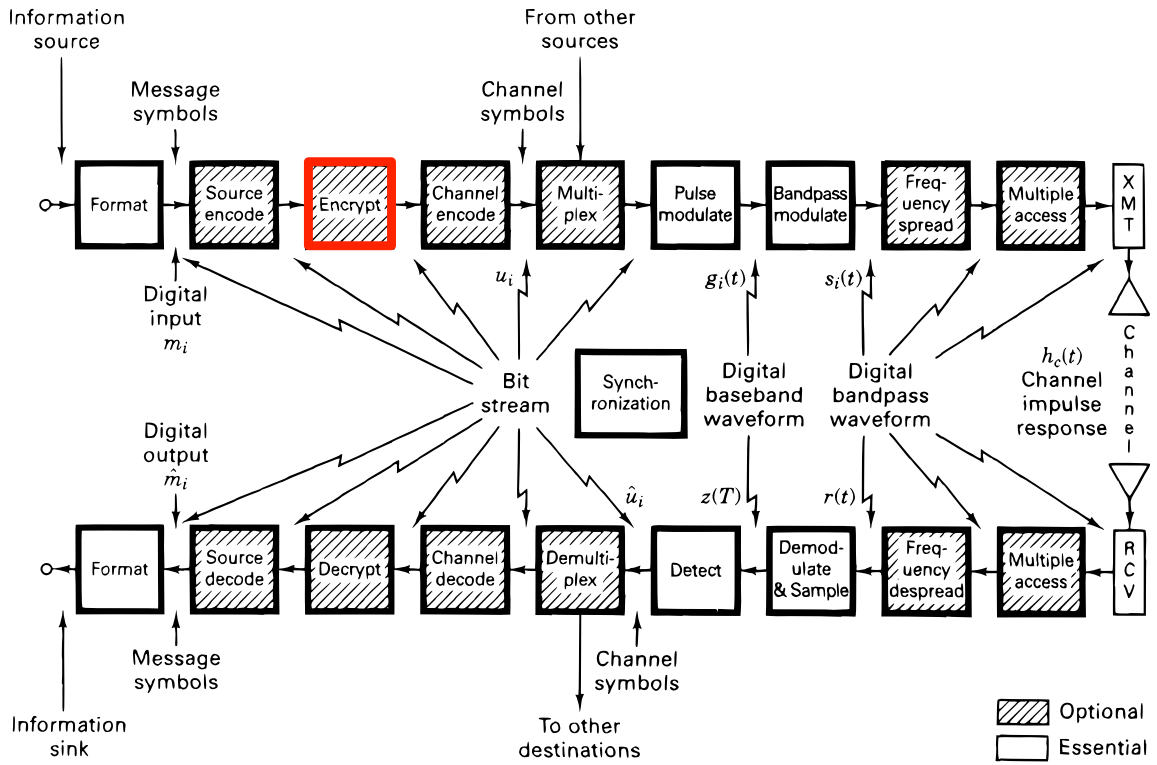
Cryptologie

Transmissions Numériques

Cédric RICHARD
Université Nice Sophia Antipolis

Cryptologie



Digital Communications, B. Sklar, Prentice Hall

Cryptologie

Principes préalables

Le cryptage (ou chiffrement) est mis en œuvre dans deux cadres d'utilisation :

- ▷ **Confidentialité** contre les attaques passives.
- ▷ **Authentification** contre les attaques actives.

On distingue deux types de cryptage :

- ▷ **Symétrique** :
  une clé unique (et partagée) permet de crypter et de décrypter le message
- ▷ **Asymétrique ou à clé publique** :
  le cryptage et décryptage se font avec des clés différentes

Cryptologie

Généalogie

Période artisanale

- ▷ Stéganographie (dissimulation et non cryptage)
- ▷ Scytale (Sparte, 400 avant J. C.)
- ▷ Chiffre de César (décalage de l'alphabet)
- ▷ Chiffre de Vigenère (décalage avec clé, 1553)
- ▷ Enigma (1920)

Scytale

Cryptologie

Généalogie : stéganographie

Lettre de George Sand (1804-1876) à Alfred de Musset (1810-1857)

Cher ami,

Je suis toute émue de vous dire que j'ai
bien compris l'autre jour que vous aviez
toujours une envie folle de me faire
danser. Je garde le souvenir de votre
(...) et je voudrais bien que ce soit
une preuve que je puisse être aimée
par vous. Je suis prête à montrer mon (...)

Votre poupée

Cryptologie

Généalogie : stéganographie

Réponse d'Alfred de Musset à George Sand

Quand je vous jure, hélas, un éternel hommage
Voulez-vous qu'un instant je change de language
Que ne puis-je, avec vous, goûter le vrai bonheur
Je vous aime, ô ma belle, et ma plume en délire
Couche sur le papier ce que je n'ose dire
Avec soin, de mes vers, lisez le premier mot
Vous saurez quel remède apporter à mes maux.

Fin du dialogologue

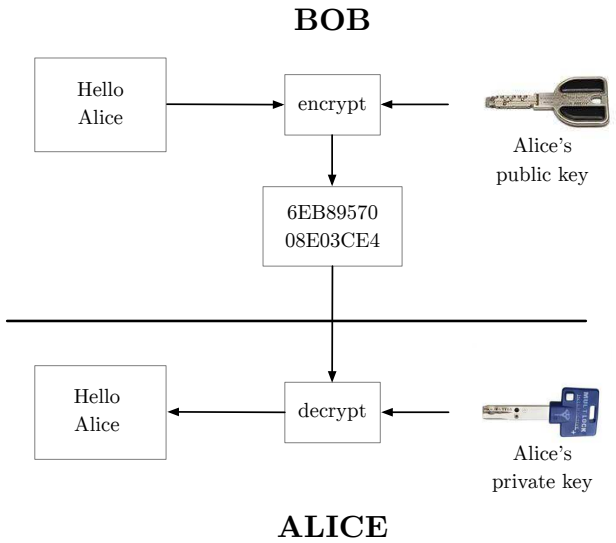
Cette grande faveur que votre ardeur réclame
Nuit peut-être à l'honneur mais répond à ma flamme.

