CRYPTOGRAPHIE

Chiffrement symétrique

E. Bresson

SGDN/DCSSI
Laboratoire de cryptographie

Emmanuel.Bresson@sgdn.gouv.fr

I. CHIFFREMENT SYMÉTRIQUE

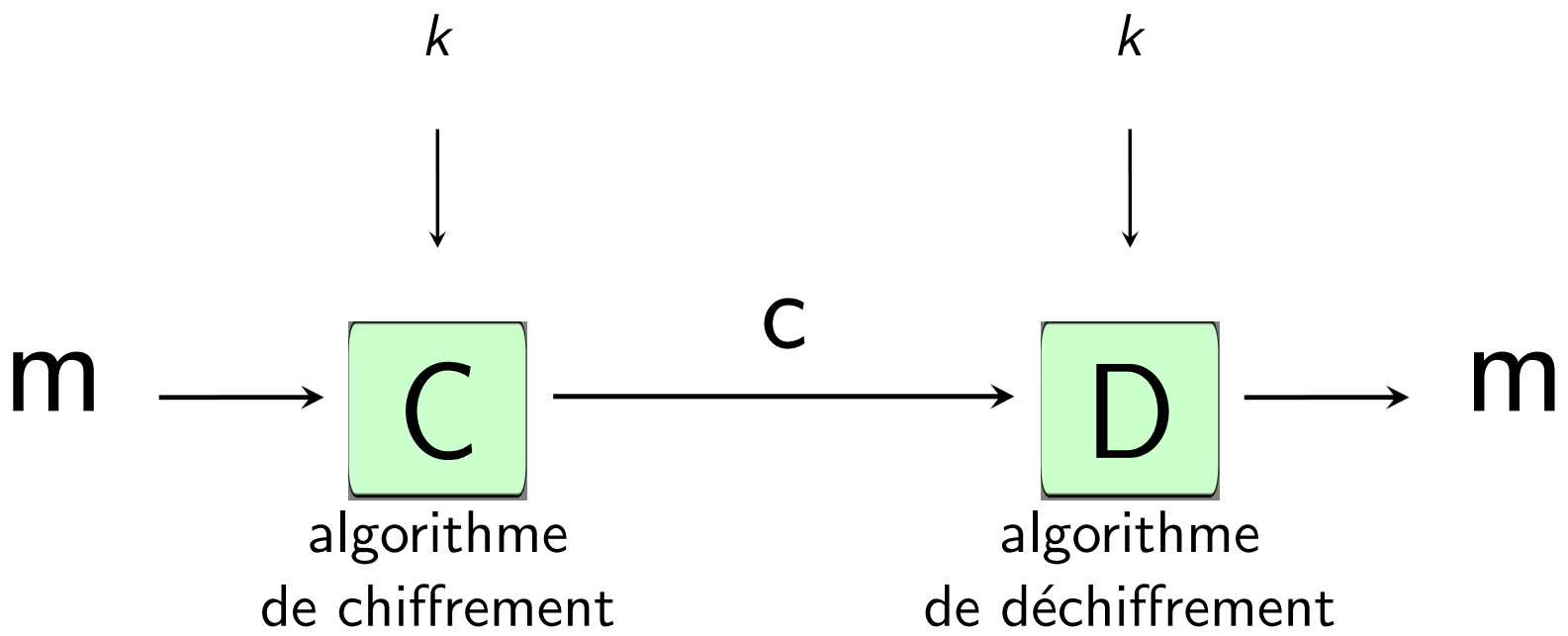
I.1. GÉNÉRALITÉS

Organisation de la section « GÉNÉRALITÉS »

Chiffrement à clé secrète
Chiffrement par blocs
Schémas de Feistel

LE CHIFFREMENT SYMÉTRIQUE

La clé de chiffrement est la même que la clé de déchiffrement



CARACTÉRISTIQUES DU CHIFFREMENT SYMÉTRIQUE

Avantages

- Systèmes rapides (implantation matérielle)
- Clés relativement courtes (128 ou 256 bits)

Inconvénients

- Gestion des clés difficiles (nombreuses clés)
- Point faible = échange d'un secret

LE CHIFFREMENT SYMÉTRIQUE MODERNE

2 grandes familles: blocs et flots

Chiffrement par blocs: les messages sont découpés en blocs

- DES: blocs de 64 bits, clés de 56 bits
- IDEA: blocs de 64 bits, clés de 128 bits
- AES: blocs de 128 bits, clés de 128, 256 bits
- ...

Chiffrement par flots: les données sont traitées en flux

- Pseudo-Vernam : on « XOR » un pseudo-aléa au flux
- RC4 : chiffrement octet par octet
- ...

DÉFINITION FORMELLE

Un chiffrement symétrique est défini par trois algorithmes:

Algorithme de génération des clés

$\mathcal{KG}(\ell) = k$: à partir d'un paramètre de sécurité, il produit une clé aléatoire de ℓ bits

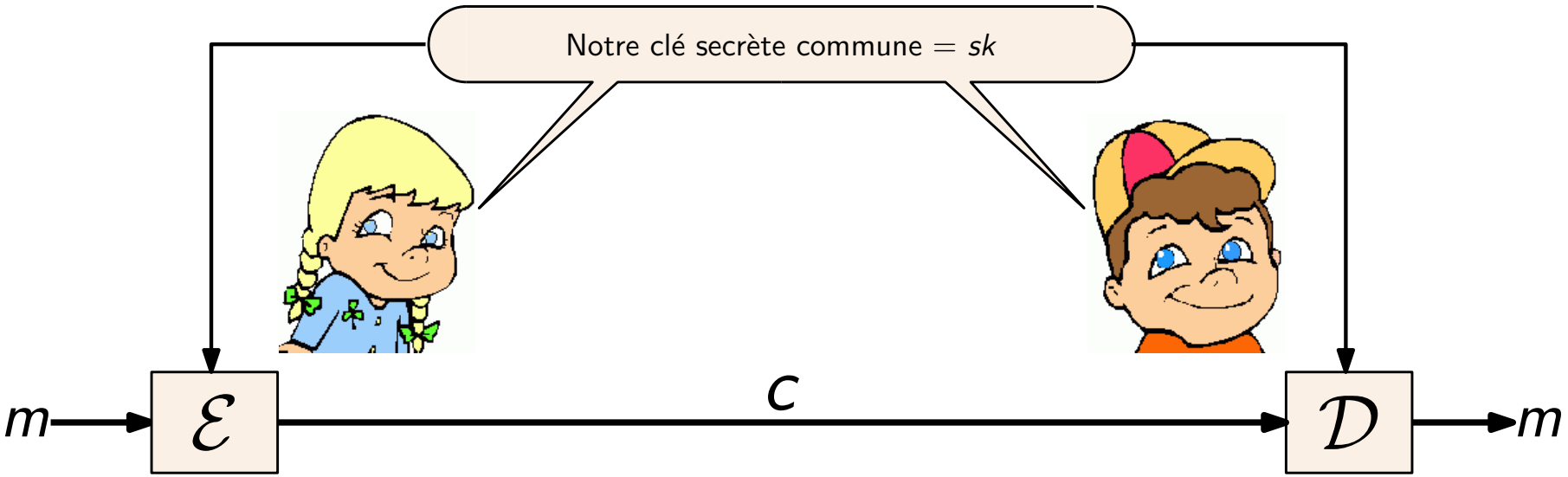
Algorithme de chiffrement

$\mathcal{E}_k(m) = c$: produit le chiffré, par la clé k, d'un message m

Algorithme de déchiffrement

$\mathcal{D}_k(c) = m$: utilise la clé pour retrouver m à partir de c

PROPRIÉTÉ



Consistance

Le chiffrement est inversible: $\mathcal{D}_k(\mathcal{E}_k(m)) = m$

PRINCIPES DE CONCEPTION

César, scytales, Vigenère : peu sûrs...

