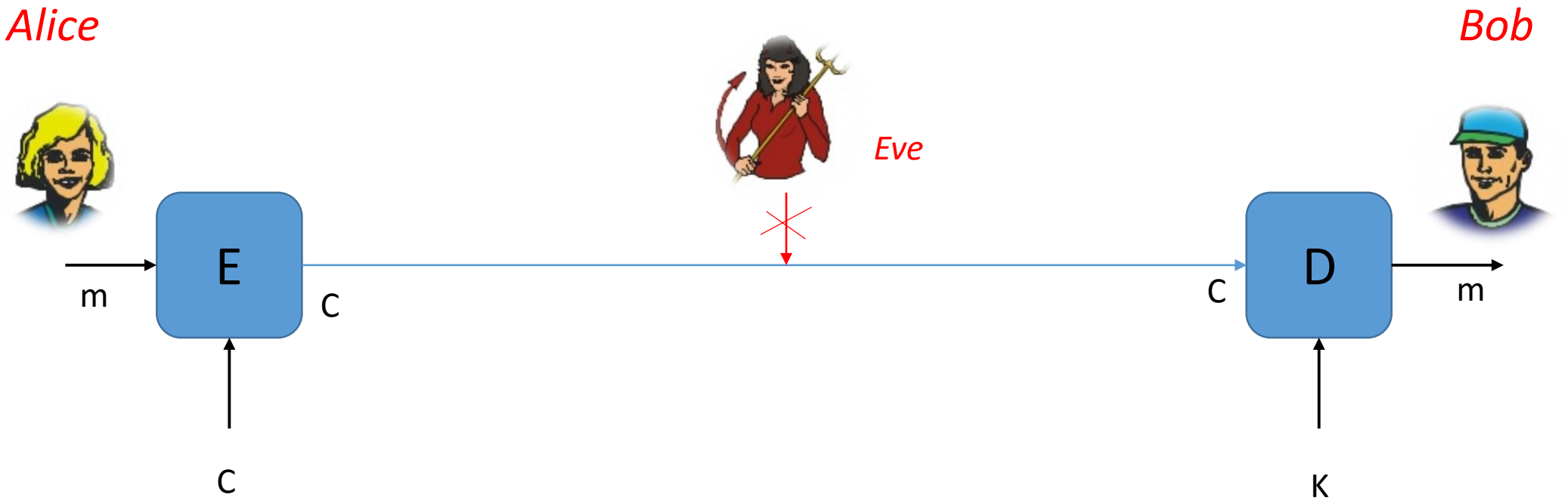
Introduction à la cryptographie (cours 4): Chiffrement par bloc (AES)

Université Paris 13 Villetaneuse

01/02/2016

Houda FERRADI

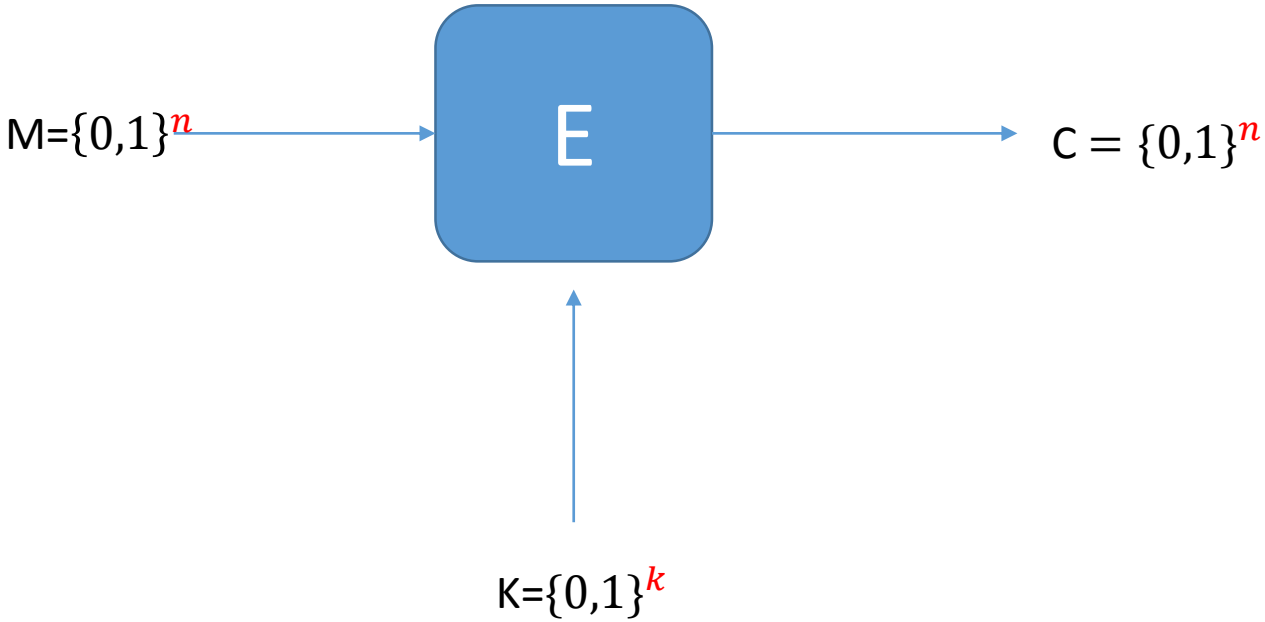
Rappel : chiffrement symétrique ou à clé secrète



E (Fonction de chiffrement) et D (Fonction de déchiffrement): Fonctions inversibles et efficaces
K: Clé secrète ou symétrique
C: Le message chiffré
m, k, et c sont de taille déterminée!