Cryptologie

Généalogie

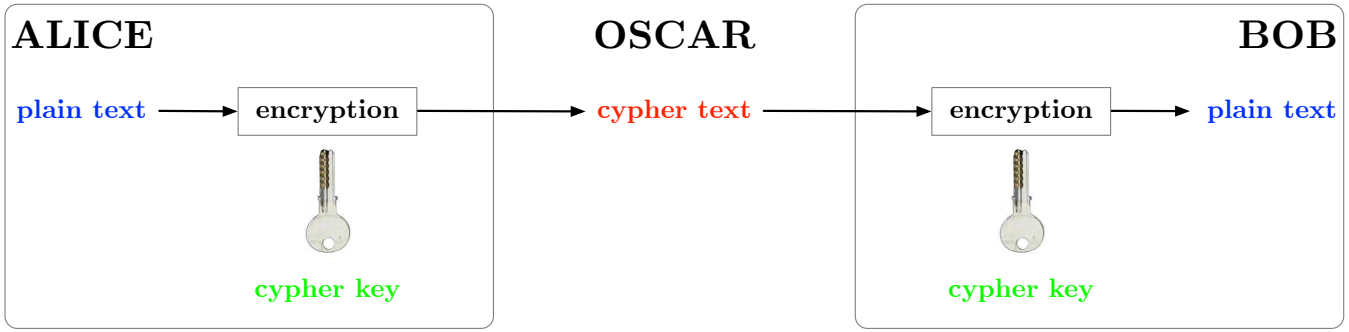
Période moderne

- ▷ 1977 : Data encryption Standard (DES)
- ▷ 1998 : Advanced Encryption Standard (AES)
- ▷ 1976 : Cryptage par clés publiques (W. Diffie and M. Hellman)
- ▷ 1978 : RSA Algorithm
- ▷ 1991 : Pretty Good Privacy (PGP)



Cryptologie

Définitions générales



Définitions

- ▷ Cryptage symétrique : utilisant une même clef pour le chiffrage et déchiffrage
- ▷ Cryptage asymétrique : utilisant des clefs différentes
- ▷ Cryptage par bloc ou par flot.

Attaques

- ▷ Cypher text only attack : accès uniquement à des textes cryptés
- ▷ Known plain text attack : accès à des textes connus cryptés
- ▷ Chosen text attack : accès aux textes cryptés de textes choisis

Cryptologie

César, Trithème, Vigenère

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

Cryptologie

Chiffre de César

Principe

Décalage de l'alphabet d'un nombre défini par la clé `K`.

Exemple (`K = B`)

```
Texte :   N O W I S T H E T I M E
Clé :     B B B B B B B B B B B B
Chiffre : O P X J T U I F U J N F
```

Décryptement

Par recherche exhaustive des clefs

Cryptologie

Chiffre de Trithème

Principe

Suite de décalages de César : la première lettre n'est pas décalée, la deuxième d'un cran, la deuxième de deux crans, etc.

Exemple

```
Texte :   N O W I S T H E T I M E
Clé :     A B C D E F G H I J K L
Chiffre : N P Y L W Y N L B R W P
```

Cryptologie

Chiffre de Vigenère

Principe

Décalage décidé par une clé pré-définie. Plus la clé est longue, plus le code est sûr.
Variante : utilisation du texte initial ou crypté comme clé.

Exemple (`K = TYPE`)

```
Texte :   N O W I S T H E T I M E
Clé :     T Y P E T Y P E T Y P E
Chiffre : G M L M L R W I M G B I
```

Décryptement

Résiste à la méthode des fréquences
Décrypté indépendamment par Babbage/Kasiski
Indécryptable pour une clé aussi longue que le texte clair (masque jetable)

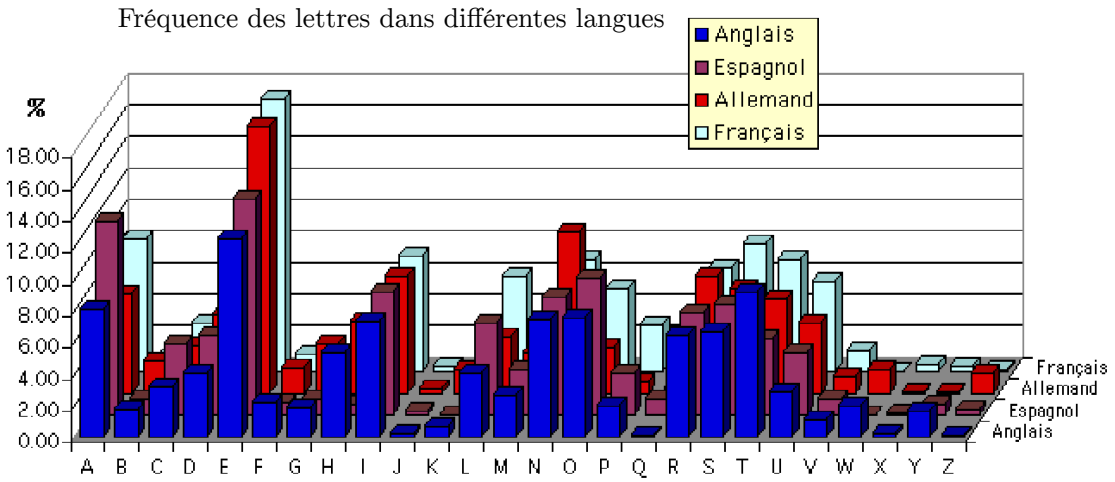
Cryptologie

Méthode des fréquences

Principe

Connaissant la langue du cryptogramme, remplacer :

- ▷ la lettre la plus fréquente du cryptogramme par la lettre la plus fréquente de la langue considérée
- ▷ la deuxième par la deuxième plus fréquente de la langue
- ▷ etc.

