.
Ainsi, le e clair, au lieu d'être toujours chiffré par 4 p.e., pourra être remplacé par 37, 38, 39, ...
Ces différentes **unités cryptographiques** correspondant à un même caractère du clair sont dites **homophones**.

lettre	fréquence	lettre	fréquence
a	0,26,27,28,29,30	n	13,68,69,70,71,72
b	1	o	14,73,74,75,76
c	2,31,32,33,34	p	15,77,78
d	3,35,36	q	16
e	4,37,...,54	r	17,79,80,81,82
f	5,55	s	18,83,84,85,86,87
g	6,56	t	19,88,89,90,91,92,93
h	7,57	u	20,94,95,96,97
i	8,58,59,60,61,62	v	21
j	9	w	22
k	10	x	23
l	11,63,64,65,66	y	24,98
m	12,67	z	25

Transposition

Implémente une permutation des caractères clairs $\mathcal{A}_C = A_M$.

$$\forall i, \quad 0 \leq i < 0 \quad \begin{array}{l} f : \mathcal{A}_M \to \mathcal{A}_M \\ \eta : \mathbb{Z}_n \to \mathbb{Z}_n \\ c_i = f(m_i) = m_{\eta(i)} \end{array}$$

Transposition simple à tableau

A partir d'une phrase clé, définir une clé numérique :

T	R	A	N	S	P	O	S	I	T	I	O	N	S	I	M	P	L	E
18	14	1	8	15	12	10	16	3	19	4	11	9	17	5	7	13	6	2

On chiffre, «*le chiffrement est l'opération qui consiste à transformer un texte clair, ou libellé, en un autre texte inintelligible appelé texte chiffré ou chiffré*» [5].

18	14	1	8	15	12	10	16	3	19	4	11	9	17	5	7	13	6	2
l	e	c	h	i	f	f	r	e	m	e	n	t	e	s	t	l	o	p
é	r	a	t	i	o	n	q	u	i	c	o	n	s	i	s	t	e	à
t	r	a	n	s	f	o	r	m	e	r	u	n	t	e	x	t	e	c
l	a	i	r	o	u	l	i	b	e	l	l	é	e	n	u	n	a	u
t	r	e	t	e	x	t	e	i	n	i	n	t	e	l	l	i	g	i
b	l	e	a	p	p	e	l	é	t	e	x	t	e	c	h	i	f	f
r	é	o	u	c	r	y	p	t	o	g	r	a	m	m	e			

Chiffre de Vernam (1917)

One-time pad est chiffre «parfait» au sens de la théorie de l'information.

A et B partagent une suite aléatoire de n bits : la clé secrète K.
A chiffre M de n bits en $C = M \oplus K$.
B déchiffre C en $M = K \oplus C$.

Exemple
$M = 0011$, $K = 0101$
$C = 0011 \oplus 0101 = 0110$
$M = K \oplus C$.

Non-réutilisation : à chaque nouveau message, engendrer une nouvelle clé.

Pourquoi changer de clé ?

... pour ne pas révéler d'information sur le $\oplus$ des clairs.

Eve peut intercepter $C = \{M\}_K$ et $C' = \{M'\}_K$ et calculer :

$$C \oplus C' = (M \oplus K) \oplus (M' \oplus K) = M \oplus M'$$

Avec suffisamment de chiffrés, elle peut retrouver un clair par analyse des fréquences [4].

En respectant les conditions, Vernam garantit le secret parfait.

Condition (du secret parfait)

$$p(M = m \mid C = c) = p(M = m)$$

Intercepter C ne révèle aucune information au cryptanalyste.

Pourquoi est-il sûr ?

Le chiffre de Vernam assure le **secret parfait**.
On définit trois classes d'informations

- les clairs M de probabilités $p(M)$ t.q. $\sum_M p(M) = 1$
- les chiffrés C de probabilités $p(C)$ t.q. $\sum_C p(C) = 1$
- les clés de probabilités $p(K)$ t.q. $\sum_K p(K) = 1$

$p(M \mid C)$ = probabilité que M ait été envoyé sachant que C a été reçu (C est le chiffré de M). La condition du secret parfait est définie comme

$$p(M \mid C) = p(M)$$

L'interception du chiffré ne fournit aucune information au cryptanalyste.