Vernam : peu pratique...

Comment construire des schéma à la fois sûrs et efficaces ?

C. Shannon a montré que la combinaison de *confusion* et *diffusion* permettait d'obtenir une sécurité convenable

- confusion = masquer la relation entre le clair et le chiffré
- diffusion = cacher la redondance en répartissant l'influence d'un bit de clé sur tout le chiffré

LE CHIFFREMENT PAR BLOCS

Principe de fonctionnement

On chiffre des blocs de message de taille fixe (typiquement 64, 128 ou 256 bits)

Principaux algorithmes:

DES (NBS, 1977): blocs de 64 bits, clé de 56 bits

IDEA (Massey-Lai): blocs de 64 bits, clés de 128 bits

Rijndael (1997): blocs de 128 ou 256 bits, clé de 128, 192 ou 256 bits

HISTORIQUE

Avant 1975: chiffrements artisanaux (Vigenère, Hill)

1975–2000: le DES (*Data Encryption Standard*), mais aussi FEAL, IDEA, RC5,...

2000–... AES (*Advanced Encryption Standard*), RC6, CAMELLIA,...

CHIFFREMENTS PAR BLOCS: CARACTÉRISTIQUES

Bonnes performances, et sécurité bien étudiée

Avantages

Les *block ciphers* sont de façon générale:

- rapides (en matériel et en logiciel)
- bien conçus car théorie sous-jacente mature

Inconvénients

Principaux problèmes spécifiques aux blocs:

- utilisation des modes opératoires
- sécurité difficile à évaluer exactement

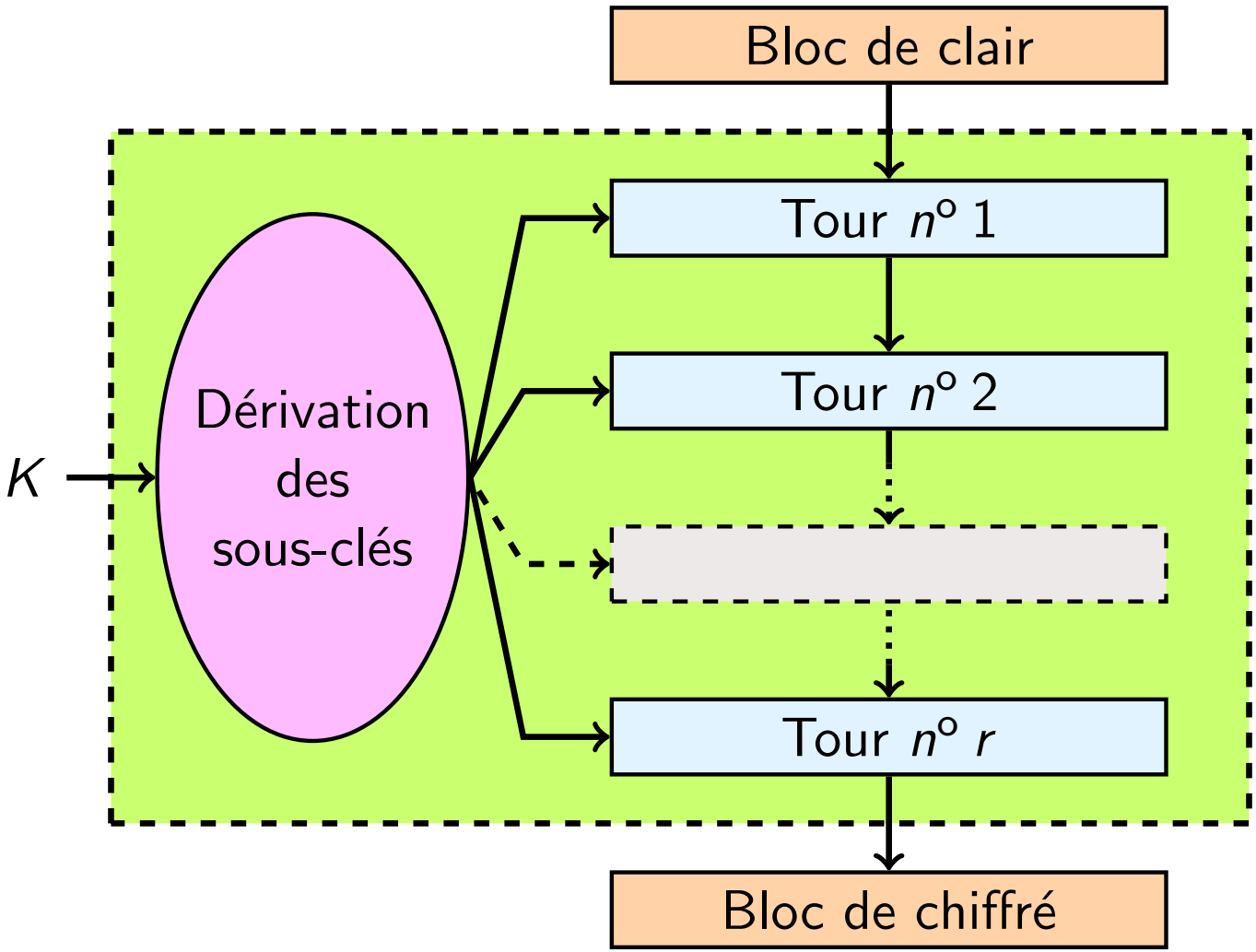
CONSTRUCTION DE CHIFFREMENT BLOCS

Principe général

Chiffrement **produit** = empilement de **tours**, utilisant chacun une **sous-clé**

- Construction itérative (et modulaire)
- Les sous-clés (ou *clés de tours*) sont dérivées de la clé K
- La *fonction de tour* est destinée à être optimisée (opérations simples, recherche de performances)

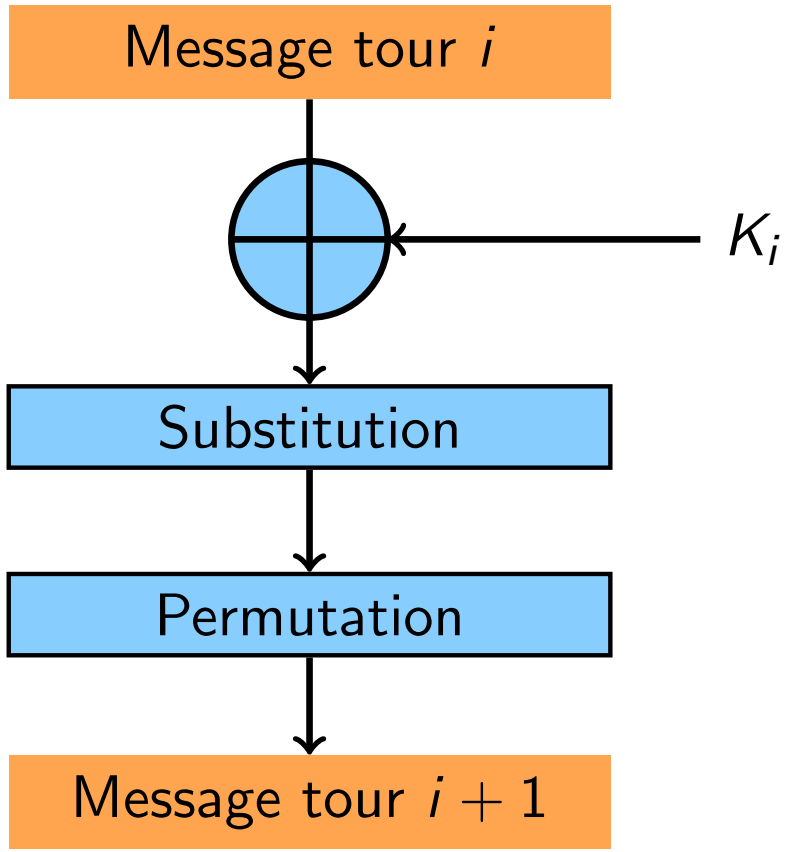
CONSTRUCTION DE CHIFFREMENT BLOCS



MÉTHODE Nº 1: SUBSTITUTIONS–PERMUTATIONS

Décomposition d'un tour:

- Intervention de la sous-clé
- Couche de substitution
- Couche de permutation



MÉTHODE Nº 2: SCHÉMA DE FEISTEL

Brique de base

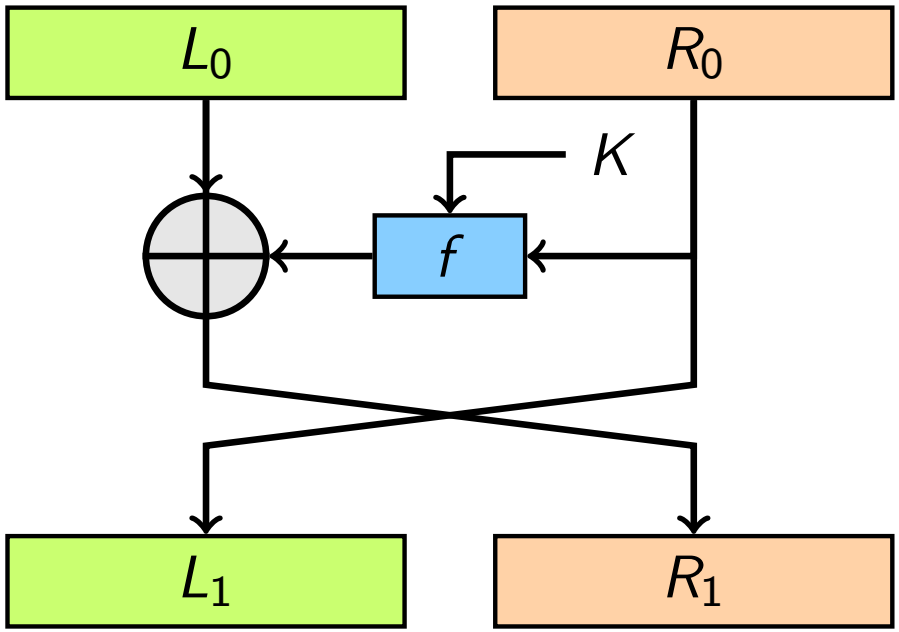
Obtenir une bijection sur $2n$ bits, à partir d'une fonction non-bijective sur n bits

Chiffrement:

$$L_1 = R_0$$
$$R_1 = L_0 \oplus f(R_0)$$

Le déchiffrement est trivial :

$$R_0 = L_1$$
$$L_0 = R_1 \oplus f(R_0)$$

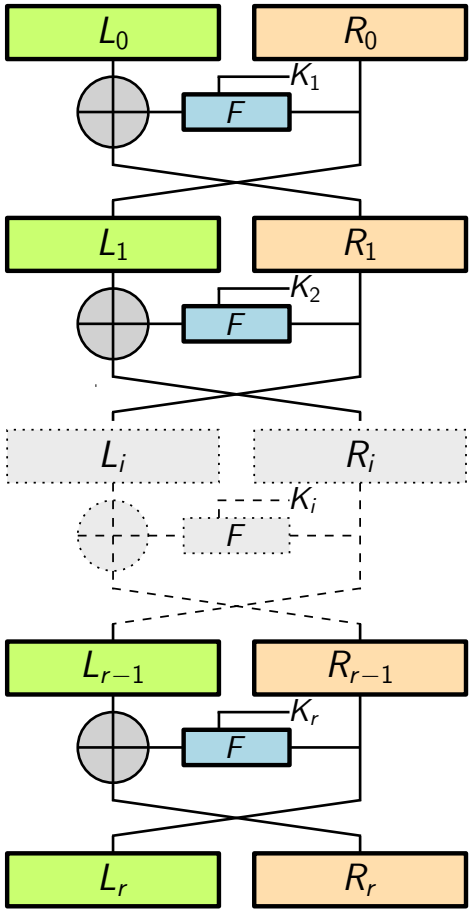


La fonction f est appelée la *fonction de confusion*

SCHÉMAS DE FEISTEL

Empilement de schéma de Feistel

Un tour isolé donne une bijection simpliste, la complexité croît de façon exponentielle avec le nombre de tours



I. CHIFFREMENT SYMÉTRIQUE

I.2. DATA ENCRYPTION STANDARD

Organisation de la section « DATA ENCRYPTION STANDARD »

Description
Implémentation et performances
Limites du DES

DES = DATA ENCRYPTION STANDARD

- Algorithme de chiffrement par blocs
- Utilise une clé de 56 bits et des blocs de 64 bits
- Feistel 16 tours avec des sous-clés de 48 bits
- Conçu et standardisé dans les années 70
- Devenu obsolète à cause de son âge

LE DATA ENCRYPTION STANDARD

Algorithme conçu par IBM au début des années 70 (*Lucifer*)

Repris et *corrigé* par la NSA (*National Security Agency*) pour le *National Bureau of Standards* (NBS) — adopté comme standard (FIPS 46-2) en 1977

- Clé réduite de 64 à 56 bits
- Boîtes S revues et corrigées

D'où une controverse sur les intentions de la NSA, qui ne sera (partiellement) résolue qu'en 1990...

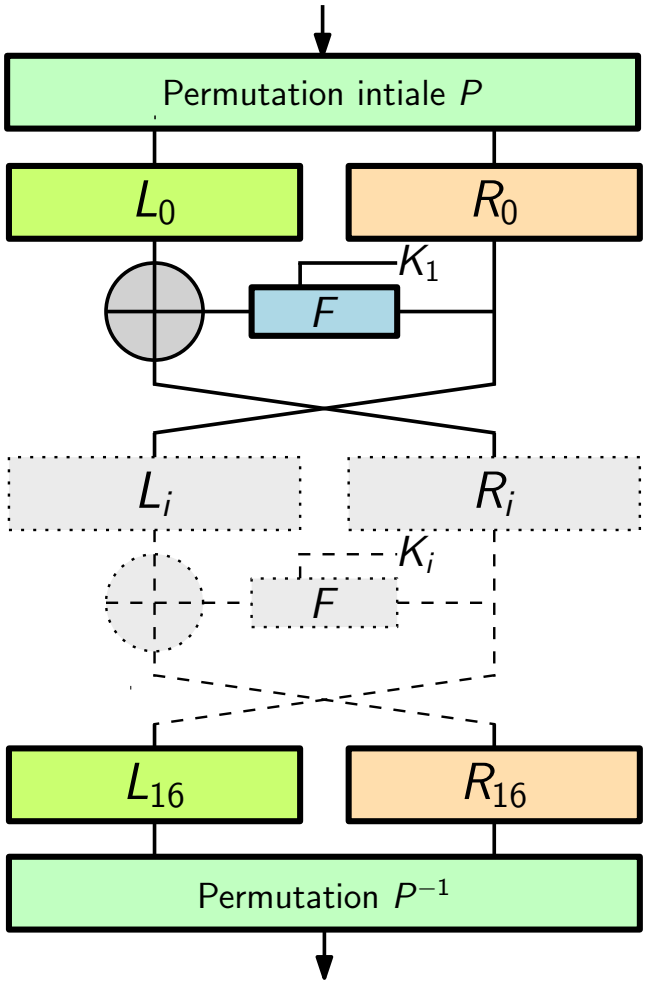
LE SCHÉMA DU DES

Application de la théorie de Shannon préconisant de mêler *confusion* et *diffusion*