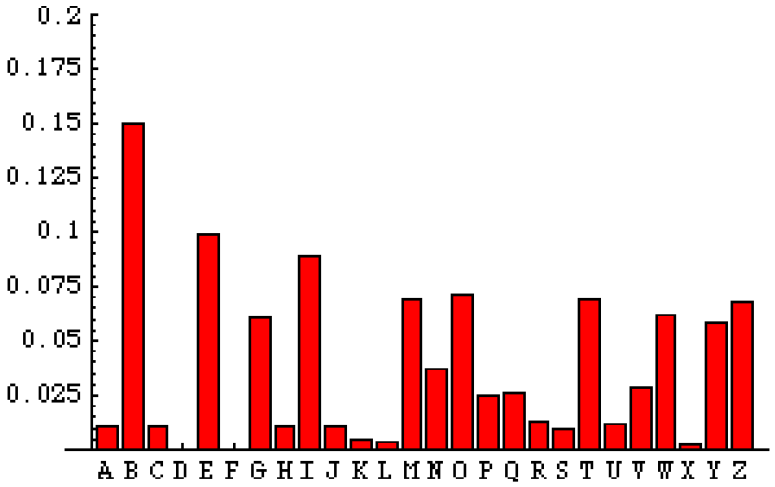


Cryptologie

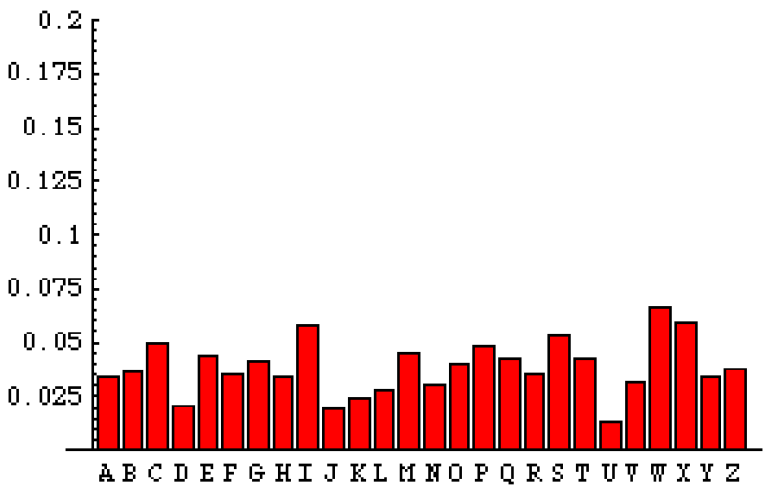
Chiffre de Vigenère

Résistance à la méthode des fréquence

Effet d'égalisation de l'histogramme



Substitution simple



Chiffre de Vigenère

Cryptologie

Chiffre de Vigenère

Décryptement (méthode de Babbage, 1854)

Recherche des répétitions de séquences de lettres dans le cryptogramme :

KQOWE FVJPU JUUNU KGLME KJINM WUXFQ MKJBG WRLFN FGHUD WUUMB SVLPS
NCMUE KQCTE SWREE KOYSS IWCTU AXYOT APXPL WPNTC GOJBG FQHTD WXIZA
YGFFN SXCSE YNCTS SPNTU JNYTG GWZGR WUUNE JUUQE APYME KQHUI DUXFP
GUYTS MTFFS HNUOC ZGMRU WEYTR GKMEE DCTVR ECFBD JQCUS WVBPN LGOYL
SKMTE FVJJT WWMFM WPNME MTMHR SPXFS SKFFS TNUOC ZGMDO EOYEE KCPJR
GPMUR SKHFR SEIUE VGOYC WXIZA YGOSA ANYDO EOYJL WUNHA MEBFE LXYVL
WNOJN SIOFR WUCCE SWKVI DGMUC GOCRU WGNMA AFFVN SIUDE KQHCE UCPFC
MPVSU DGAVE MNYMA MVLFM AOYFN TQCUA FVFJN XKLNE IWCWO DCCUL WRIFT
WGMUS WOVMA TNYBU HTCOC WFYTN MGYTQ MKBBN LGFBT WOJFT WGNTE JKNEE
DCLDH WTVBU VGFBI JG

Cryptologie

Chiffre de Vigenère

Décryptement (méthode de Babbage, 1854)

Recherche de la longueur de la clé :

		longueurs de clef possibles			
séquences répétées	espace de répétition	2	3	5	19
WUU	95			x	x
EEK	200	x		x	
WXIZAYG	190	x		x	x
NUOCZGM	80	x		x	
DOEOY	45		x	x	
GMU	90	x	x	x	

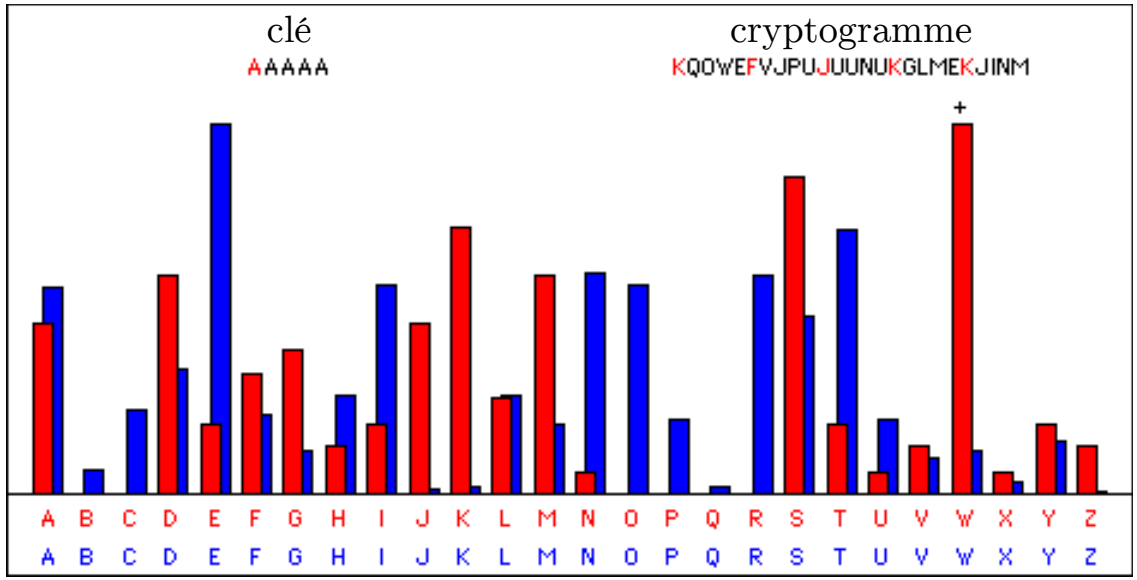
La clé est de longueur 5.