Rappel : chiffrement symétrique

Définition : Un algorithme de chiffrement symétrique transforme *un message en clair M* avec *une clé secrète K*. Le résultat est *un chiffré C*



Deux grandes catégories

Chiffrement par blocs

- M est traité par blocs de données (ex: 64 bits ou 128 bits)

Exemple d'algorithmes : DES, AES, IDEA, RC6, BLOWFISH, …

Chiffrement par flots

- M est traité bit par bit (cours précédent)

Exemple d'algorithmes: RC4, Bluetooth E0/1, GSM A5/1,

Introduction: Chiffrement par blocs

- Dans un système de chiffrement par blocs, chaque texte clair est découpé en blocs de même longueur et chiffré bloc par bloc.
- La taille de bloc (n = 64 ou 128 bits) Les modes opératoires permettent généralement des attaques quand plus de $2^{n/2}$ blocs sont chiffrés avec une même clé.
- La clé soit être suffisamment grande (k>128): Pour un bon algorithme, la meilleure attaque doit coûter 2^{k} opérations (la technique utilisée est l'attaque exhaustive).

Exemple:

- AES: n= 128 bits , k=128, 192, 256 bits
- 3 DES: n= 64, k= 168 bits ou 112 bits si $k_1 = k_2$

2 principes fondamentaux pour AES

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

- Confusion == Masquer toute relation linéaire entre le *chiffré* et le *message en clair*.

- Diffusion == Cacher la redondance en répartissant l'influence d'un bit de clé sur tout le chiffré.

Fonction aléatoire toujours notre objectif

- Un bon algorithme à clé secrète doit transformer le message clair en un chiffré qui ressemble autant que possible à une suite aléatoire, pour limiter au minimum les risques d'une attaque par analyse statistique du chiffré, de ses redondances.

- Exemple dans le chiffrement de flux : Le « masque jetable », clé tirée uniformément d'un espace de clés K.

Construction: Fonction aléatoire

Nouvelle définition dans le chiffrement par blocs Fonction aléatoire ⟺ Permutation aléatoire

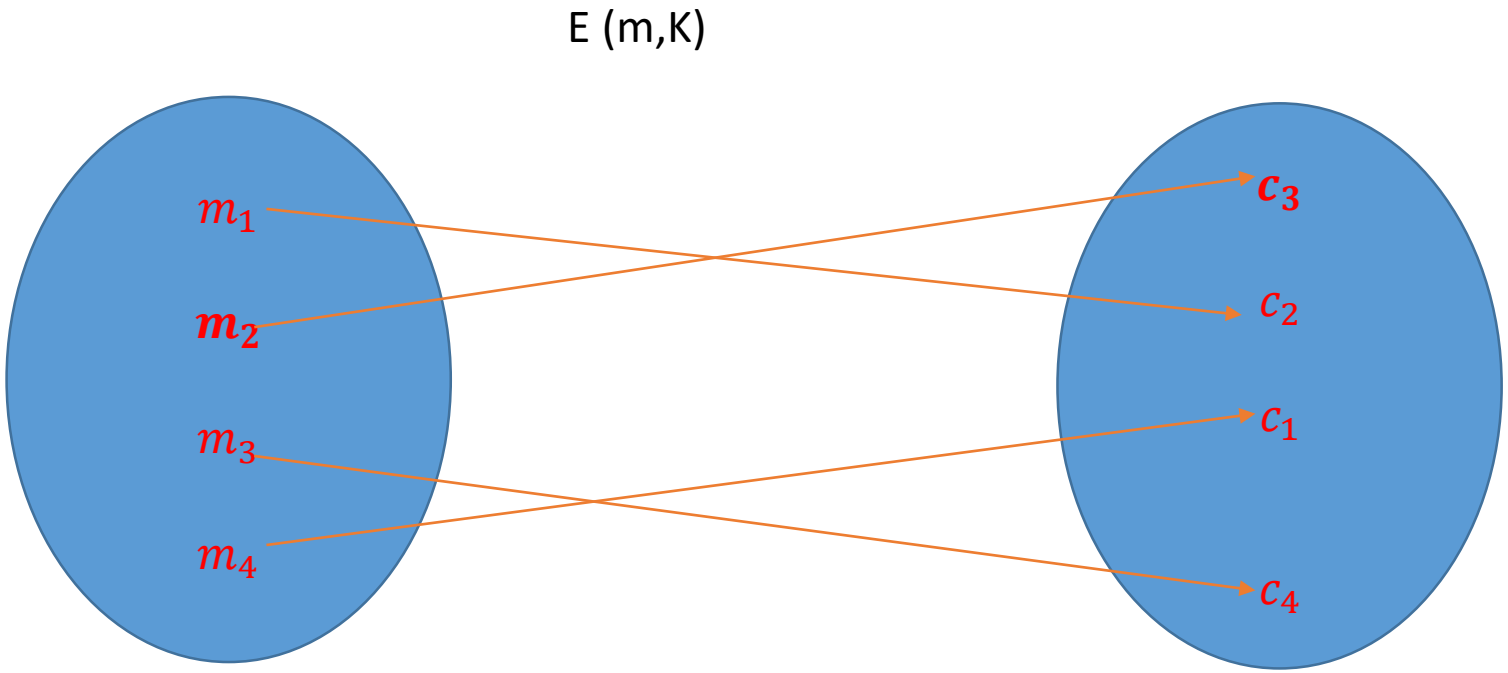
Telle que une fonction de chiffrement E(k,m) on a:

- Il existe une façon *efficace* d'évaluer E(k,m)
- Il existe un algorithme d'*inversion* efficace D(k,c)

=> E(k,m) doit être une fonction *bijective*

Exemple d'une fonction bijective

- E (m, k) est une fonction de chiffrement bijective



AES (Advanced Encryption Standard)