- confusion = masquer la relation entre le clair et le chiffré
- diffusion = cacher la redondance en répartissant l'influence d'un bit de clé sur tout le chiffré

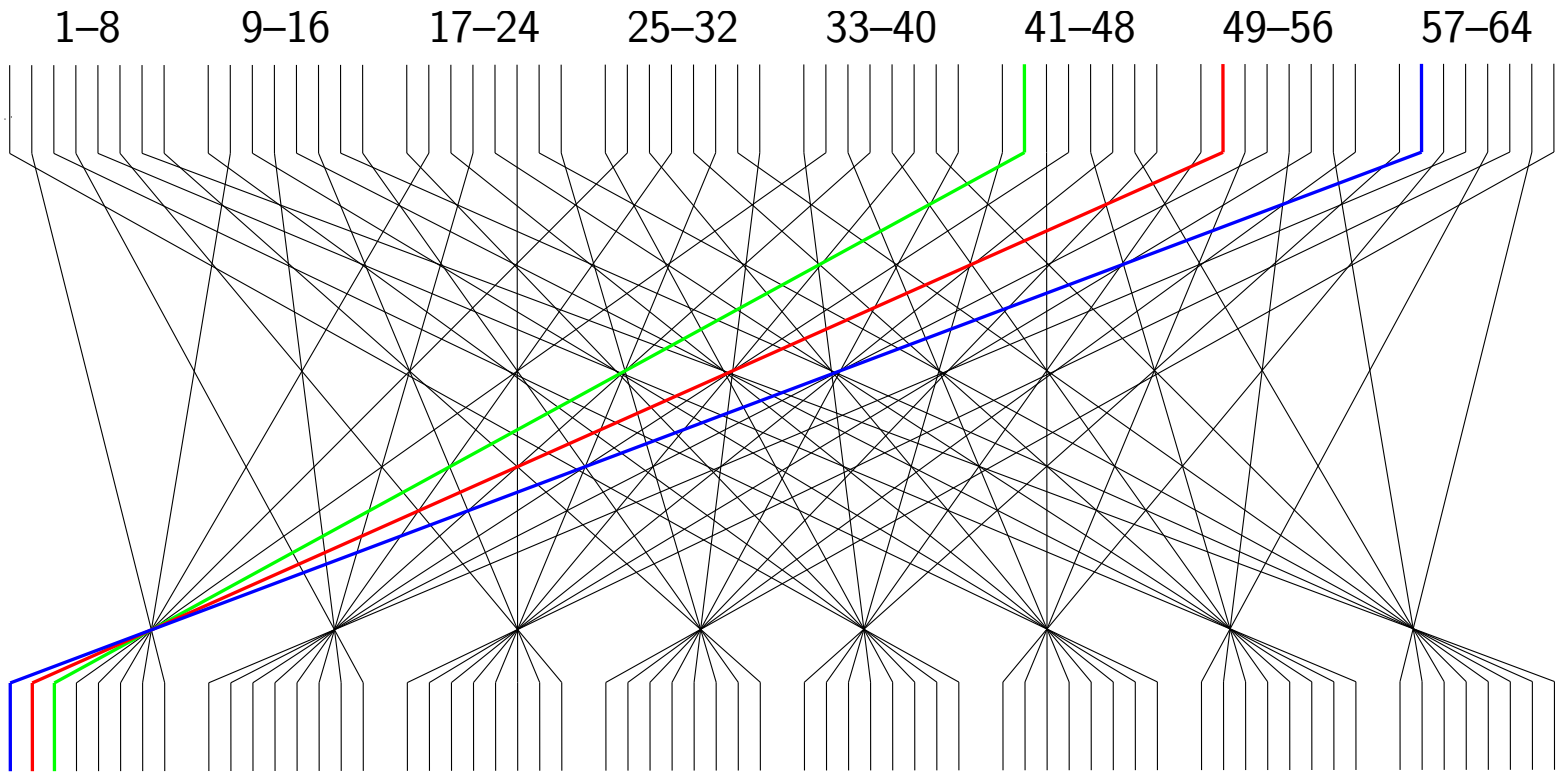
Le DES est un algorithme basé sur le schéma de Feistel, à 16 tours

LE SCHÉMA DU DES



LA PERMUTATION INITIALE

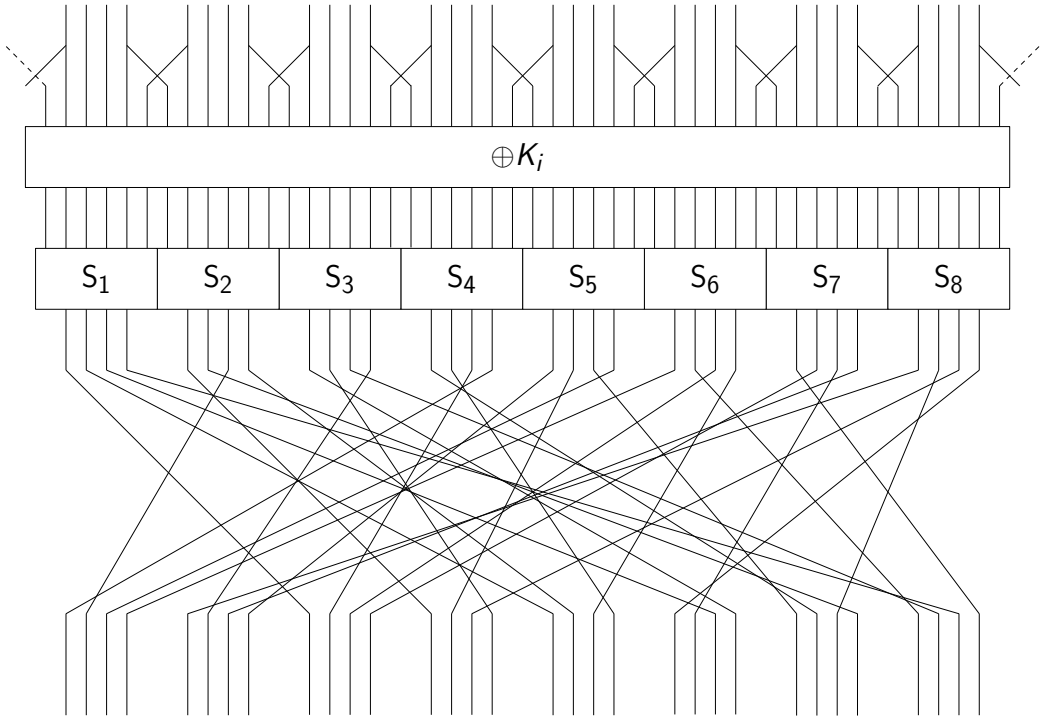
58 50 42 34 26 18 10 02 60 52 44 36 28 20 12 04
62 54 46 38 30 22 14 06 64 56 48 40 32 24 16 08
57 49 41 33 25 17 09 01 59 51 43 35 27 19 11 03
61 53 45 37 29 21 13 05 63 55 47 39 31 23 15 07