Cryptologie

Chiffre de Vigenère

Décryptement (méthode de Babbage, 1854)

Extraction des sous-cryptogrammes associés à chacun des caractères de la clé
Application de la méthode des fréquences à chacun pour retrouver chaque clé



Le décalage est de 18. La première clé est S.

Cryptologie

Chiffres de Feistel

Principe

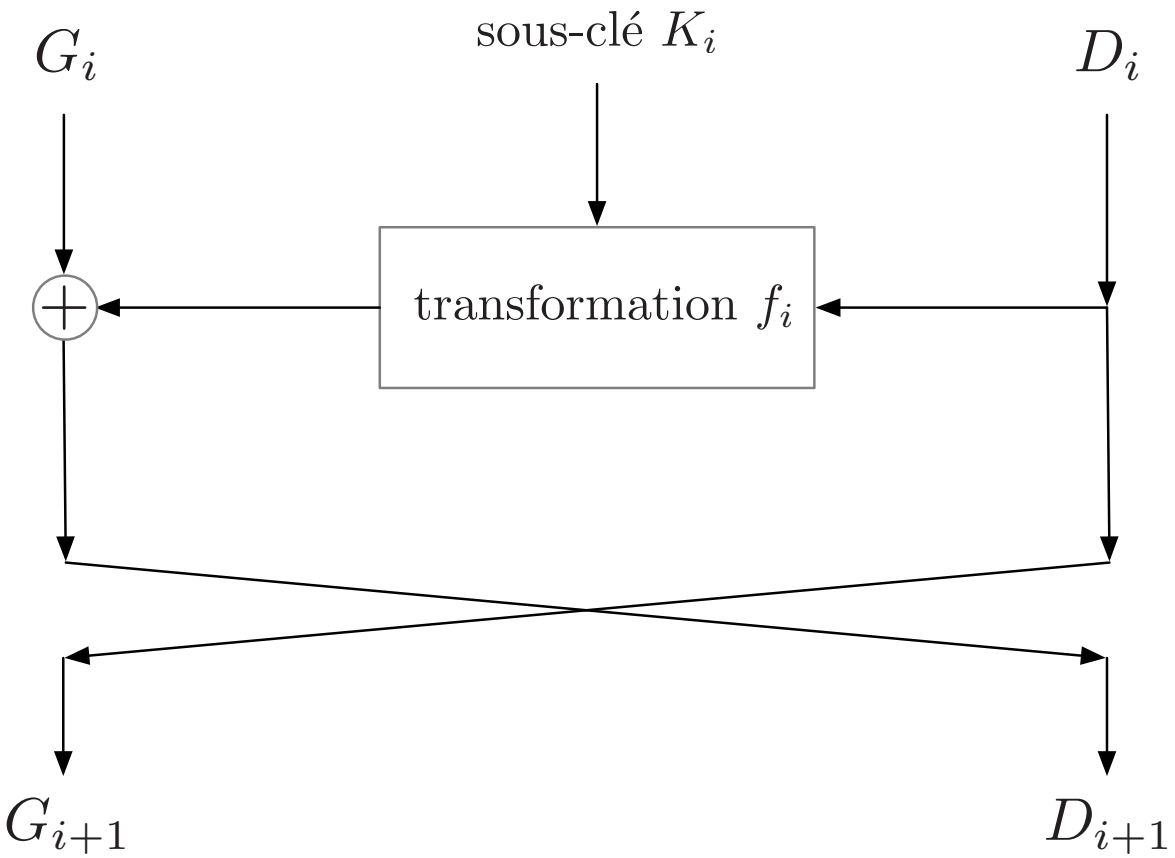
- ▷ Un bloc de texte en clair est découpé en deux
- ▷ Une transformation, dite *ronde* ou *tour*, est appliquée à l'une des moitiés
- ▷ Le résultat est combiné à l'autre moitié par une opération simple, e.g., XOR
- ▷ Les deux demi-blocs sont intervertis pour le tour suivant