Appel d'offre en 1997

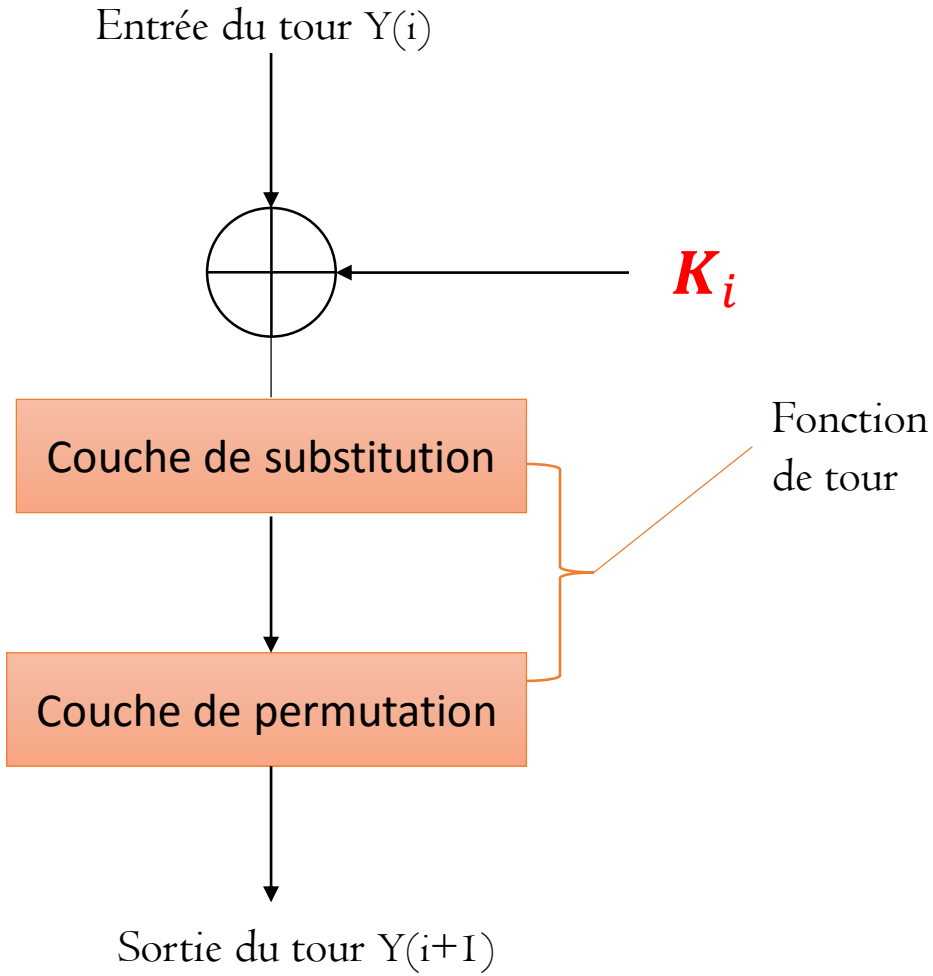
- Avant 1997: DES (schéma de Feistel), vulnérable à l'attaque exhaustive!
- 1997: NIST publie une demande de propositions.
- 1998: Quinze propositions des universités comme: RC6, IDEA
- 1999: NIST choisit 5 finalistes dont: RC6 (schéma de Feistel généralisé) et IDEA (schéma de Lai-Massey)
- 2000: NIST choisit Rijndael pour AES (conçu par Vincent Rijmen et Joan Daemen).

Désignation d'AES en 2000

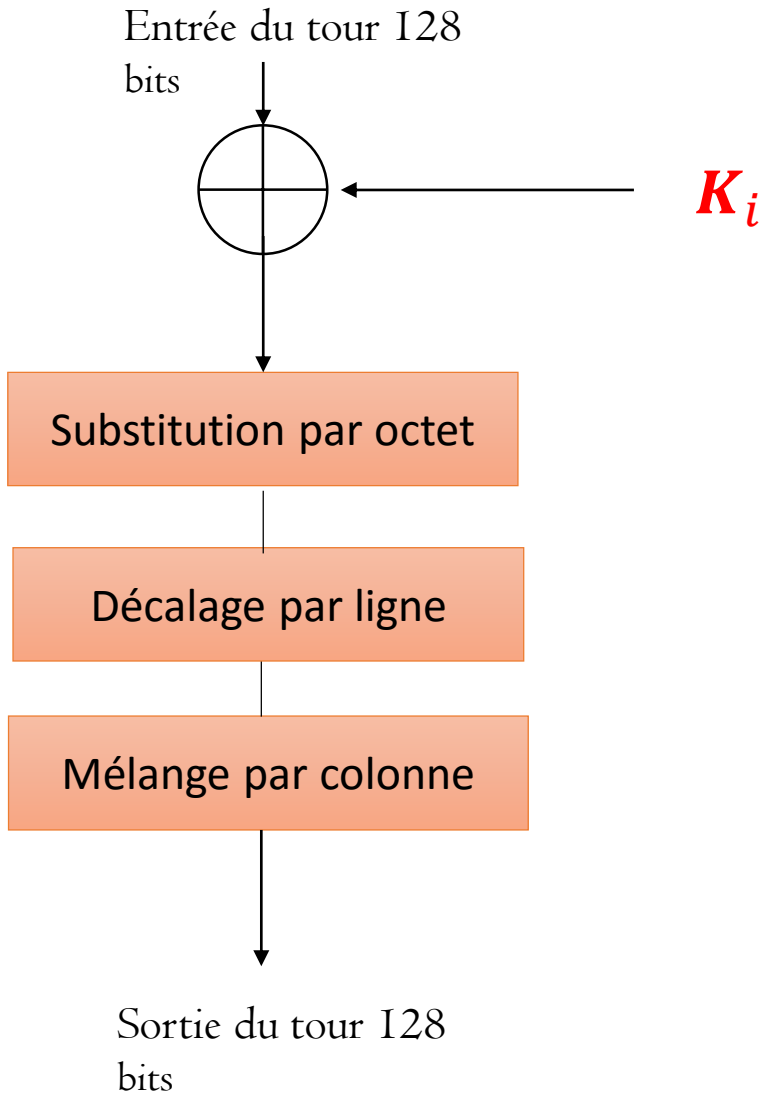
- AES est un algorithme de chiffrement itératif, mais contrairement à 9 autres candidats, ce n'est pas un chiffrement de Feistel (définit dans le cours précédent)
- Taille de bloc est de 128 bits
- Chiffrement à 128, 128 ou 256 bits de clés
- Basé sur la théorie de Galois