LA FONCTION F ET LES BOÎTES S

Dans le DES, la fonction f est une fonction de 32 bits vers 32 bits, constituée:

- d'une *expansion* de message de 32 vers 48 bits
- d'un XOR avec 48 bits dérivés de la clé
- de la concatenation de 8 sous-fonctions de 6 vers 4 bits, appelées *boîtes S*
- d'une permutation des 32 bits sortants



QUELQUES REMARQUES

- La fonction f n'a pas besoin d'être inversible (elle ne l'est pas)
- Expansion: certains bits sont dupliqués
- L'ajout de la sous-clé (un simple "xor") se fait sur 48 bits
- Les boîtes S assurent la non-linéarité (6 bits $\longrightarrow$ 4 bits, 8 fois)
- La permutation P contribue à la diffusion (en plus du "croisement" dans le Feistel)

LES BOÎTES S

Boîte S: tableau de $2^6 = 64$ entrées, à valeurs dans $2^4 = 16$

$$S_1(110101) = 1001 = 9$$

1010 ↓

S_1	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
11 →	4	1	14	8	13	6	2	11	15	12	**9**	7	3	10	5	0
	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

S_2	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

S_3	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

S_4	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

LES BOÎTES S: PROPRIÉTÉS

- Chaque ligne de chaque colonne est une permutation des entiers de 0 à 15
- La modification d'un bit en entrée provoque la modification d'au moins deux bits en sortie
- Pour tout $x \in \mathbb{F}_{2^6}$, les images de x et $x \oplus 001100$ diffèrent d'au moins deux bits
- Les images de x et $x \oplus 11ij00$ diffèrent
- Si l'on fixe un bit de l'entrée, la valeur en sortie d'un bit particulier (en fonction des 32 entrées possibles) est quasi-uniforme

LES BOÎTES S

S_5	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

S_6	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

S_7	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

S_8	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

PROPRIÉTÉS DU DES

- Le déchiffrement est identique au chiffrement, à condition de prendre les sous-clés dans l'ordre inverse

- **Complémentation:** pour tout message m et toute clé k:

$$DES_k(m) = \overline{DES_{\bar{k}}(\bar{m})}$$

PERFORMANCES DU DES

Performances

Le DES est très efficace, et particulièrement bien adapté aux implémentations matérielles

Logiciel: 192 Mbps (3 millions de blocs) sur Pentium III à 666MHz

Matériel: 1Gbps (16 millions de blocs) sur une puce DEC 250MHz, 50 000 transistors

- La structure de Feistel est rapide dans les deux sens
- Le *Key Scheduling* (dérivation des sous-clés) est très simple
- Les boîtes S se « câblent » facilement

HISTORIQUE DES ATTAQUES SUR DES

- Attaques sur des versions réduites (moins de 16 tours)
- 1990–92: cryptanalyse différentielle en 2^{47} (Biham-Shamir)
- 1993: cryptanalyse linéaire en 2^{43} (Matsui)
- 1997: attaque de Davies et Murphy, améliorée en 2^{45}

LES LIMITES DE DES

Taille des clés : la recherche exhaustive (2^{56}) devient réaliste

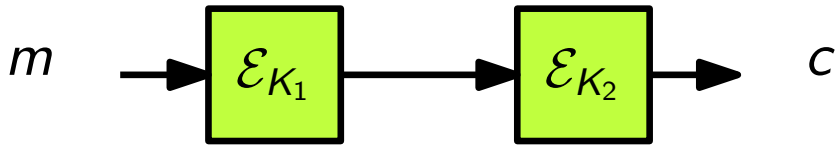
L'Electronic Frontier Foundation exhibe en juillet 1998 une machine « crackant » le DES en 9 jours maximum. Coût : 250,000 $

Taille des blocs : 64 bits est devenu court et présente des risques d'attaques en distinguabilité (2^{32})

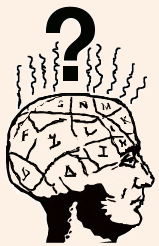
SOLUTION: LE DOUBLE DES ?

Idée

Deux chiffrements successifs avec deux clés différentes



Question



Atteint-on le niveau de sécurité d'une clé double (*i.e.*, recherche exhaustive en 2^{112}) ?

LE DOUBLE DES

Le double DES est à proscrire

Attaque par le milieu

Avec 2 couples (clair,chiffré) connus:
l'attaquant retrouve les deux clés secrètes avec la complexité d'un simple DES: 2^{57} calculs (et stockage 2^{56})
au lieu de 2^{112}

LE DOUBLE DES: ATTAQUE

Pour un couple (M, C), i.e., message et chiffré:

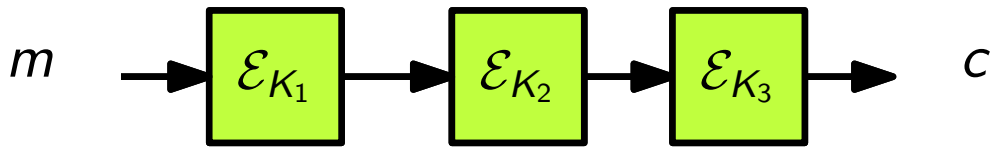
1. Calculer $U_i = DES_i(M)$ pour toutes les clés i
2. Pour chaque clé j:
   - Calculer $V_j = DES_j^{-1}(C)$
   - Chercher les valeurs i tels que $U_i = V_j$
   - Si $DES_j(DES_i(M')) = C'$ alors `Succès`

ANALYSE DE L'ATTAQUE

- 2^{56} chiffrés U_i
- 2^{56} déchiffrés V_j $\Longrightarrow$ 2^{112} paires
- Sur 64 bits, cela donne $2^{112-64} = 2^{48}$ collisions possibles

LE TRIPLE DES

Soient k_1, k_2 et k_3 trois clés

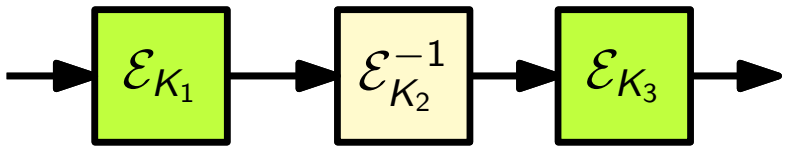


Certaines variantes ne sont pas sûres. . .

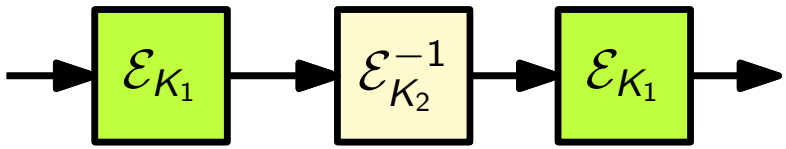
LE TRIPLE DES

Variante recommandée (NIST, FIPS 46-3):

- utilisé dans le milieu bancaire
- utiliser DES^{-1} avec k_2 (compatibilité)



- deux clés au lieu de 3 (avec $k_1 = k_3$)



INCONVÉNIENTS DU TRIPLE DES

Inconvénients

Le triple DES offre une sécurité convenable, mais...

- Le problème lié à la taille du bloc subsiste
- L'algorithme est trois fois plus lent que le DES !

