MT10

Mathématiques pour la cryptographie

Deuxième Partie

Anneaux de Polynômes et corps finis

Walter SCHÖN

Cryptographie, anneaux de polynômes et corps finis

- Le standard actuel de cryptographie à clé secrète (Advanced Encryption System AES) repose sur l'arithmétique dans les anneaux de polynômes et dans les corps finis.
- Rappel : les polynômes à coefficients dans un corps commutatif (C, R, Q, Z/pZ pour p premier qui dans ce cas est un corps, …) forment un anneau Euclidien (la division Euclidienne est possible avec le degré comme valuation Euclidienne : le degré du polynôme reste est strictement inférieur au degré du polynôme diviseur). Il est donc en particulier :
  - ✓ Commutatif (la multiplication est commutative)
  - ✓ Unitaire (élément neutre de la multiplication : polynôme 1)
  - ✓ Intègre (sans diviseur de zéro : P1*P2=0 => P1=0 ou P2=0)
  - ✓ Principal (tous ses idéaux sont principaux i.e. engendrés par un unique élément)
  - ✓ Factoriel (ses éléments peuvent s'écrire de manière unique à une permutation près comme un produit d'éléments irréductibles et d'un élément inversible).

Cryptographie, anneaux de polynômes et corps finis

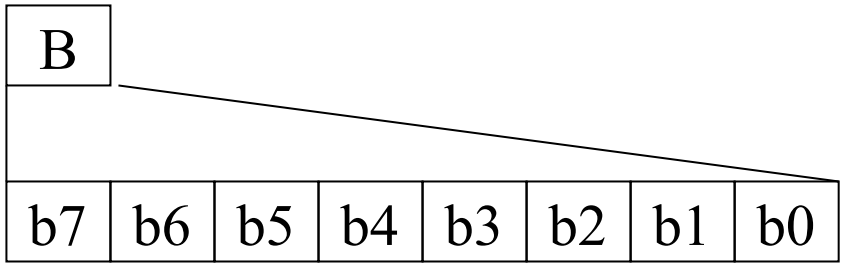
- Dans ces conditions la plupart des notions étudiées dans Z (autre anneau commutatif unitaire intègre et Euclidien)
  - ✓ Il existe des polynômes dits « irréductibles » qui ne sont divisibles que par les constantes et les produits d'eux mêmes par une constante (Equivalents des nombres premiers)
  - ✓ Tout polynôme peut être décomposé en un produit de polynômes irréductibles unitaires (coefficient du terme dominant = 1) et d'une constante, cette décomposition est unique à l'ordre près (équivalent du théorème fondamental de l'arithmétique)
- Parmi ces anneaux de polynômes est utilisé en particulier (pour des raisons évidentes d'implantation en machine) celui pour lequel le corps sous-jacent est Z/2Z : l'anneau Z/2Z [X]
- Les éléments de Z/2Z[X] sont les polynômes à une indéterminée X dont les coefficients sont entiers modulo 2 (de valeur 0 ou 1 ce qui est commode s'agissant de problématiques informatiques)
- X^3+X+1 par exemple est un élément de Z/2Z[X]

Cryptographie, anneaux de polynômes et corps finis

- Z/2Z[X] est un monde merveilleux car le corps sous-jacent est de caractéristique 2 : 1+1 = 0 dans Z/2Z (autrement dit on peut voir l'addition comme un XOR)
- Par conséquent pour tout élément de P de Z/2Z[X]
  - ✓ P+P=0
  - ✓ Donc P=-P
  - ✓ Q+P = Q-P quels que soient les polynômes P et Q
- Un monde merveilleux donc où l'addition et la soustraction sont une seule et même opération, et où donc la faute de signe n'existe pas !