Différentes couches d'AES

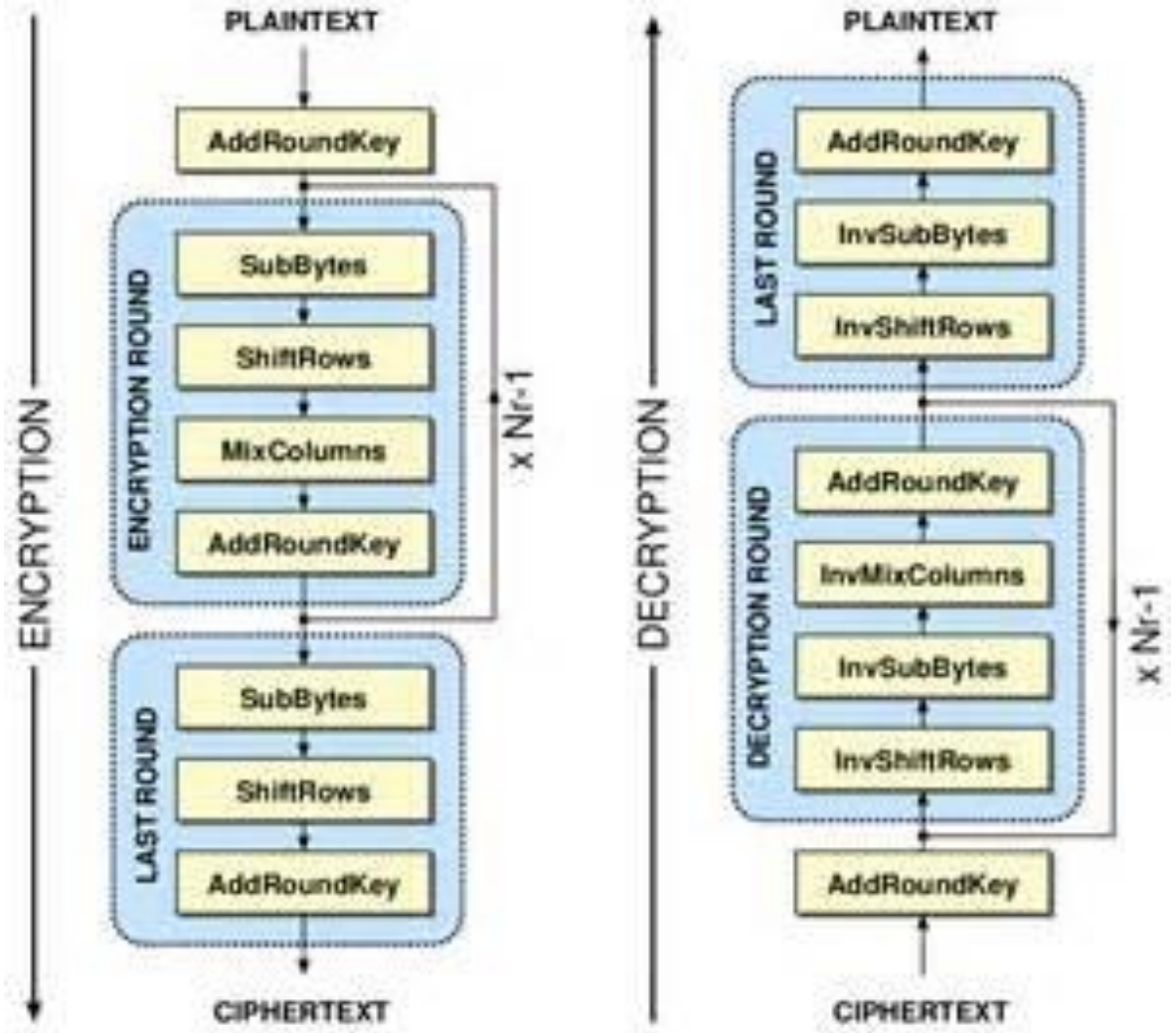
- A chaque tour, le chiffré Y(i) produit par le tour précédent subit une substitution non-linéaire qui assure la confusion puis une permutation linéaire qui assure la diffusion, puis la clé du tour est ajoutée bit à bit pour donner Y(i+1). Le nombre de tours est 10 pour une clé de 128 bits et de 14 pour une clé de 256 bits.