I. CHIFFREMENT SYMÉTRIQUE

I.3. ADVANCED ENCRYPTION STANDARD

Organisation de la section « ADVANCED ENCRYPTION STANDARD »

Historique
Description

APPEL D'OFFRE AES 1997

DES toujours pas cassé... mais clés trop courtes !
La recherche exhaustive devient possible

Remplaçant pour DES : plus efficace que le triple DES, avec des clés de 128 ou 256 bits en « natif », avec des blocs plus longs

Advanced Encryption Standard: appel d'offre international
Requis: des blocs de 128 bits, des clés de 128, 192 ou 256 bits Une quinzaine de candidats (dont DFC, par l'ÉNS)

LES CANDIDATS AES 1997

- CAST-256 (Adams, Tavares, Heys et Wiener): Feistel 48 tours
- CRYPTON (Lim *et al.*): substitutions/permutations 12 tours
- DEAL (Outerbrideg et Knudsen): Feistel 6 tours dérivé de 3DES
- DFC (Gilbert, Girault, Hoogvorst, Noilhan, Pornin, Poupard, Stern, Vaudenay): Feistel 8 tours
- E2 (Aoki et Kanda): Substitutions/permutations. Lent
- FROG (Georgoudis, Leroux et Chaves): Polymorphique à 8 tours
- HPC (Schroeppel)
- LOKI97 (Brown, Pieprzyk et Seberry): Feistel 16 tours
- MAGENTA (Huber, Deutsche Telekom): Feistel 6 tours. Faible et lent.
- MARS (Coppersmith, Zunic *et al.*): Feistel hétérogène 16 + 16 tours
- RC6 (Kaliski, Rivest etal): Rotations similaires RC5, 20 tours
- Rijndael (Rijmen et Daemen): substitutions/permutations 10 à 14 tours
- SAFER+ (Massey, Williams): substitutions/permutations 12 tours
- Serpent (Anderson, Biham et Knudsen): substitutions/permutations 32 tours
- Twofish (Schneier, Kelsey, Whiting, Wagner, Hall et Ferguson): Feistel + Hadamard 16 tours

DÉSIGNATION DE L'AES EN 2000

5 « survivants » en 1999 :

1. MARS, par IBM
2. RC6, par RSA Security Inc.
3. Rijndael, par Daemen et Rijmen
4. Serpent, par Anderson, Biham et Knudsen
5. Twofish, par Schneier, Kelsey, Whiting, Wagner, Hall et Ferguson

Définition (Advanced Encryption Standard)

La version à blocs de 128 bits de Rijndael est désignée gagnante.
Taille de clés possibles : 128, 192 ou 256 bits

Rijndael peut aussi fonctionner avec des blocs de 192 ou 256 bits

CHIFFREMENT AES

Les blocs de messages (128 bits) sont découpés en 16 octets, placés dans une matrice 4×4

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

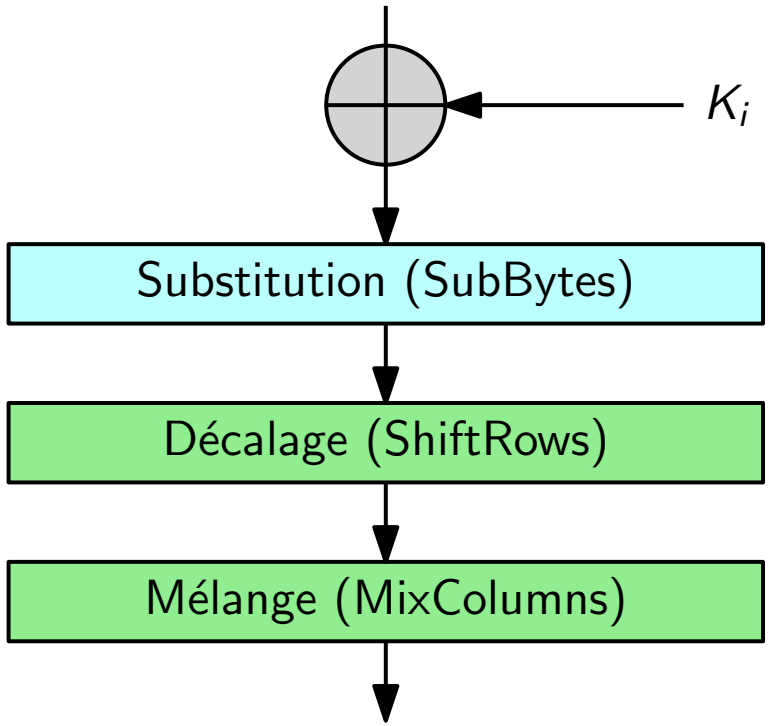
$a_{0,0}$	$a_{0,1}$	$a_{0,2}$	$a_{0,3}$
$a_{1,0}$	$a_{1,1}$	$a_{1,2}$	$a_{1,3}$
$a_{2,0}$	$a_{2,1}$	$a_{2,2}$	$a_{2,3}$
$a_{3,0}$	$a_{3,1}$	$a_{3,2}$	$a_{3,3}$

CHIFFREMENT AES

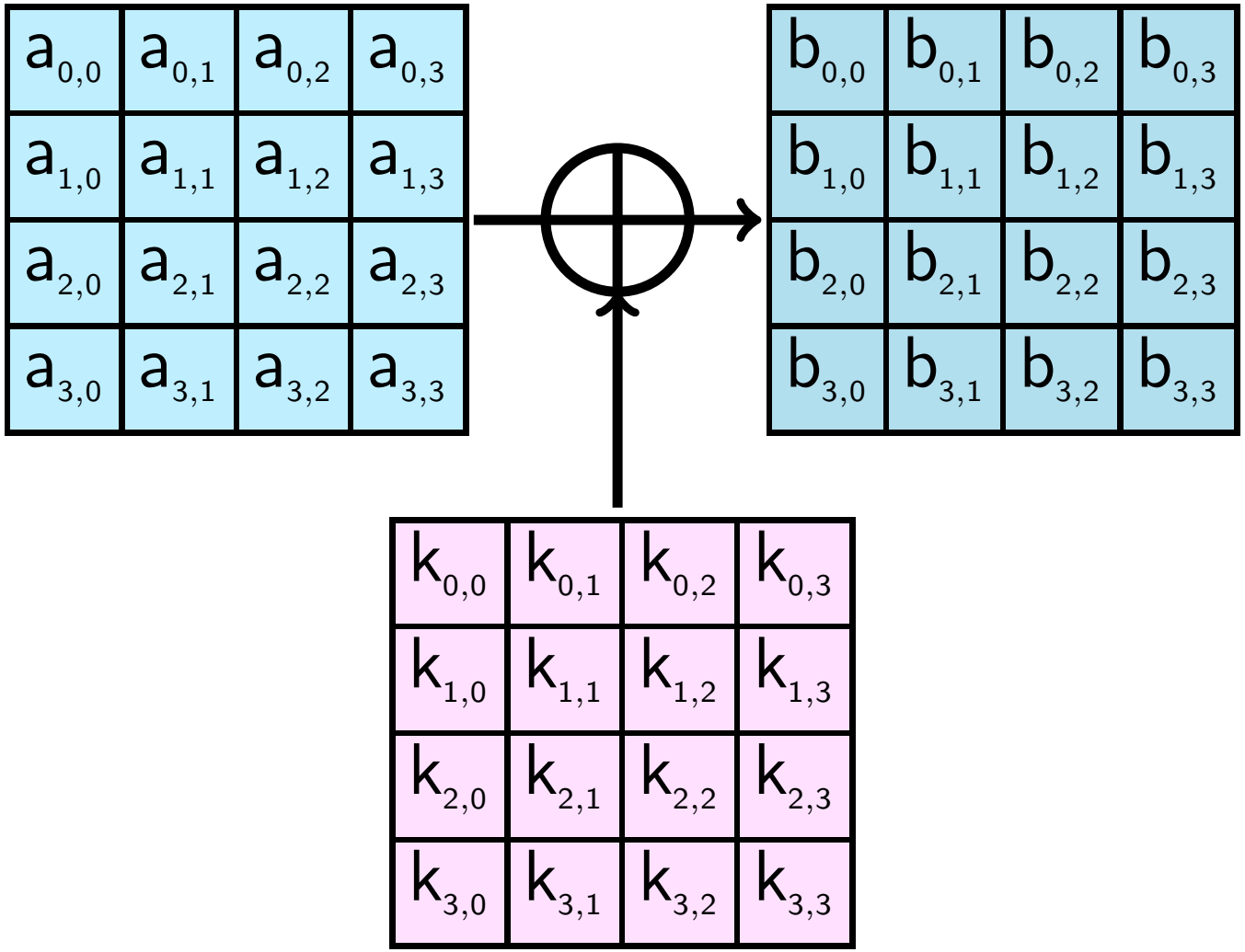
Cette matrice subit ensuite 4 transformations par tour