Cryptographie, anneaux de polynômes et corps finis

- Pour l'utilisation cryptographique, les algorithmes assimilent un octet au polynôme de degré maximal 7 dont les coefficients sont les chiffres de la représentation binaire de cet octet :



$$B \Leftrightarrow \sum_{i=0}^{7} bi.x^i$$

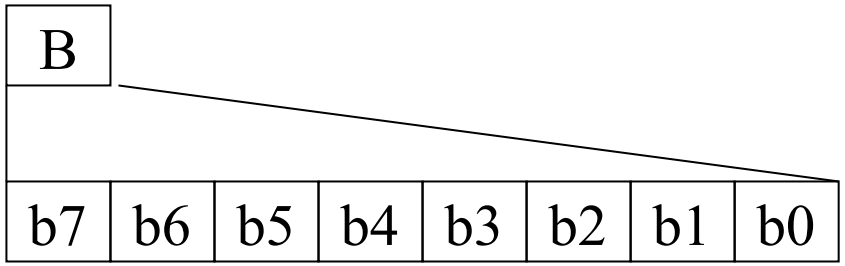
Exemple : {9D} <=> 10011101 <=> $x^7+x^4+x^3+x^2+1$

L'addition de deux octets est alors l'addition modulo 2 des coefficients (équivalent au XOR bit à bit) :

$$\{57\} \oplus \{83\} = ?$$

Cryptographie, anneaux de polynômes et corps finis

- Pour l'utilisation cryptographique, les algorithmes assimilent un octet au polynôme de degré maximal 7 dont les coefficients sont les chiffres de la représentation binaire de cet octet :



$$B \Leftrightarrow \sum_{i=0}^{7} bi.x^i$$

Exemple : {9D} <=> 10011101 <=> $x^7+x^4+x^3+x^2+1$

L'addition de deux octets est alors l'addition modulo 2 des coefficients (équivalent au XOR bit à bit) :

$$\{57\} \oplus \{83\} = 01010111 \oplus 10000011 = 11010100 = \{D4\}$$

Le problème est maintenant de définir la multiplication…

Corps finis : notions de base

- On rappelle qu'un corps est un anneau dans lequel tout élément en dehors de 0 (élément neutre de l'addition) possède un inverse. Un corps est donc en particulier un anneau intègre (car les diviseurs de zéro d'un anneau non intègre ne peuvent avoir d'inverse : preuve triviale).
- Un corps fini possède un nombre fini d'éléments appelé son cardinal. Dans un corps fini F il existe un plus petit entier p tel que la somme de p termes égaux à l'unité (notée p.1) soit égale à 0
  - Preuve : toutes les sommes n.1 ne peuvent être différentes car le corps est fini. Il existe donc des paires d'entiers i, j telles que
    i.1=j.1 soit k.1=0 avec k=i-j. Notons p le plus petit entier k ayant cette propriété
- L'entier p, appelé caractéristique du corps fini F, est forcément un nombre premier
  - Preuve : si p pouvait être factorisé en q.r (q, r différents de p et de 1) alors (q.r).1=(q.1).(r.1)=0 donc q.1=0 ou r.1=0 car il n'y a pas de diviseurs de 0 ce qui contredit la minimalité de p
  - Nota : il n'y a aucune entourloupe dans la formule (q.r).1=(q.1).(r.1) qui mélange pourtant allègrement la multiplication des entiers et celle du corps (ainsi que la « multiplication » des entiers par les éléments du corps). Pour prendre un exemple vous pourriez ne pas trouver évident que $(2.1_F)*(2.1_F)=4.1_F$ (où l'on a ici distingué les notations). Ecrite $(1_F+1_F)*(1_F+1_F)=1_F+1_F+1_F+1_F$ l'égalité résulte pourtant immédiatement des définitions. En termes techniques, on manipule ici un morphisme d'anneaux (celui qui à tout entier p de Z fait correspondre $p.1_F$ dans le corps).

Construction des corps

- En termes plus abstraits si l'on considère pour tout corps K (pas nécessairement fini) le morphisme d'anneaux de Z dans K : $n \rightarrow n.1_K$, son noyau est donc un idéal de Z donc l'ensemble (p) des multiples d'un entier p (tous les idéaux de Z sont principaux). Deux cas se présentent donc :
  - ✓ Ce noyau est réduit à {0} ce qui signifie que le morphisme est injectif (on rappelle que le noyau mesure le degré de « non injectivité » du morphisme). Le corps K contient donc (un anneau isomorphe à) Z et comme c'est un corps contient donc le corps Q des rationnels. De tels corps sont dits de caractéristique 0.
  - ✓ Ce noyau est (p)=pZ auquel cas p est nécessairement premier (car si p=a.b, $(a.b).1_K=0_K$ impose $a.1_K$ ou $b.1_K=0_K$ donc a ou b égal à p) de tels corps sont dits de caractéristique p. Le corps K contient (donc un corps isomorphe à) Z/pZ (les éléments $n.1_K$ pour n allant de 0 à p-1)
- Nous avons donc deux sortes de corps :
  - ✓ Ceux contenant Q (caractéristique 0)
  - ✓ Ceux contenant Z/pZ pour p premier (caractéristique p)
- Le corps Q des rationnels et les corps Z/pZ des entiers modulo p pour p premier sont pour cette raison appelés corps premiers