Conclusion

Sûreté absolue mais difficile à mettre en œuvre.

- engendrer de grandes clés aléatoires
- les stocker et de les partager avec les destinataires

exemple d'utilisation : «téléphone rouge».

Chiffres produits et itérés

Améliorations : combiner substitutions+transpositions (**produit**)

Un chiffre est **itéré** si le chiffré est obtenu par applications itérées d'une fonction de tour plusieurs fois au même clair.
A chaque tour, combiner une clé de tour avec le texte d'entrée.

Définition
*Dans un chiffre itéré à r tours, le chiffré est calculé par application itérée au clair d'une **fonction de tour** g t.q.*

$$C_i = g(C_{i-1}, K_i) \quad i = 1, \ldots, r$$

C_0 le clair, K_i clé de tour et C_r le chiffré.
Déchiffrement en inversant l'équation précédente. À K_i fixée, g doit être inversible.

Cas particulier, **les chiffres de Feistel**.

Chiffre de Feistel

Un **chiffre de Feistel** de taille de bloc $2n$ à r tours est défini par :

$$g : \{0,1\}^n \times \{0,1\}^n \times \{0,1\}^m \to \{0,1\}^n \times \{0,1\}^n$$

$$X, Y, Z \mapsto (Y, F(Y, Z) \oplus X)$$

g fonction de $2n \times m$ bits dans $2n$ bits et $\oplus$ XOR sur n bits.
Fonctionnement
Etant donné un clair $P = (P^L, P^R)$ et r clés de tour $K_1, \ldots, K_r$, le chiffré (C^L, C^R) est calculé en r tours.
On pose $C_0^L = P^L$ et $C_0^R = P^R$ et on calcule pour $i = 1, \ldots, r$

$$(C_i^L, C_i^R) = (C_{i-1}^R, F(C_{i-1}^R, K_i) + C_{i-1}^L)$$

avec $C_i = (C_i^L, C_i^R)$ et $C_r^R = C^L$ et $C_r^L = C^R$
Les clés de tour $K_1, \ldots, K_r$, sont calculées par un algorithme de séquencement de la clé sur une clé principale K.

Le DES

- NBS lance un appel d'offre en 1973
- DES (*Data Encryption Standard*) déposé par IBM en 1975
- adopté en 1977
- évalué tous les 4 ans
- on connaît son remplaçant : AES ou Rijndael [2]
- exemple de chiffrement par le DES dans STINSON [9]

Utilité du DES
Le DES était le chiffre le plus utilisé (banques, systèmes de sécurité informatiques architecturés autour de DES).
Chiffre de Feistel qui possède des propriétés particulières.

Fonctionnement

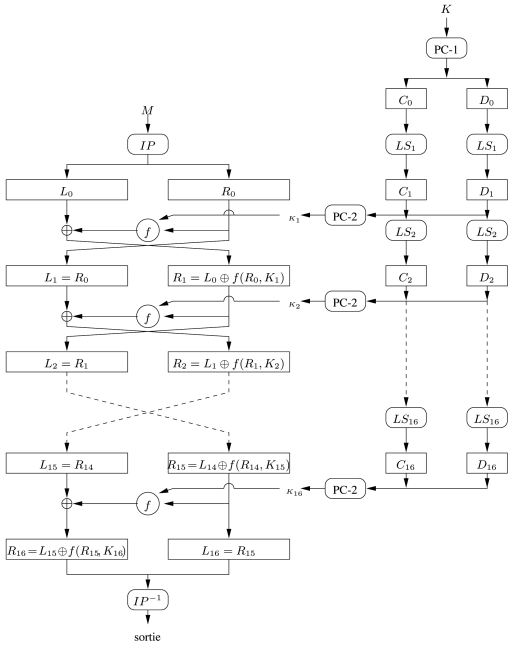
DES reçoit en entrée :

- un message M de 64 bits ;
- une clé K de 56 bits.

et fournit un chiffré C de 64 bits.
L'algorithme fait subir à M une permutation initiale IP donnant le message «permuté» M'.
M' est ensuite découpé en deux mots de 32 bits :

- L_0 qui représente la partie gauche de M'
- R_0 pour la partie droite.

DES exécute ensuite 16 itérations de la fonction f qui combine substitutions et transpositions.