Déchifrement

Le chiffrement et le déchiffrement sont structurellement identiques

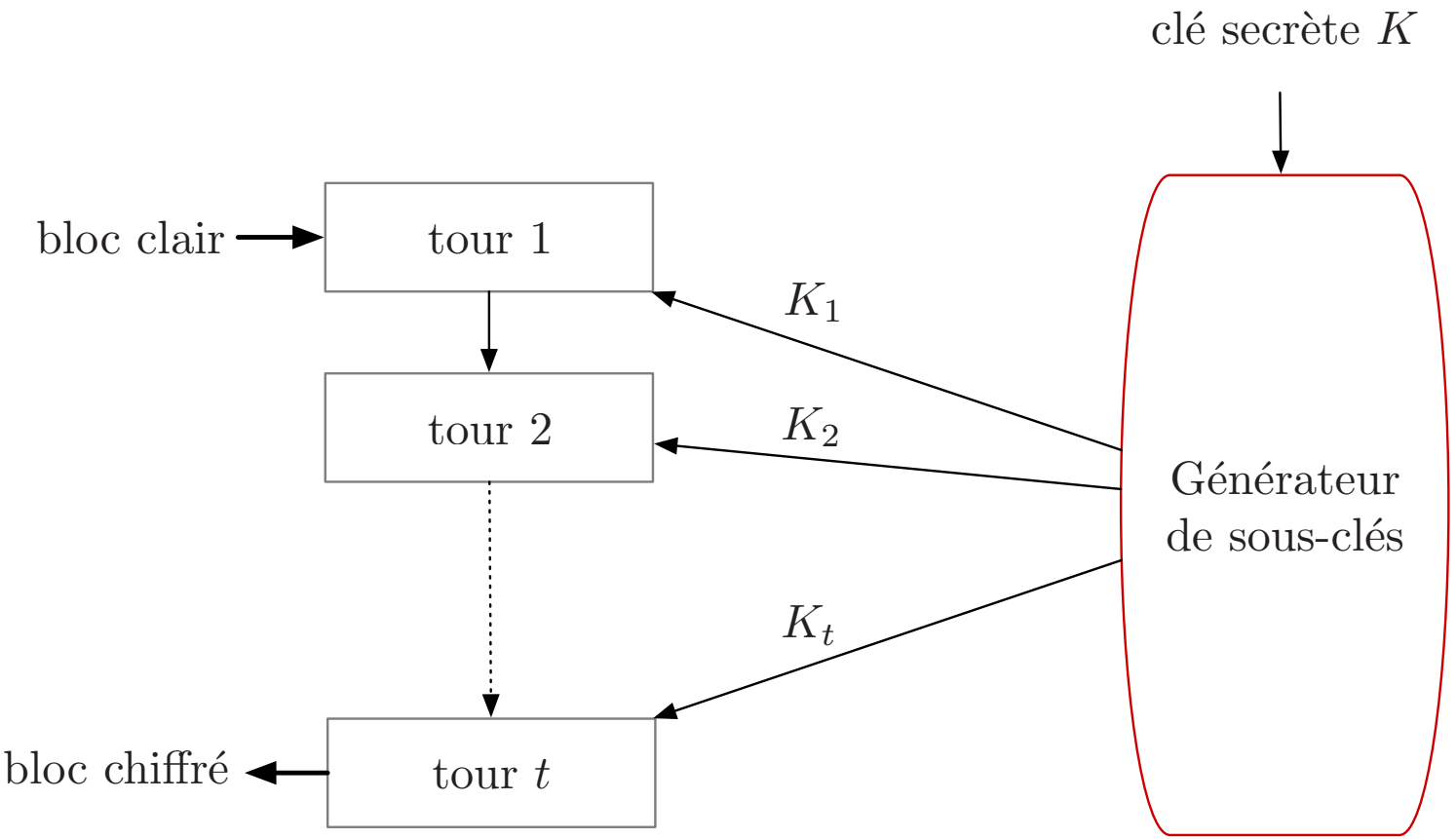
Cryptologie

Chiffres de Feistel



Cryptologie

Chiffres de Feistel



Exemple

On considère un réseau de Feistel à 2 tours appliqué à un message de 4 bits.
On suppose que les 2 clés nécessaires conduisent aux transformations suivantes :

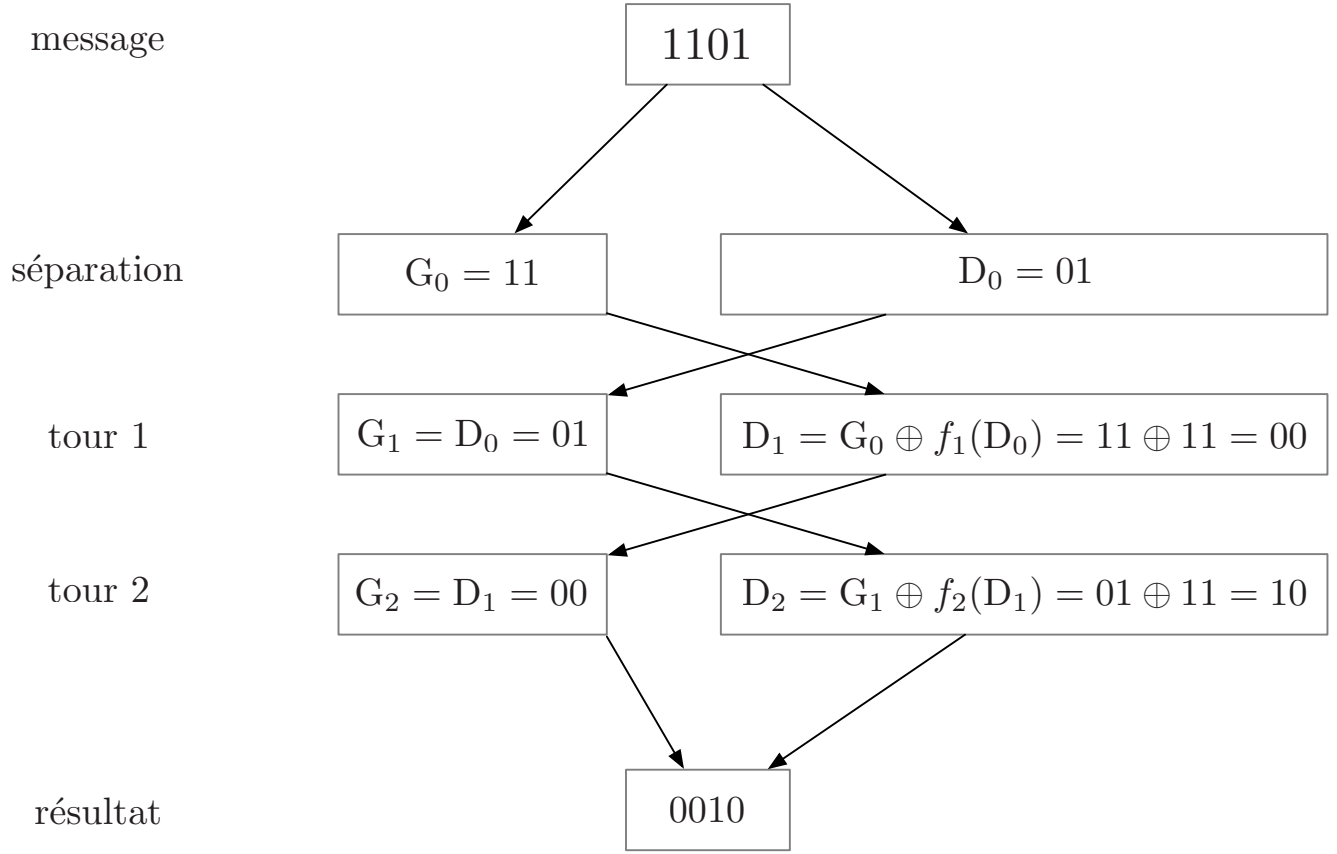
in	f_1	out	in	f_2	out
00	$\rightarrow$	01	00	$\rightarrow$	11
01	$\rightarrow$	11	01	$\rightarrow$	00
10	$\rightarrow$	10	10	$\rightarrow$	00
11	$\rightarrow$	01	11	$\rightarrow$	01