Plus de précisions

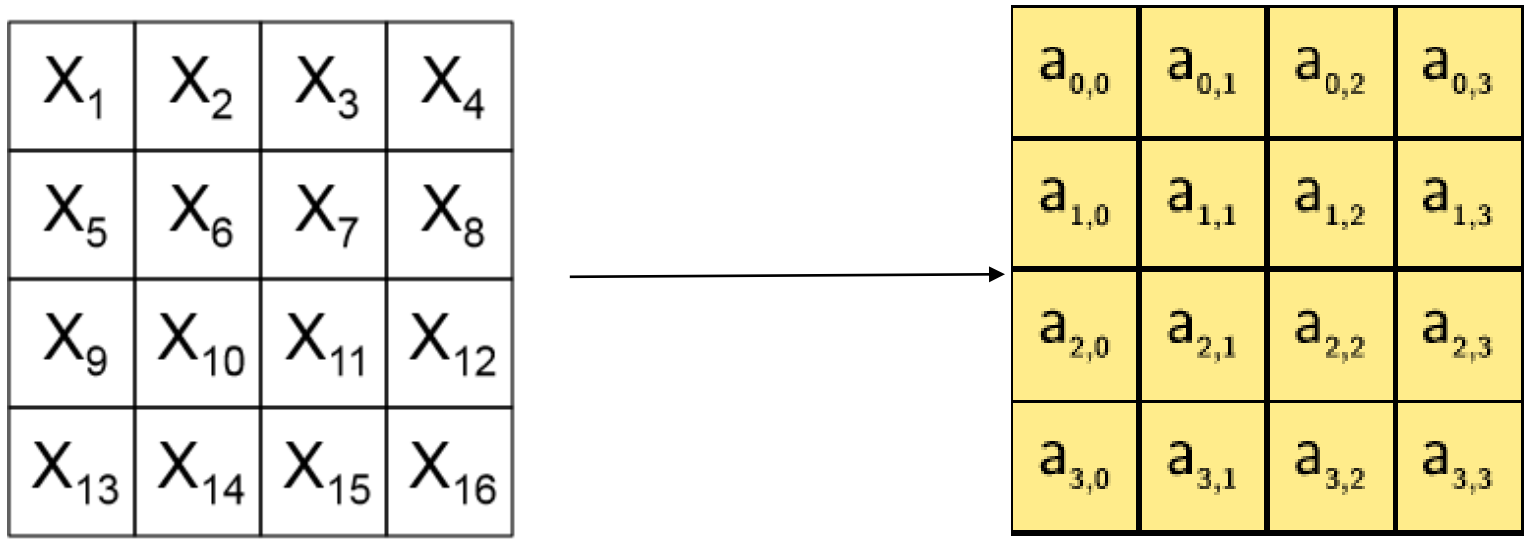


Structure générale



Ière étape

Ière étape: le stockage des données dans un « carré » de 4 x 4 = 16 cases ensuite dans une matrice 4 x 4 appelée $A_{i,j}$



Chaque case contient 1 octet (8 x 16 = 128 bits d'état interne)

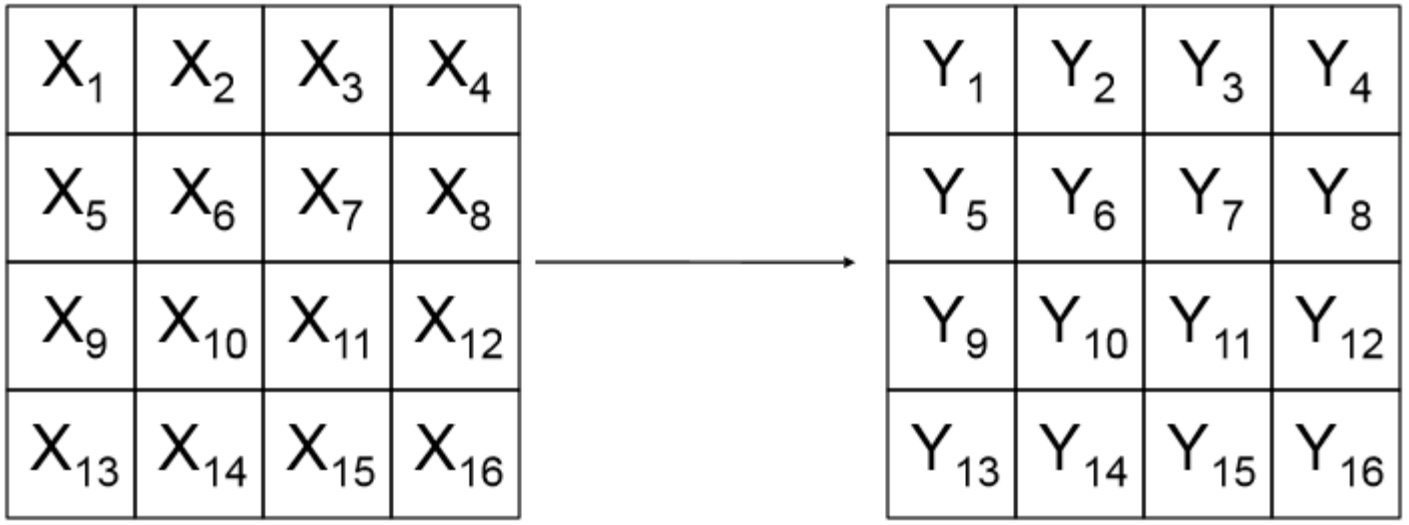
2e étape: AddRoundKey

2e étape: XOR la matrice avec la sous-clé

$$A_{i,j} \oplus K_{i,j} = B_{i,j}$$

3e étape: SubBytes

3e étape: Ca consiste à un passage de la matrice $B_{i,j}$ dans une S-Box: transformation non-lineaire (confusion).



Pour : 1 ≤ i ≤ 16, Yi = S(Xi)

3e étape: SubBytes

- S-Box est une fonction fixe et bijective de 8 bits vers 8 bits
- Définie comme un tableau à $2^8 = 256$ entrées
- Nécessite donc 256 octets de mémoire
- Basée sur une opération algébrique qui s'écrit sous forme:

S(X) = Affine(Inverse(X)) ou $S(X) = L \cdot \frac{1}{X} + c$

- L et C évitent les points fixes et particuliers

où l'inverse est pris dans GF(2^8)

S-Box pour AES

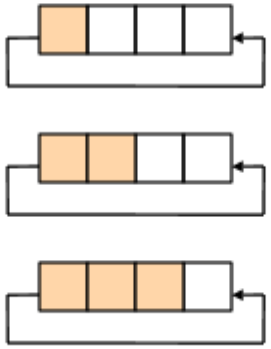
S(95)=42=0x2a

	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

4e étape: ShiftRows

4e étape: Consiste à décaler les lignes en rotation: transformation linéaire (diffusion).