Contenu

Analogie avec $\mathbb{R}$

On construit le corps des complexes $\mathbb{C}$ à partir du corps des réels $\mathbb{R}$ en ajoutant une racine imaginaire i, racine de l'équation $x^2 + 1 = 0$ qui n'a pas de racine dans $\mathbb{R}$. On note $\mathbb{C} = \mathbb{R}(i)$.

On part

- d'un corps de base $\mathbb{F}_2 = (\{0, 1\}, +, .)$. Les éléments du corps sont $\{0, 1\}$, il a deux opérations $+, .$ et vérifie que tout élément a un opposé pour $'+'$ et un inverse pour $'.'$
- d'un polynôme p **irréductible**, i.e. qui n'a pas d'autre diviseurs que 1 et lui-même dans $\mathbb{F}_2[x]$. De plus, ni 0 ni 1 ne sont racine de ce polynôme.

On construit ensuite un **corps d'extension** de $\mathbb{F}_2[x]/p = \mathbb{F}_2(\eta)$ si η est racine de p.

Exemple

On peut prendre $p(x) = x^3 + x + 1$ qui est irréductible.

Vérifier l'irréductibilité

On vérifie que $p(x) = x^3 + x + 1$ est irréductible :

- ni 0 ni 1 ne sont racine
- aucun des polynômes de degré inférieur ne le divisent : $\{x + 1, x^2, x^2 + 1, x^2 + x, x^2 + x + 1\}$

Exemple

$x^3+x+1 \mid x^2+x$

x^3+x^2 — $x+1$

x^2+x+1

x^2+x

1 ← le reste n'est pas nul
le reste est 1 donc
x^2+x inverse de $x+1 \bmod x^3+x+1$

$x^3+x+1 = 1 + (x^2+x)(x+1)$ $\bmod x^3+x+1$

$1 = (x^2+x)(x+1)$

$x^3+x^2+x^2+x$

$x+1 \quad + \quad x = 1$

Eléments du corps d'extension

L'équation associée au polynôme $p(x) = x^3 + x + 1 = 0$ définit une relation de réécriture (d'équivalence) :

$$x^3 = x + 1$$

On construit alors l'extension $\mathbb{F}_2[x]/x^3 + x + 1 \simeq \mathbb{F}_8 = GF(8)$ qui a comme éléments :

polynôme	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
binaire	000	001	010	011	100	101	110	111

Il faut vérifier qu'on a bien un corps en écrivant les tables des opérations '+' et '.' sur ces éléments en faisant les calculs modulo p.

Addition

	0	1	x	$1+x$	x^2	$1+x^2$	x^2+x	$1+x+x^2$
0	0	1	x	$1+x$	x^2	$1+x^2$	x^2+x	$1+x+x^2$
1	1	0	$1+x$	x	$1+x^2$	x^2	$1+x+x^2$	$x+x^2$
x	x	$1+x$	0					
$1+x$								
x^2								
$1+x^2$								
$x+x^2$								
$1+x+x^2$								

Produit

	0	1	x	$1+x$	x^2	$1+x^2$	x^2+x	$1+x+x^2$
0	0	0	0	0	0	0	0	0
1	0	1	x	$1+x$	x^2	$1+x^2$	x^2+x	$1+x+x^2$
x	0	x	x^2	$x+x^2$				
$1+x$	0	$1+x$	$x+x^2$					
x^2	0	x^2						
$1+x^2$	0	$1+x^2$						
$x+x^2$	0	$x+x^2$						
$1+x+x^2$	0	$1+x+x^2$						

Conclusion

On a défini un corps d'extension à 8 éléments à partir de $\mathbb{F}_2$ et d'un polynôme irréductible de degré 3 (notez que $8 = 2^3$). Ce corps est unique (à isomorphisme près) et noté $\mathbb{F}_8$.
Ses éléments de base sont

polynôme	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
binaire	000	001	010	011	100	101	110	111

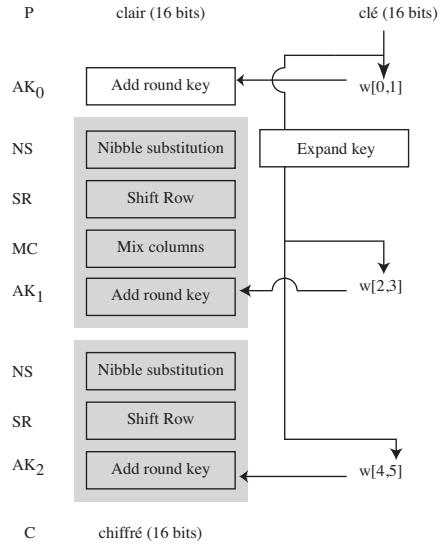
Les opérations internes sont définies en effectuant les calculs modulo le polynôme irréductible (en utlisant la règle de réécriture).