Remarque

Ni f_1, ni f_2, ne sont bijectives
On note $\oplus$ l'opérateur XOR : $0 \oplus 0 = 1 \oplus 1 = 0 \quad 0 \oplus 1 = 1 \oplus 0 = 1$

Cryptologie

Chiffres de Feistel



Cryptologie

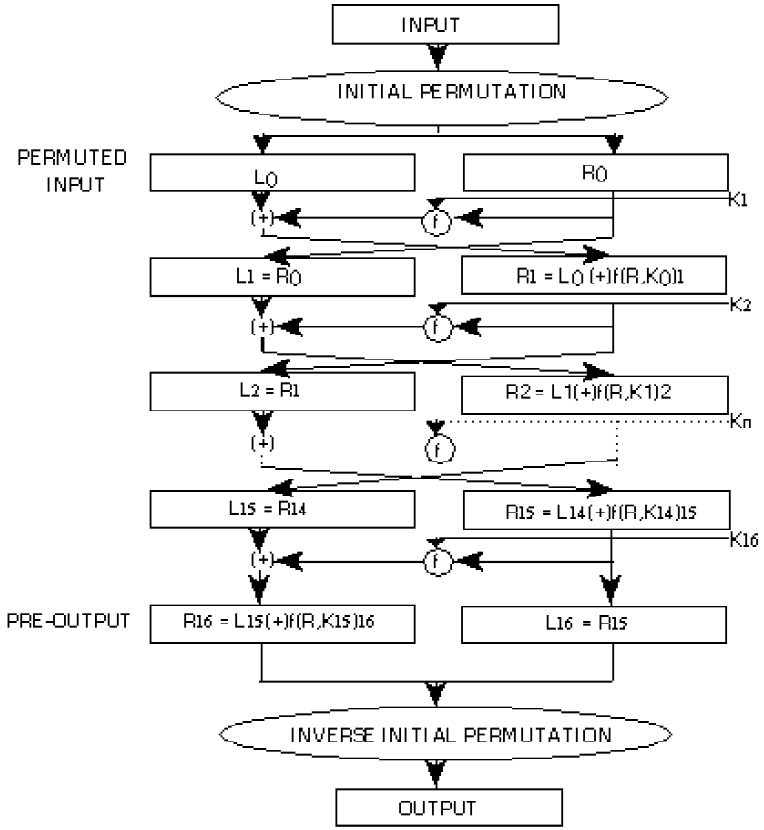
Data Encryption System (DES)

Principe

- ▷ Algorithme développé par IBM dans les années 70
- ▷ Adopté comme standard US par le NBS (FIPS 46-2) en 1977
- ▷ Taille des blocs : 64 bits
- ▷ Taille des clés : 56 bits
- ▷ Schéma de Feistel à 16 tours

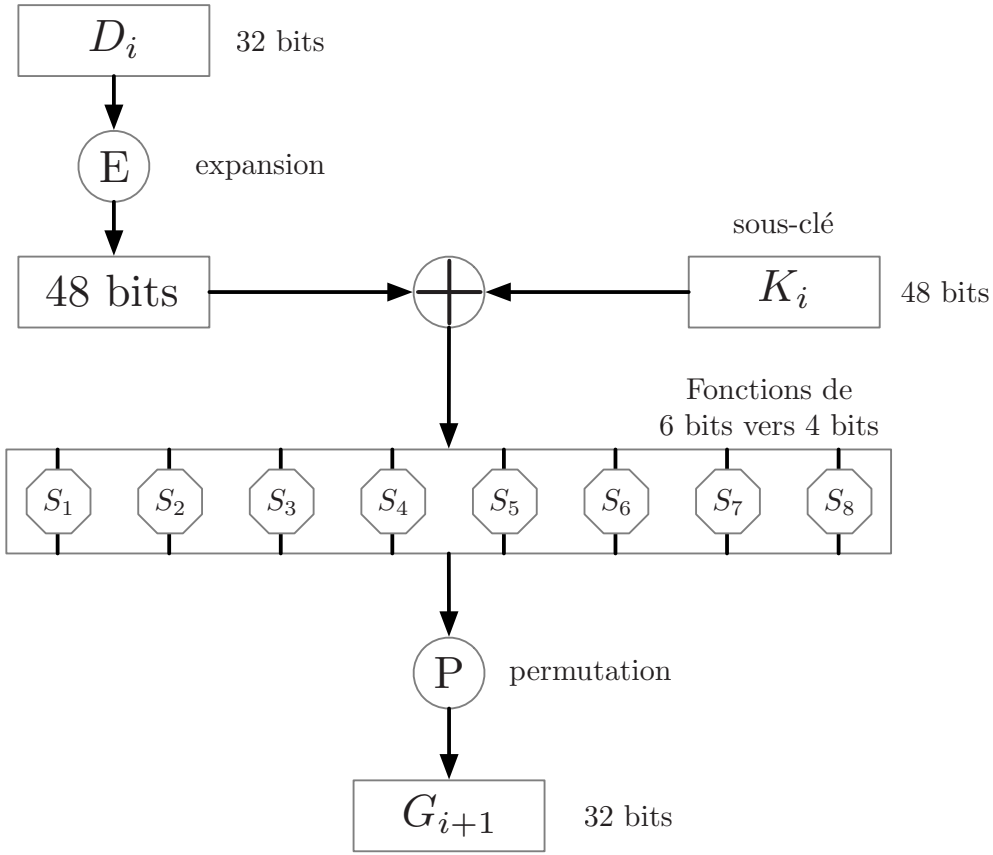
Cryptologie

Data Encryption System (DES)



Cryptologie

Data Encryption System (DES)



Cryptologie

Data Encryption System (DES)

Informations complémentaires

- ▷ Expansion de 32 bits à 48 bits par duplication de bits
- ▷ Chaque boîte S est codées comme un tableau de $2^6 = 64$ entrées
- ▷ A chaque tour, choix de 48 des 56 bits de la clé pour former la sous-clé K_i
- ▷ Sélection de K_i par permutation circulaire de la clé et tables d'extraction