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}

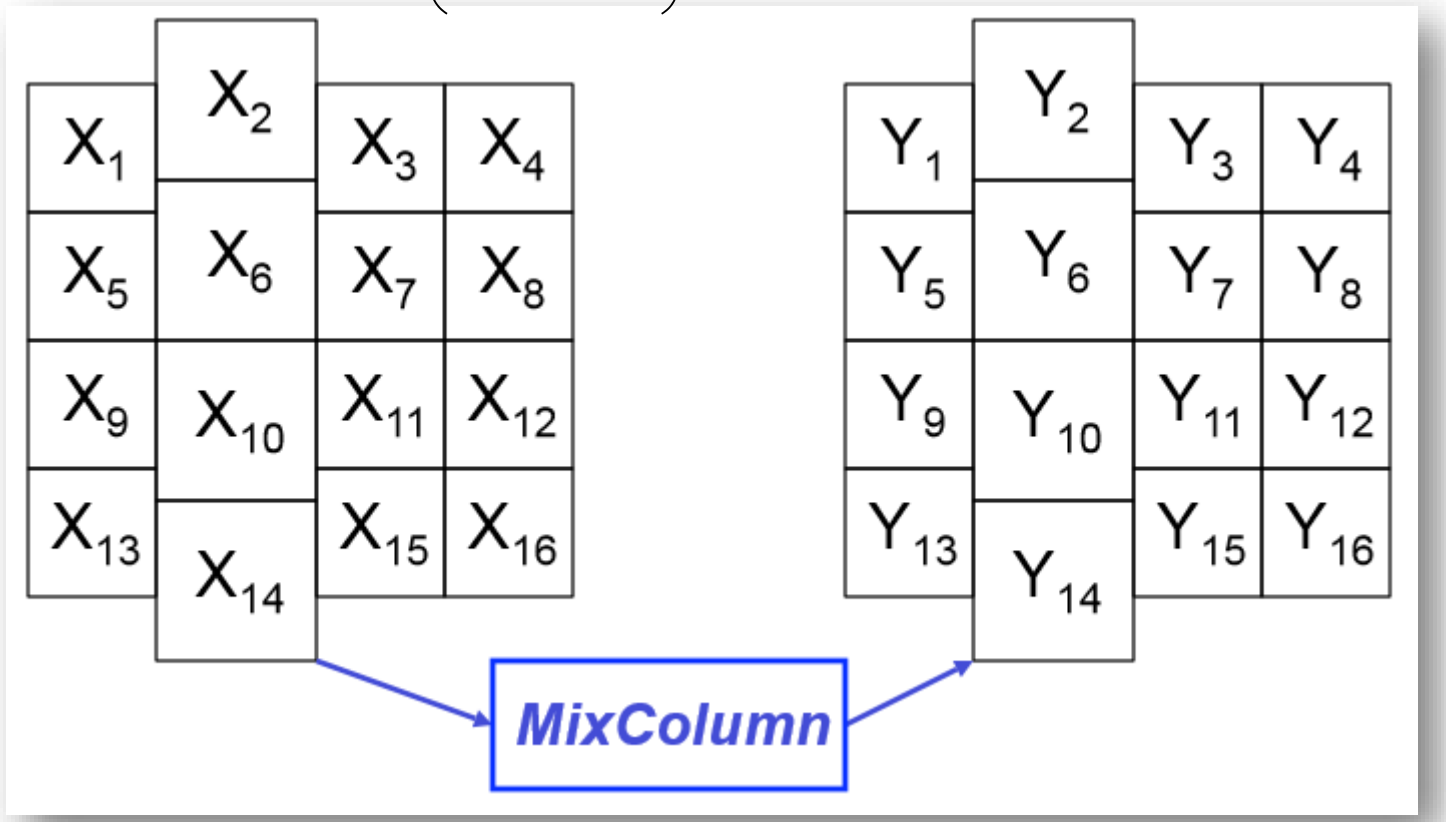


X_1	X_2	X_3	X_4
X_6	X_7	X_8	X_5
X_{11}	X_{12}	X_9	X_{10}
X_{16}	X_{13}	X_{14}	X_{15}

Décalage circulaire (vers la gauche) de i cases pour la ligne numéro i, $0 \leq i \leq 3$