Cette construction algébrique est de plus en plus utilisée en cryptographie.

Contenu

Chiffres symétriques
- Chiffres par substitution
- Chiffres par transposition
- Chiffre de Vernam (à longueur variable)
- Chiffres produits et itérés
- Extension de corps
- (S)AES ou Rijndael[3]

Modes d'utilisation



State matrix & nibbles

- 1 nibble = mot de 4 bits (E/S des composants de SAES)

$$\begin{array}{c|c} b_0b_1b_2b_3 & b_8b_9b_{10}b_{11} \\ \hline b_4b_5b_6b_7 & b_{12}b_{13}b_{15}b_{15} \end{array} = \begin{array}{c|c} S_{0,0} & S_{0,1} \\ \hline S_{1,0} & S_{1,1} \end{array}$$

- représentation de la clé :

$$\underbrace{k_0k_1\ldots k_7}_{w[0]} \quad \underbrace{k_8\ldots k_{15}}_{w[1]}$$

Opérations dans $GF(16) \simeq \mathbb{F}_2[x]/x^4+x+1$

- $m(x) = x^4 + x + 1$ est un irréductible de $\mathbb{F}_2$
- éléments : nibble $b_0b_1b_2b_3 \overset{\theta}{\leftrightarrow} b_0x^3 + b_1x^2 + b_2x + b_3$
- addition : addition des coefficients : $(x^3 + x + 1) + (x^2 + 1)$
- multiplication : produit des polynômes $\mod m(x)$
- codage octet : dans extension quadratique $\mathbb{F}_{16}[z]/z^2 + 1$
- attention ! $z^2 + 1$ non inversible dans $GF(16)$
- Rappel : trouver l'inverse d'un élément : Euclide étendu sur polynômes $(x + 1, m) = (x^3 + x^2 + x)(x + 1) + 1 \cdot m$

Inverses dans $\mathbb{F}_{16}$

1	0001	1	1	0001	1
2	0010	x	x^3+1	1001	9
3	0011	$x+1$	x^3+x^2+x	1110	e
4	0100	x^2	x^3+x^2+1	1101	d
5	0101	x^2+1	x^3+x+1	1011	b
6	0110	x^2+x	x^2+x+1	0111	7
7	0111	x^2+x+1	x^2+x	0110	6
8	1000	x^3	x^3+x^2+x+1	1111	f
9	1001	x^3+1	x	0010	2
a	1010	x^3+x	x^3+x^2	1100	c

Boîte S utilisée dans Nibble substitution

$i\downarrow$	00	01	10	11
00	9	4	a	b
01	d	1	8	5
10	6	2	0	3
11	c	e	f	7

$=$

1001	0100	1010	1011
1101	0001	1000	0101
0110	0010	0000	0011
1100	1110	1111	0111

- $\forall$ nibble : $\underbrace{b_0 b_1}_{\text{ligne}}\ \underbrace{b_2 b_3}_{\text{colonne}}$: 00 01 $\overset{S}{\to}$ 01 00
-

$$\begin{array}{|c|c|}\hline 0001 & 0001 \\ \hline 1100 & 1110 \\ \hline \end{array} \overset{S}{\to} \begin{array}{|c|c|}\hline 0100 & 0100 \\ \hline 1100 & 1111 \\ \hline \end{array} = \begin{array}{|c|c|}\hline 4 & 4 \\ \hline c & f \\ \hline \end{array}$$

Retrouver la boîte S algébriquement

1. initialiser la boîte S avec les nibbles rangés en tableau 1D ligne à ligne
2. convertir chaque nibble en polynôme
3. inverser chaque nibbble dans $\mathbb{F}_{16}$
4. associer à l'inverse son polynôme dans $\mathbb{F}_{16}[y]/y^4-1=N(y)$
5. calculer $a(y)N(y)+b(y) \mod y^4+1$ avec $a=y^3+y^2+1$ et $b=y^3+1$