1. *AddRoundKey*: XOR avec la sous-clé
2. *SubBytes*: passage dans une S-box
3. *ShiftRows*: décalage des ligne (rotation)
4. *MixColumns*: mélange des colonnes (sauf dernier tour)

. . .ceci 10 à 14 fois (tours)

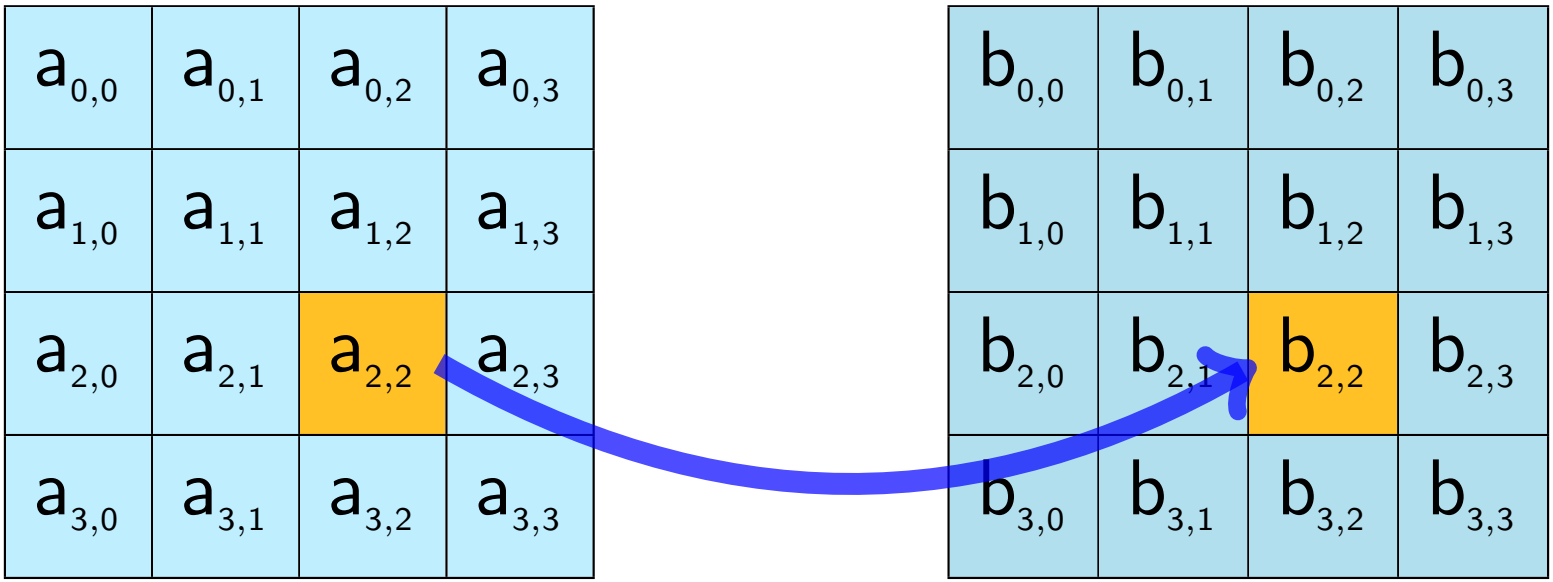


ÉTAPE ADDROUNDKEY



ÉTAPE SUBBYTES

Étape non-linéaire (*confusion*)



ÉTAPE SUBBYTES

La substitution S est une fonction fixe de 8 bits vers 8 bits, c'est-à-dire de $[0, 255]$ vers $[0, 255]$
Basée sur une relation algébrique:

$$S(X) = L \cdot \frac{1}{X} + C$$

- L'inverse est pris dans $GF(2^8)$
- L et C évitent les points fixes ou particuliers
- Opération hautement non-linéaire

LA SUBSTITUTION AES

S(95)=42=0x2a

	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15
00	99	124	119	123	242	107	111	197	48	1	103	43	254	215	171	118
01	202	130	201	125	250	89	71	240	173	212	162	175	156	164	114	192
02	183	253	147	38	54	63	247	204	52	165	229	241	113	216	49	21
03	4	199	35	195	24	150	5	154	7	18	128	226	235	39	178	117
04	9	131	44	26	27	110	90	160	82	59	214	179	41	227	47	132
05	83	209	0	237	32	252	177	91	106	203	190	57	74	76	88	207
06	208	239	170	251	67	77	51	133	69	249	2	127	80	60	159	168
07	81	163	64	143	146	157	56	245	188	182	218	33	16	255	243	210
08	205	12	19	236	95	151	68	23	196	167	126	61	100	93	25	115
09	96	129	79	220	34	42	144	136	70	238	184	20	222	94	11	219
10	224	50	58	10	73	6	36	92	194	211	172	98	145	149	228	121
11	231	200	55	109	141	213	78	169	108	86	244	234	101	122	174	8
12	186	120	37	46	28	166	180	198	232	221	116	31	75	189	139	138
13	112	62	181	102	72	3	246	14	97	53	87	185	134	193	29	158
14	225	248	152	17	105	217	142	148	155	30	135	233	206	85	40	223
15	140	161	137	13	191	230	66	104	65	153	45	15	176	84	187	22