5e étape: MixColumns

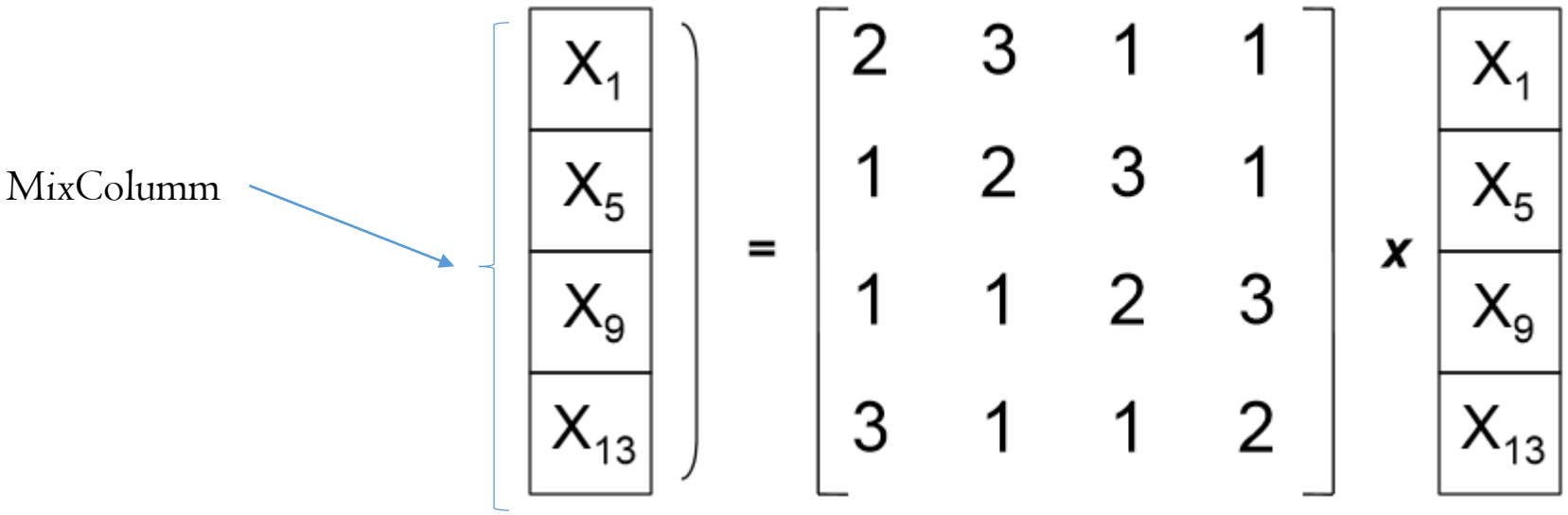
5e étape: Mélanger les colonnes , sauf le dernier tour d'AES (10e ou 14e):
Permet la transformation linéaire (diffusion)



MixColumn() est appliquée à chaque colonne

5e étape: MixColumns

Pour chaque colonne on applique une multiplication par une matrice circulante:



Opérations linéaires dans GF(2^8)

Rappel de Notions d'algèbre

Groupes

Définition : un ensemble G muni d'une loi interne, notée * par exemple, est appelé un **groupe** ssi cette loi vérifie les trois axiomes suivants, pour tout x, y, z dans G:

- $x*(y*z) = (x*y)*z$
- Il existe e tel que $x*e = e*x = x$ (e est un élément neutre)
- Pour tout x de G, il existe x' de G, tel que $x*x'=x'*x=e$ (existence d'un élément symétrique x').

Un tel groupe est noté (G,*) ou G.

Un groupe G est dit fini si card(G) est fini. Le nombre d'éléments d'un groupe est appelé **ordre du groupe.**

Définition : un sous-ensemble H d'un groupe G est un **sous-groupe** s'il est lui-même un groupe pour les opérations de G. Si H est un sous-groupe strictement inclus dans G, alors H est dit être un sous-groupe propre.

Théorème de Lagrange : Si G est un groupe fini et H est un sous-groupe de G, alors card(H) divise card(G).
Par conséquent, si **a** appartient à G, alors **ord (a)** divise **card(G)**.

Anneaux

Définition : un anneau (R,+,x) est un ensemble R munis de deux opérations binaires notées + et * telles que :

- (R,+) est un groupe abélien (dont l'identité est notée 0)
- La loi * est associative sur R
- Il existe un élément de R, noté I, tel que pour tout a dans R, a*I=I*a=a
- La loi * est distributive par rapport à la loi + i.e. a*(b+c) = (a*b)+(a*c) et (b+c)*a = (b*a)+(c*a).

L'anneau est commutatif si la loi est * est commutative sur R.

Corps

Définition : un **corps** est un anneau dans lequel tous les éléments non-nuls ont un inverse pour la multiplication.

Anneaux des polynômes

Définition : si R est un anneau commutatif, alors un **polynôme** en x sur R est une expression de la forme:

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x^1 + a_0$$

Définition : si R est un anneau commutatif, **l'anneau des polynômes** R[x] est l'anneau formé par l'ensemble des polynômes en x à coefficients dans R.

Définition : soit K un corps et soit f(x) un polynôme dans K[x] de degré au moins 1. f(x) est **irréductible** dans K[x] s'il ne peut pas se décomposer en le produit de deux polynômes de K[x] dont les degrés sont supérieurs ou égaux à 1.

Définition : $K[x]/f(x)$ désigne l'ensemble des polynômes de K[x] dont le degré est inférieur ou égal à n=deg(f(x)). Les opérations d'addition et de multiplication sont effectuées modulo f(x).

Note : $K[x]/f(x)$ est un anneau commutatif. Si f(x) est irréductible sur K, alors $K[x]/f(x)$ est un corps.

Espaces vectoriels

Un espace vectoriel E sur un corps K est un groupe abélien (E,+) munis d'une loi multiplicative noté . telle que a,b dans K et tout couple (u,v) dans E×E, on a:

1. $a.(v+w) = a.v + a.w$
2. $(a+b).v = a.v + b.v$
3. $(ab).v = a.(b.v)$
4. $1.v = v$

Les éléments de E sont appelés **vecteurs** et les éléments de K sont appelés **scalaires.**

Définition : une **combinaison linéaire** d'éléments d'un sous-ensemble $S = \{v1, v2, \ldots, vn\}$ de vecteurs d'un espace vectoriel sur un corps K est une expression de la forme

$$a_1 v_1 + a_2 v_2 + \cdots + a_n v_n, \;\; a_i \in K$$

L'**espace noté <S> engendré par S** est l'ensemble de toutes les combinaisons linéaires des éléments de S.

Les éléments de S sont dits être **linéairement dépendants** s'il existe un ensemble de scalaires $a_1, a_2, \cdots, a_n$ tels que $a_1 v_1 + a_2 v_2 + \cdots + a_n v_n = 0$

.

Dans le cas contraire les éléments de S sont être **linéairement indépendants**.

Une famille de vecteurs linéairement indépendants engendrant un espace V est dit être une **base** de V.

La **dimension** d'un espace vectoriel E, noté **dim E**, est le nombre de vecteurs que contient une base de E.