Normalement $S(0011)=1011\equiv S(3)=b$

$S(0011)=1011\equiv S(3)=b$

1. initialiser la boîte S avec les nibbles rangés en tableau 1D ligne à ligne
2. convertir chaque nibble en polynôme $S(0011)=x+1$
3. inverser chaque nibbble dans $\mathbb{F}_{16}$: $(x+1)^{-1}=x^3+x^2+x$
4. associer à l'inverse son polynôme dans $\mathbb{F}_{16}[y]/y^4-1=N(y)$: $N(y)=y^3+y^2+y$
5. calculer $a(y)N(y)+b(y) \mod y^4+1$ avec $a=y^3+y^2+1$ et $b=y^3+1$:
   $(y^3+y^2+y)(y^3+y^2+1)+y^3+1 \mod y^4+1$
   $\cancel{y^6}+\cancel{y^5}+\cancel{y^3}+\cancel{y^5}+\cancel{y^4}+\cancel{y^2}+\cancel{y^4}+\cancel{y^3}+y+y^3+1$
   $\mod y^4+1=y+y^3+1=y^3+y+1$

Normalement $S(0011)=1011\equiv S(3)=b$

En python/sympy

```
from sympy import *
init_printing()
from sympy.polys.domains import ZZ
from sympy.polys.galoistools import gf_mul, gf_add, gf_gcdex,
    gf_rem
def NS(nib):
    polym=ZZ.map([1,0,0,1,1])
    polya=ZZ.map([1,1,0,1])
    polyb=ZZ.map([1,0,0,1])
    polymod=ZZ.map([1,0,0,0,1])
    invnib,t,g=gf_gcdex(nib,polym,2,ZZ)
    return(gf_rem(gf_add(gf_mul(invnib,polya,2,ZZ),polyb,2,ZZ),
           polymod,2,ZZ))
 > NS(ZZ.map([1,1]))
 [1, 0, 1, 1]
```


Autres transformations

- Shift row : transposition bits nibble :
  $b_0b_1\ b_2b_3 \mapsto b_2b_3\ b_0b_1$. $\begin{array}{c|c} 4 & 4 \\ \hline c & f \end{array} \mapsto \begin{array}{c|c} 4 & 4 \\ \hline f & c \end{array}$
- Mix columns : modification de la représ. pol. des colonnes de l'état $\begin{array}{c|c} N_i & . \\ \hline N_j & . \end{array}$; on associe $c(z) = N_iz + N_j \in \mathbb{F}_{16}[z]/z^2+1$; calculer $c(z).(x^2z+1) \bmod z^2+1$.

Exemple

Pour $4f \leftrightarrow 0100\ 1111 \mapsto c(z) = x^2z + x^3 + x^2 + x + 1$ *:* $(x^3+x^2+1)z + (x^3+x^2) = N_kz + N_\ell \leftrightarrow 1101\ 1100$ *car* $z^2 = 1, x^4 = x+1$ *et* $x^5 = x^2+x$.

Mix columns (matriciel)

On travaille directement sur l'état :

$$\begin{pmatrix} 1 & x^2 \\ x^2 & 1 \end{pmatrix} \cdot \begin{pmatrix} S_{0,0} & S_{0,1} \\ S_{1,0} & S_{1,1} \end{pmatrix} =_{\mathbb{F}_{16}} \begin{pmatrix} 1 & 4 \\ 4 & 1 \end{pmatrix} \cdot \begin{pmatrix} S_{0,0} & S_{0,1} \\ S_{1,0} & S_{1,1} \end{pmatrix}$$

Exemple

$$\begin{pmatrix} 1 & x^2 \\ x^2 & 1 \end{pmatrix} \cdot \begin{pmatrix} x^2 & x^2 \\ x^3+x^2+x+1 & x^3+x^2 \end{pmatrix} = \begin{pmatrix} x^3+x^2+1 & 1 \\ x^3+x^2 & x^3+x^2+x+1 \end{pmatrix} = \begin{pmatrix} d & 1 \\ c & f \end{pmatrix}$$