Sous-corps et extension de corps

- Considérons maintenant un corps K, dont une partie k est un corps, k est dit dans ce cas sous-corps de K et K une extension de k.
- Point fondamental : dans ce cas, K vérifie toutes les propriétés voulues pour être k-espace vectoriel en effet :
  - ✓ L'addition des « vecteurs » (élément de K) est celle de K, donnant donc un groupe commutatif
  - ✓ Le « scalaire unité » (unité dans k) : 1_k est neutre pour la multiplication d'un « scalaire » (élément de k) par un « vecteur » (élément de K) car $1_k=1_K$
  - ✓ La multiplication des « vecteurs » par les « scalaires » est distributive par rapport à l'addition des « vecteurs » et par rapport à l'addition des « scalaires », car la multiplication dans K est distributive par rapport à l'addition dans K : $a_k.(b_K+c_K)=a_k.b_K+a_k.c_K$ et $(a_k+b_k).c_K=a_k.c_K+b_k.c_K$
  - ✓ La multiplication des « vecteurs » par les « scalaires » est exo-associative $(a_k.b_k).c_K=a_k.(b_k.c_K)$: ici le même symbole . est volontairement utilisé pour les deux opérations (car dans les deux cas il s'agit de la multiplication dans K)
  - ✓ La multiplication d'un « vecteur » quelconque par le « scalaire » 1_k est bien égale au vecteur lui-même $1_k.c_K=c_K$
- Connaître la structure de tout corps possible, se ramène donc à trouver une base de ce corps en tant qu'espace vectoriel sur les corps premiers Q ou Z/pZ

Extension par adjonction

- A titre de corollaire important : tout corps fini K contient Z/pZ avec p premier comme sous-corps, et est par conséquent un Z/pZ-espace vectoriel engendré par une base finie de dimension n: la cardinalité (nombre d'éléments) d'un corps fini vaut donc nécessairement p^n avec p premier et n entier strictement positif.
- Le « jeu » pour trouver les extensions de corps consiste à exhiber la base de ces corps en tant qu'espace vectoriel sur un sous-corps.
- Une manière de faire est d'ajouter à un corps, de nouveaux éléments qui sont racines de polynômes irréductibles dans le corps d'origine faisons le en illustrant le propos par des exemples que vous allez reconnaître…

Extension par adjonction

- Considérons un corps K et k un sous-corps de K. Un élément α de K est dit algébrique sur k s'il existe un polynôme non nul Q de k[X] tels que $Q(\alpha)=0$. Si tel est le cas, il existe un polynôme P unitaire (coefficient du monôme de plus haut degré égal à l'unité) de plus petit degré tel que $P(\alpha)=0$ (tous les polynômes Q tels que $Q(\alpha)=0$ étant multiples de P).
- Le polynôme P est appelé polynôme minimal de α sur k est irréductible sur k (ne peut s'exprimer comme produit de deux polynômes non constants de k[X]), son degré, n, s'appelle degré de α dans k
- Pour tout élément a de k, le polynôme minimal est X-a, les éléments de K-k ayant donc un polynôme minimal de degré >1 : par exemple le nombre $\sqrt{2}$ est de degré 2 dans Q et n'est donc pas un rationnel (racine du polynôme X^2-2 qui est irréductible sur Q) et bien sûr de degré 1 dans R (racine du polynôme $X-\sqrt{2}$), car $\sqrt{2}$ est un réel…

Extension par adjonction

- Si l'on considère maintenant l'ensemble usuellement noté $k(\alpha)$ constitué des éléments de K qui peuvent s'exprimer par une expression polynômiale de α à coefficient dans k (combinaisons linéaires à coefficients dans k des puissances de α).
  - ✓ $k(\alpha)$ est un sous corps de K, c'est le plus petit sous-corps de K contenant k et α, appelé extension élémentaire (ou simple, ou primitive) de degré n de k, dont α est appelé un générateur