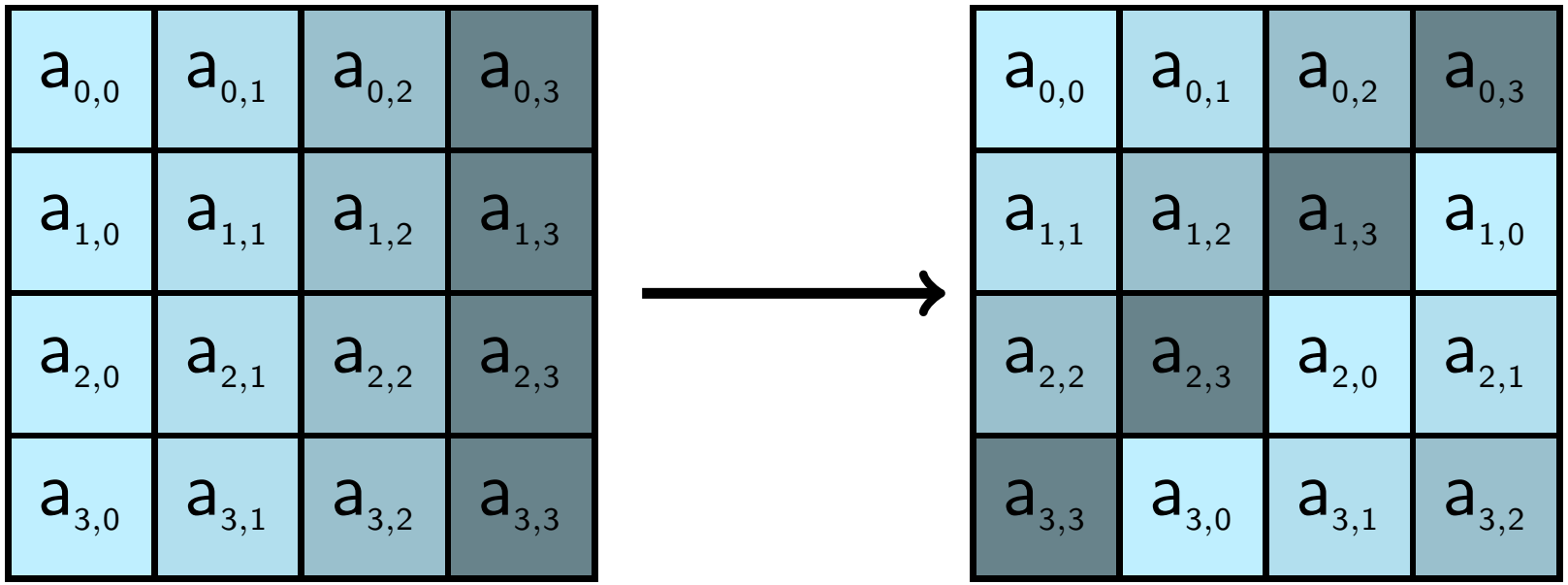
LA SUBSTITUTION AES

S(95)=42=0x2a

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

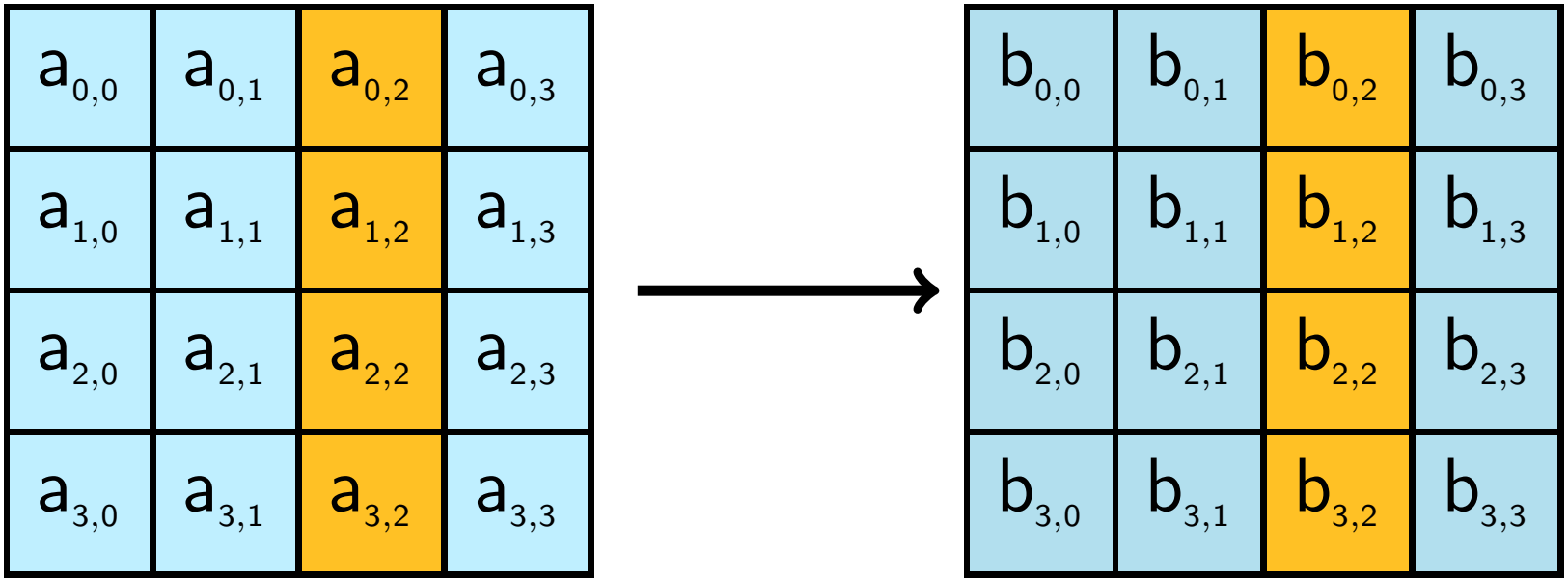
ÉTAPE SHIFTROWS

Transformation linéaire (*diffusion*)



ÉTAPE MIXCOLUMNS

Transformation linéaire (*diffusion*)



Remplacée dans le dernier tour par *AddRoundKey*

ÉTAPE MIXCOLUMNS

For MixColumns, we have:

$$\begin{bmatrix} r_0 \\ r_1 \\ r_2 \\ r_3 \end{bmatrix} = \begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix}$$

For InvMixColumns, we have:

$$\begin{bmatrix} r_0 \\ r_1 \\ r_2 \\ r_3 \end{bmatrix} = \begin{bmatrix} 14 & 11 & 13 & 9 \\ 9 & 14 & 11 & 13 \\ 13 & 9 & 14 & 11 \\ 11 & 13 & 9 & 14 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix}$$

ÉTAPE MIXCOLUMNS

La fonction est linéaire, elle contribue, avec le *ShiftRows*, à la **diffusion**

Elle peut être interprétée de deux façons:

- multiplication de la colonne (vue comme un polynôme sur $GF(2^8)$) par le polynôme $3X^3 + X^2 + X + 2$ modulo $X^4 + 1$. L'inverse de ce polynôme est $11X^3 + 13X^2 + 9X + 14$
- multiplication par une matrice dans $GF(2^8)$

NOMBRE DE TOURS

Le nombre de tours varie suivant la taille des blocs et la taille des clés

	$\|k\| = 128$	$\|k\| = 192$	$\|k\| = 256$
blocs 128	10	12	14
blocs 192	12	12	14
blocs 256	14	14	14

PERFORMANCES

La comparaison la plus pertinente est celle entre AES128 et TDES:

- le triple DES est 3 fois plus lent que DES
- l'AES est 2,7 fois plus rapide que TDES

On a donc un gain de sécurité sans perte de performances (quasi)

SÉCURITÉ DE L'AES

- L'AES a été conçu pour résister au mieux à la cryptanalyse linéaire et différentielle
- Les attaques *algébriques* ont laissé entrevoir un moment un espoir d'attaquer efficacement l'AES
  - ...mais pas réalistes
  - linéariser et résoudre un système d'équations énormes
- On ne connaît pas de clés faibles pour AES (2005)
- La meilleure attaque reste à l'heure actuelle la recherche exhaustive de la clé

RECHERCHE EXHAUSTIVE DE CLÉ

Il est impossible d'effectuer une recherche exhaustive sur 128 bits

Comparaison DES/AES: en imaginant une machine cassant un chiffrement DES par seconde, il faudrait 149 mille milliards d'années pour retrouver une clé de 128 bits

Pour casser un tel chiffrement, il faut trouver une autre méthode
Il est probable qu'une telle méthode existe et soit moins coûteuse

AES AVEC MOINS DE TOURS

Il existe des attaque sur

- 7 tours avec clés de 128 bits
- 8 tours avec clés de 192 bits
- 9 tours avec clés de 256 bits

AES COMME STANDARD

La NSA a annoncé que l'AES était apte à protéger des informations classifiées jusqu'au niveau SECRET, et même TOP SECRET si on utilise des clés de 256 bits