Séquencement de la clé

- initialisation : $w[0] = k_0 \dots k_7 \qquad w[1] = k_8 \dots k_{15}$
- $2 \le i \le 5$

$$\begin{cases} w[i] = w[i-2] \oplus \text{RCON}(i/2) \oplus \text{SubNib}(\text{RotNib}(w[i-1])) & i \text{ pair} \\ w[i] = w[i-2] \oplus w[i-1] & i \text{ impair} \end{cases}$$

Avec

- RCON[i]=RC[i]0000
- RC[i] $= x^{i+2} \in \mathbb{F}_{16}$ (RC[1]=$x^3 \leftrightarrow 1000$)
- RotNib(N_0N_1)=N_1N_0
- SubNib(N_0N_1)=$S(N_0)S(N_1)$ où S est la S-box

Exemple

avec $w[0]w[1] = 0101\ 1001\ 0111\ 1010$*, on a* $w[2] = 1101\ 1100$*,* $w[3] = 1010\ 0101$*,* $w[4] = 0110\ 1100$ *et* $w[5] = 1100\ 1010$

Pourquoi SAES ?

- introduit dans [7] pour des raisons pédagogiques
- version simplifiée de AES utilisable « à la main »
- permet de voir le fonctionnement des cryptanalyses
- illustre tous les principes de fonctionnement de AES

Et le vrai AES ?

Fonctionne avec un nombre de tours r variable, fonction de la taille des blocs et de la clé :

clés \ blocs	128	192	256
128	10	12	14
192	12	12	14
256	14	14	14

On travaille dans GF(256), engendré par le polynôme $x^8 + x^4 + x^3 + x + 1$. Sinon tout fonctionne comme pour SAES.

Contenu

ECB : electronic codebook mode

Celui décrit précédemment, étant donné un clair, chaque bloc x_i est chiffré avec la clé K, donnant le chiffré $y_1 y_2 \ldots$

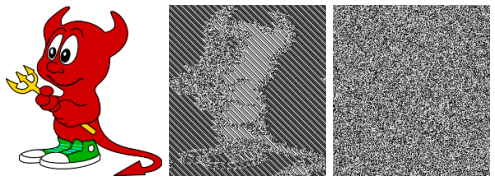
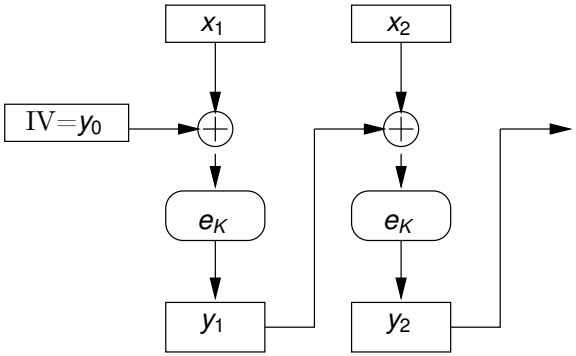


Figure – Beastie / ECB / CBC

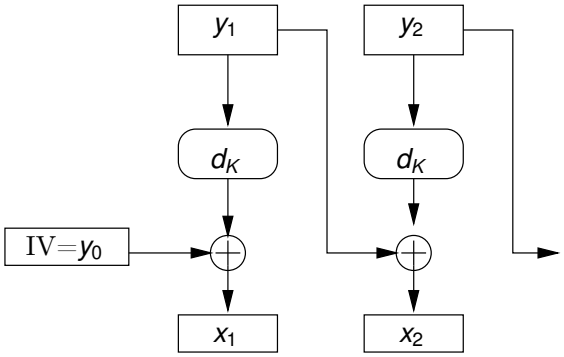
http://en.wikipedia.org/wiki/Block_cipher_mode_of_operation

CBC : cipher block chaining mode

Chaque chiffré y_i agit sur le bloc de clair suivant x_{i+1} avant son chiffrement par une opération de ou exclusif.