    Preuve : La stabilité par multiplication et addition est claire, l'existence de l'inverse d'un élément $Q(\alpha)$ résulte du fait que P est irréductible sur k, donc premier avec Q, donc en écrivant Bezout dans l'anneau k[X] on sait trouver deux polynômes A et B de k[X] tels que AP+BQ=1 donc $B(\alpha)$ est l'inverse cherché (car $P(\alpha)=0$ par définition), ce qui montre que $k(\alpha)$ est bien un corps. Le fait qu'il soit le plus petit est clair.
  - ✓ Les n premières puissances de α ($1, \alpha, \alpha^2, \ldots \alpha^{n-1}$) forment une base de $k(\alpha)$ en tant que k-espace vectoriel (qui est donc de dimension n sur k ce que l'on note $[k(\alpha):k]=n$)

    Preuve : Soit un élément de $k(\alpha)$, donc de la forme $Q(\alpha)$, par division Euclidienne de Q(X) par P(X) dans k[X] on a $Q=D.P+R$ ou $\deg(R)<n$ donc $Q(\alpha)$ s'exprime bien sous la forme de la combinaison linéaire $R(\alpha)$ des n premières puissances de α. D'autre part ces puissances sont bien indépendantes, car une combinaison linéaire nulle non triviale donnerait un polynôme de degré < n ayant α pour racine ce qui contredit la minimalité de P.

Extension par adjonction

- En termes plus abstraits, k(α) peut être identifié à l'anneau quotient k[X]/(P) de k[X] par l'idéal principal engendré par P, les éléments de k(α) étant les classes d'équivalence de la congruence modulo P (car P(α) = 0) que l'on peut désigner par un polynôme de degré < n :
  - ✓ L'addition de ces polynômes de degré < n étant effectuée normalement
  - ✓ La multiplication étant effectuée modulo P
  - ✓ Noter que ce que l'on notait α jusqu'ici n'est rien d'autre que la classe d'équivalence du polynôme X dans la congruence modulo P
  - ✓ Un élément quelconque de k(α) noté jusqu'à présent $a_{n-1}\alpha^{n-1}+\ldots+a0$ est par conséquent la classe du polynôme $a_{n-1}X^{n-1}+\ldots+a0$ dans la congruence modulo P et peut être désigné par ce polynôme
  - ✓ Cela permet de construire les extensions élémentaires en ne faisant apparaître que le polynôme irréductible P (et pas la racine explicite α ni le « grand » corps K le contenant)

Extension par adjonction

- Exemple 1
  - ✓ Si k=Q et P=X^2-2, l'extension est de degré 2 (Q-espace vectoriel de dimension 2) et peut être vue comme l'ensemble des polynômes de degré <2 à coefficients dans Q tels que :
    - ✓ aX+b +cX+d=(a+c)X+(b+d)
    - ✓ [aX+b][cX+d]=acX^2+(ad+bc)X+bd mod X^2-2=(ad+bc)X+bd+2ac autrement dit en notant √2 la classe de X : [a√2+b][c√2+d] = (ad+bc)√2 +bd+2ac… Ce corps s'appelle Q(√2), ce n'est pas ainsi que nous construirons R, car R est de dimension infinie sur Q
- Exemple2
  - ✓ Si k=R et P=X^2+1, l'extension est de degré 2 (R-espace vectoriel de dimension 2) et peut être vue comme l'ensemble des polynômes de degré <2 à coefficients dans R tels que :
    - ✓ aX+b +cX+d=(a+c)X+(b+d)
    - ✓ [aX+b][cX+d]=acX^2+(ad+bc)X+bd mod X^2+1=(ad+bc)X+bd-ac autrement dit en notant i la classe de X : [a.i+b][c.i+d] = (ad+bc)i + bd - ac… Corps qui doit vous rappeler quelque chose… A partir du même polynôme mais sur Q, on construit Q(i), sous ensemble des nombres complexes dont les parties réelles et imaginaires sont rationnelles…