Attaques

- ▷ Avant 1990, attaques contre des versions réduites (inférieures à 16 tours)
- ▷ Problème 1 : taille des clés (recherche en $\mathcal{O}(2^{56})$ réaliste)
- ▷ Problème 2 : taille du bloc (attaque avec $\mathcal{O}(2^{32})$ messages)
- ▷ DES demeure malgré tout un algorithme très bien conçu

Cryptologie

Advanced Encryption System (AES)

Principe

- ▷ Connu sous le nom d'algorithme de Rijndael
- ▷ Ne repose pas sur un schéma de Feistel
- ▷ Standard américain (NIST, 2000), en remplacement de DES
- ▷ Actuellement le plus utilisé et le plus sûr
- ▷ Taille des blocs : 128 bits
- ▷ Taille des clés : 128, 192 et 256 bits
- ▷ Schéma à 10 tours (AES-128), 12 tours (AES-192), 14 tours (AES-256)

Cryptologie

Advanced Encryption System (AES)

Données

Les données sont stockées dans une matrice carrée de taille $4 \times 4 = 16$

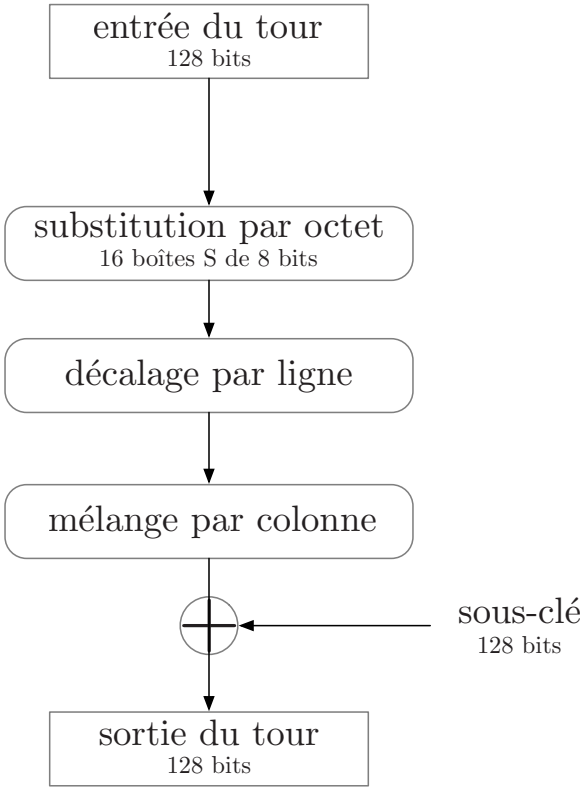
- ▷ Données stockées dans une matrice carrée de taille $4 \times 4 = 16$
- ▷ Chaque entrée X_i de la matrice contient 1 octet
- ▷ Taille de la représentation interne : $8 \times 16 = 128$ bits

X_1	X_2	X_3	X_4
X_5	X_6	X_7	X_8
X_9	X_{10}	X_{11}	X_{12}
X_{13}	X_{14}	X_{15}	X_{16}

Cryptologie

Advanced Encryption System (AES)

Fonction de tour



Substitution par octet

La boîte S est une fonction fixée de 8 bits vers 8 bits :

- ▷ définie à partir d'un tableau de $2^8 = 256$ entrées
- ▷ nécessite 256 octets de mémoire

X_1	X_2	X_3	X_4
X_5	X_6	X_7	X_8
X_9	X_{10}	X_{11}	X_{12}
X_{13}	X_{14}	X_{15}	X_{16}

$\Longrightarrow$

Y_1	Y_2	Y_3	Y_4
Y_5	Y_6	Y_7	Y_8
Y_9	Y_{10}	Y_{11}	Y_{12}
Y_{13}	Y_{14}	Y_{15}	Y_{16}

$$Y_i = S(X_i) \qquad i = 1, \ldots, 16$$

Définition de la boîte S

La boîte S repose sur une opération algébrique dans $GF(2^8)$:

$$S(X) = \text{affine}(B) \quad \text{avec} \quad B = X^{-1}$$

$$\begin{bmatrix} s_0 \\ s_1 \\ s_2 \\ s_3 \\ s_4 \\ s_5 \\ s_6 \\ s_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

Définition de la boîte S

octet de poids faible

octet de poids fort	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
00	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
10	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
20	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
30	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
40	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
50	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
60	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
70	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
80	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
90	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A0	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B0	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C0	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D0	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E0	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F0	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

exemple : $S(9\text{A}) = \text{B8}$

Définition de la boîte S^{-1}

octet de poids faible

octet de poids fort	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f
00	52	09	6A	D5	30	36	A5	38	BF	40	A3	9E	81	F3	D7	FB
10	7C	E3	39	82	9B	2F	FF	87	34	8E	43	44	C4	DE	E9	CB
20	54	7B	94	32	A6	C2	23	3D	EE	4C	95	0B	42	FA	C3	4E
30	08	2E	A1	66	28	D9	24	B2	76	5B	A2	49	6D	8B	D1	25
40	72	F8	F6	64	86	68	98	16	D4	A4	5C	CC	5D	65	B6	92
50	6C	70	48	50	FD	ED	B9	DA	5E	15	46	57	A7	8D	9D	84
60	90	D8	AB	00	8C	BC	D3	0A	F7	E4	58	05	B8	B3	45	06
70	D0	2C	1E	8F	CA	3F	0F	02	C1	AF	BD	03	01	13	8A	6B
80	3A	91	11	41	4F	67	DC	EA	97	F2	CF	CE	F0	B4	E6	73
90	96	AC	74	22	E7	AD	35	85	E2	F9	37	E8	1C	75	DF	6E
A0	47	F1	1A	71	1D	29	C5	89	6F	B7	62	0E	AA	18	BE	1B
B0	FC	56	3E	4B	C6	D2	79	20	9A	DB	C0	FE	78	CD	5A	F4
C0	1F	DD	A8	33	88	07	C7	31	B1	12	10	59	27	80	EC	5F
D0	60	51	7F	A9	19	B5	4A	0D	2D	E5	7A	9F	93	C9	9C	EF
E0	A0	E0	3B	4D	AE	2A	F5	B0	C8	EB	BB	3C	83	53	99	61
F0	17	2B	04	7E	BA	77	D6	26	E1	69	14	63	55	21	0C	7D

exemple : $S^{-1}(\text{B8}) = \text{9A}$

Cryptologie

Advanced Encryption System (AES)

Décalage par ligne

Décalage circulaire de i cases à gauche pour la ligne i, avec $0 \leq i \leq 3$

X_1	X_2	X_3	X_4
X_5	X_6	X_7	X_8
X_9	X_{10}	X_{11}	X_{12}
X_{13}	X_{14}	X_{15}	X_{16}

$\Longrightarrow$

X_1	X_2	X_3	X_4
X_6	X_7	X_8	X_5
X_{11}	X_{12}	X_9	X_{10}
X_{16}	X_{13}	X_{14}	X_{15}

Mélange par colonne

La fonction de mélange est appliquée à chaque colonne. Les opérations sont effectuées dans $GF(2^8)$.