CBC – Déchiffrement



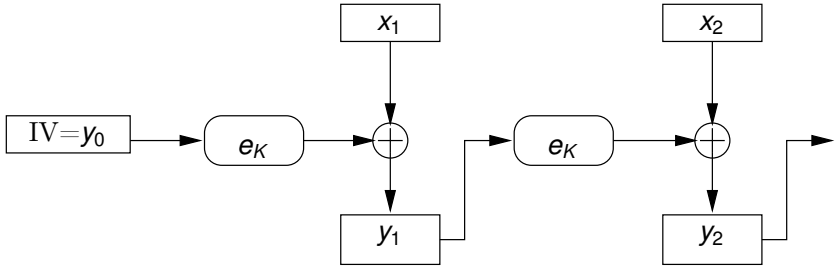
OFB (output feedback mode) et CFB (cipher feedback mode)

Le chiffrement du clair se fait par une suite de ou exclusifs avec des clés issues du chiffrement par un chiffre symétrique.

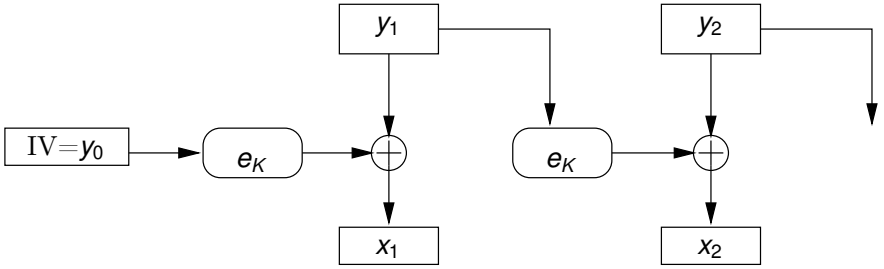
- **OFB** : suite des clés est un chiffrement itéré d'une valeur initiale IV de 64 bits. On définit z_0=IV et on calcule la suite $z_1 z_2 \ldots$ par $z_i = e_K(z_{i-1})$.
- **CFB** : on commence avec y_0=IV (un bloc de 64 bits) et la clé suivante est produite en chiffrant le chiffré précédent $z_i = e_K(y_{i-1})$.

Dans les 2 cas, Le clair est chiffré par $y_i = x_i \oplus z_i$

Chiffrement CFB

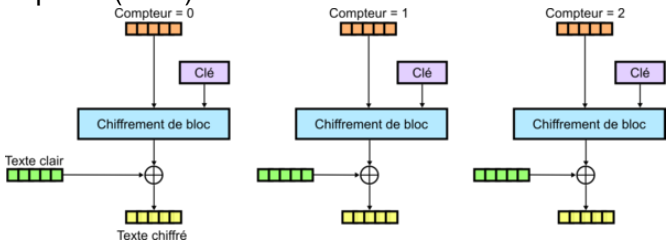


Déchiffrement CFB



Mode CTR

Le flux de clé est obtenu en chiffrant itérativement les valeurs d'un compteur (CTR)



Mode très utilisé car permet un chiffrement par flot et autorise les pré-calculs.

MAC-MDC

Pour Message Authentication Code (Modification Detection Code), ou empreinte du message (MAC=MDC+IV$\neq$ 0).

Possible avec CBC et CFB.
On démarre avec IV=0. On construit le chiffré $y_1 \dots y_n$ avec la clé K en mode CBC. MAC est le bloc y_n.
Alice transmet donc le message $x_1 \dots x_n$ et le MAC y_n.
Quand Bob reçoit $x_1 \dots x_n$, il construit $y_1 \dots y_n$ en utilisant la clé secrète K et vérifie que y_n est identique au MAC reçu.

G. Brassard.
Cryptologie contemporaine.
Logique, mathématiques, informatique. Masson, 1993.

J. Daemen and V. Rijmen.
AES proposal : Rijndael.
Technical report, Katholieke Universiteit Leuven, 1999.

J. Daemen and V. Rijmen.
The Rijndael bloc cipher.
Technical report, AES proposal, 1999.

E Dawson and L Nielsen.
Automated cryptanalysis of xor plaintext strings.
Cryptologia, XX(2) :165–181, May 1996.

D. Kahn.
La guerre des codes secrets.
InterEditions, 1980.

R.L. Rivest.
Cryptography.
In *Handbook of Theoretical Computer Science*, volume A, chapter 13. Elsevier, 1990.

W. Stallings.
Cryptography and Network Security.
Prentice-Hall, 4th. edition, 2006.

J. Stern.
La science du secret.
Odile Jacob, 1998.

D. Stinson.
Cryptographie, théorie et pratique.
International Thomson Publishing, 1995.