Corps finis

Existence et unicité : si K est un corps fini, alors K contient p^n éléments où p est un nombre premier et n est un entier strictement positif. Pour tout nombre premier p et tout entier n, il existe un unique corps fini (à isomorphisme près) de cardinal p^n Ce corps est noté $\mathbb{F}_{p^n}$

GF(2^8): construction

- Cet objet mathématique est utilisé pour définir la boîte S dans ShiftColumns et la matrice qu'on utilise pour multiplier chaque colonne dans l'étape MixColumn():
- Un corps est un anneau dans lequel tous les éléments non-nuls ont un inverse pour la multiplication.
- Soit un polynôme irréductible P(x)=$3X^3 + X^2 + X + 2$. Un polynôme est irréductible dans K[x] s'il ne peut pas se décomposer en le produit de deux polynômes de K[x] dont les degrés sont supérieurs ou égaux à 1

Exemple:

- Tous les polynômes de degré 1 sont irréductibles. Par conséquent il y a une infinité de polynômes irréductibles.
  - $X^2-1 = (X-1)(X+1) \in R[X]$ est réductible.
  - $X^2+1=(X-i)(X+i)$ est réductible dans C[X] mais est irréductible dans R[X].
  - $X^2-2=(X-\sqrt{2})(X+\sqrt{2})$ est réductible dans R[X] mais est irréductible dans Q[X].

GF(2^8): construction

- L'inverse de ce polynôme est $11X^3 + 13X^2 + 9X + 14$
- L'ensemble de ces polynômes sont dans GF(2^8) = F_2[X] / P

GF(2^8) est un corps fini avec 256 éléments, aussi appelé *corps de Galois* dont les coefficients sont dans F_2 et de degré inferieur à 8.

GF(2^8) : représentation

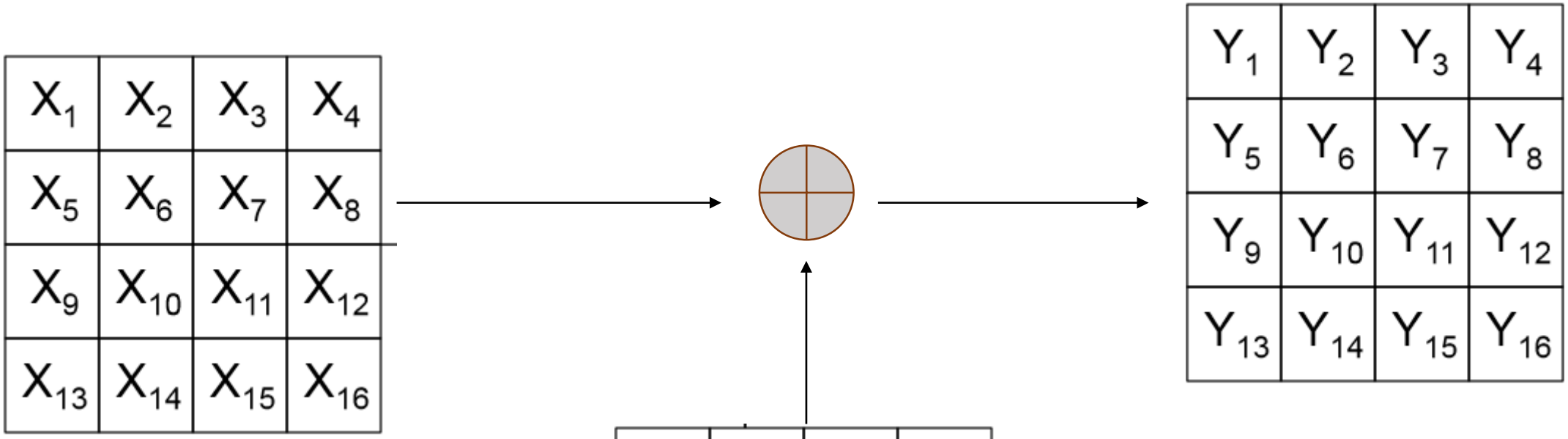
- Chaque élément de GF(2^8) est représenté comme: $b_7X^7 + b_6X^6 + \ldots + b_1X^1 + b_0$, tel que pour le stockage des octets on les stocke en binaire sur $(b_7,\ldots, b_0)$

- Dans l'étape MixColumns on effectue une multiplication du polynôme P(x)=$3X^3 + X^2 + X + 2$ fixé suivi d'une réduction mod $X^4 + 1$

- Multiplication de chaque vecteurs de colonne par le polynôme $3X^3 + X^2 + X + 2$

- Pour obtenir l'inverse on multiplie par $11X^3 + 13X^2 + 9X + 14$

Dernière étape : AddRoundKey



$$Y_i = X_i \oplus K_i$$

Synthèse

- AES est 2,7 fois plus rapide que 3 DES (gain de performance)

Le nombre de tours dépends de la taille de blocs et de la clé

	K= 128	K= 192	K=256
Bloc=128	**10**	12	14
Bloc=192	12	12	14
Bloc=256	14	14	14

- La *recherche exhaustive* reste la meilleure attaque contre AES (impossible avec 128 bits)
- NSA a annoncé que AES est le meilleur standard pour protéger des informations les plus sensibles avec des clés de 256 bits (14 tours)
- AES a été conçu pour résister à la cryptanalyse *linéaire* et *différentielle* (cours suivant)

En pratique

Algorithmes utilisés

- DES dans les anciens produits
- AES dans les nouveaux produits

Autres algorithmes utilisés ponctuellement

- IDEA (PGP)
- BlowFish

En pratique

Algorithmes utilisés

- DES dans les anciens produits
- AES dans les nouveaux produits

Autres algorithmes utilisés ponctuellement

- IDEA (PGP)
- BlowFish