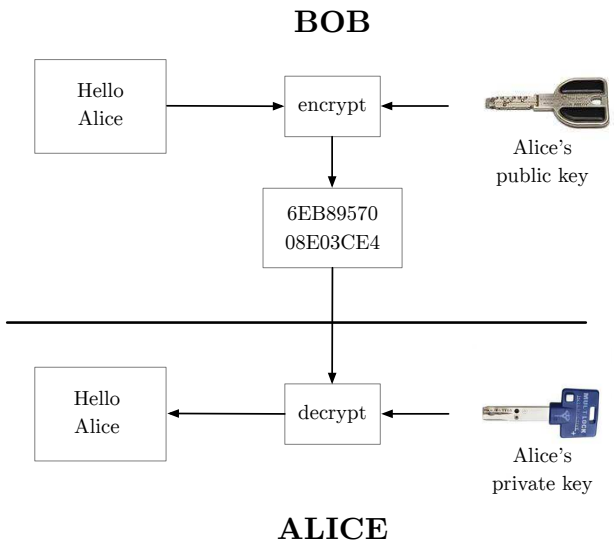
$$\text{MixColumn}\left(\begin{bmatrix} X_a \\ X_b \\ X_c \\ X_d \end{bmatrix}\right) = \begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \begin{bmatrix} X_a \\ X_b \\ X_c \\ X_d \end{bmatrix}$$

Cryptologie

Cryptage asymétrique

Principe

- ▷ Chaque utilisateur possède 2 clés, une clé privée et une clé publique
- ▷ Pour transmettre un message à Alice, Bob utilise la clé publique d'Alice
- ▷ Alice décrypte le message de Bob avec sa clé privée



Cryptologie

Cryptosystème RSA

1. Choix de la clé par Alice

- ▷ Elle choisit deux grands entiers naturels premiers p et q
- ▷ Elle calcule le produit $n = p \cdot q$
- ▷ Elle choisit un entier e premier avec $(p-1) \cdot (q-1)$
- ▷ Elle publie sa clé publique (n, e)

Exemple

- ▷ $p = 53$ et $q = 97$, gardés secret
- ▷ $n = 53 \cdot 97 = 5141$
- ▷ $e = 7$, premier avec $52 \cdot 96 = 4992$
- ▷ publication de $(5141, 7)$

2. Envoi par Bob d'un message chiffré à Alice

- ▷ Il recherche la clé publique (n, e) d'Alice
- ▷ Il découpe son message en blocs B de taille inférieure à n
- ▷ Il crypte chaque bloc par : $C = B^e$ modulo n
- ▷ Il envoie les blocs C à Alice

Exemple

- ▷ message à transmettre : je vous aime (sans espaces)
- ▷ traduit par : 10 05 22 15 21 19 01 09 13 05 (positions dans l'alphabet)
- ▷ message à crypter en bloc de taille 3 :

010 052 215 211 901 091 305

- ▷ cryptogramme transmis à Alice

0755 1324 2823 3550 3763 2237 2052

3. Déchiffrement par Alice du message de Bob

▷ Elle calcule sa clé privée d de déchiffrage telle que

$$e \cdot d \text{ modulo } ((n-1)(q-1)) = 1$$

▷ Elle déchiffre chaque bloc C par : $B = C^d \text{ modulo } n$

Exemple

▷ cryptogramme reçu par Alice :

0755 1324 2823 3550 3763 2237 2052

▷ message décrypté :

010 052 215 211 901 091 305

c'est-à-dire : jevousaime

Cryptologie

Cryptosystème RSA

Intérêt de la méthode

- ▷ impossibilité en pratique de retrouver p et q à partir de n
- ▷ temps de calcul croissant exponentiellement avec la longueur de la clé
- ▷ renouvellement des clés que si la clé privée est compromise

Taille recommandée des clés RSA : au moins 2048 bits

Cryptologie

Test de primalité de Fermat

Petit théorème de Fermat

Si p est un nombre premier, et si a est premier avec p, alors :

$$a^{p-1} - 1 \text{ est divisible par } p$$

ou encore :

$$a^{p-1} = 1 \text{ modulo } p$$

Le réciproque est fausse : il existe des nombres p non premiers vérifiant la condition.

Test de primalité

Si x n'est pas premier, alors $a^{x-1} - 1$ est de façon improbable divisible par x pour une valeur arbitraire de a.

Test PGP

Si $2^{x-1} = 3^{x-1} = 5^{x-1} = 7^{x-1} = 1 \text{ modulo } x$, alors x est probablement premier.

Cryptologie

Signature électronique avec RSA

Principe

La clé privée peut être utilisée par Alice pour chiffrer.
La clé publique sert alors à déchiffrer.

Si l'on peut déchiffrer à un message avec la clé publique d'Alice, c'est forcément Alice qui a envoyé celui-ci après l'avoir crypté avec sa clé privée.

Cryptologie

Pretty Good Privacy (PGP)

Les méthodes de cryptage asymétriques sont lourdes à mettre en œuvre, contrairement aux méthodes symétriques. PGP combine les 2 approches.

1. **Alice crypte son envoi :**
   - ▷ Elle génère une clé de session aléatoire
   - ▷ Elle code le message avec la clé de session symétrique
   - ▷ Elle code la clé de session avec la clé publique de Bob

2. **Bob décrypte le message :**
   - ▷ Il décode la clé de session avec sa clé privée
   - ▷ Il décode le message avec la clé de session