Extension de corps : propriétés

- Pour tout corps K et tout polynôme P de K[X], il existe donc une extension finie (de dimension finie sur K) de K dans laquelle P admet une racine. Une telle extension s'appelle corps de rupture de P sur K.
  Preuve : on suppose P irréductible sur K (sinon on refait le raisonnement sur ses facteurs irréductibles), l'extension élémentaire K[X]/(P) convient.
- Pour tout corps K et tout polynôme P de K[X], il existe une extension finie de K dans laquelle P se décompose en produits de polynômes de degré 1 : P pouvant être supposé unitaire sans perte de généralité (coefficient du terme dominant égal à 1) : $P(X)=(X-\alpha_1)(X-\alpha_2)\ldots(X-\alpha_n)$, où les α_i sont éléments de cette extension.
  Preuve : par récurrence immédiate en utilisant la proposition précédente, en remplaçant à chaque étape le corps par l'extension élémentaire construite pour ajouter la racine α_i et en divisant le polynôme par $(X-\alpha_i)$
- Une extension ayant cette propriété est appelée corps de décomposition de P sur K. Un corps de décomposition minimal est appelé corps des racines de P sur K. Le corps des racines d'un polynôme P sur un corps K est unique à un isomorphisme près (preuve : par une récurrence soigneuse non détaillée ici)
  Exemples : C est « le » corps des racines de X^2+1 sur R, $Q(\sqrt{2})$ « le » corps des racines de X^2-2 sur Q) et Q(i) « le » corps des racines de X^2+1 sur Q.

Structure des corps finis

- Les corps finis sont constitués exactement des racines des polynômes $X^{p^n} - X$ sur Z/pZ (p premier n entier >0), donc pour résumer sont constitués de l'élément 0 et des racines p^n-1 de l'unité…

  Preuve : par le théorème de Lagrange dans le sous-groupe multiplicatif K^* d'ordre p^n-1, la relation est vérifiée pour tout élément non nul. Elle l'est également de manière évidente pour l'élément 0. Les éléments de K sont donc exactement les p^n racines du polynôme indiqué, qui sont bien toutes distinctes comme peut s'en convaincre facilement (le polynôme dérivé vaut -1 qui n'a donc pas de racine ce qui exclut l'existence de racine multiple)

- Il existe pour tout p premier, des polynômes irréductibles sur Z/pZ de tout degré n>0, ce qui permet de construire ces corps

  Preuve : par analyse fine des polynômes cyclotomiques (relatifs aux racines nièmes de l'unité) ou comme on le fera en TD par dénombrement : il y a p polynômes unitaires de degré 1 tous irréductibles, p^2 polynômes unitaires de degré 2 dont p+p(p+1)/2 sont de degré 1 ou produits de polynômes de degré 1 il en reste donc p(p-1)/2 d'irréductibles de degré 2 etc.

- Nota : Dans les cas où il y a plusieurs polynômes irréductibles de même degré, il y a donc plusieurs constructions possibles… Les mathématiques nous affirment que ces constructions sont « isomorphes » (c.a.d. qu'on passe d'une construction à une autre par simple « renommage », des éléments, nous verrons cela en TD), il n'empêche que dans les utilisations pratiques, il vaut mieux être d'accord sur « la » construction que vous utilisez pour $F(2^8)$… Ces considérations matérielles sont sans importance pour le mathématicien… Mais vitales pour le cryptologue…

Structure des corps finis

- Dernier point que vous devez savoir pour devenir utilisateurs avisés des corps finis en cryptologie, le sous groupe multiplicatif K* d'un corps fini est cyclique, à savoir donc qu'il en existe des générateurs…
- Lemme (rappel ?) : si les ordres (p resp. q) des éléments (a resp. b) d'un groupe sont premiers entre eux, alors l'ordre de leur produit est le produit des ordres
  Preuve : 1 est le seul élément de l'intersection des groupes cycliques <a> et <b> engendrés par a et b respectivement, car l'ordre d'un élément de cette intersection doit diviser p et q et par suite vaut 1. Soit d l'ordre de ab : $(ab)^d=1$, donc $a^d=(b^d)^{-1}$ appartient donc à l'intersection, d'ou donc $a^d=b^d=1$, par conséquent d est multiple de p et q donc de pq et d'un autre côté $(ab)^{pq}=a^{pq}.b^{qp}=1$
- Lemme : Le lemme précédent s'étend par récurrence immédiate : soient n éléments d'un groupe dont les ordres sont premiers entre eux deux à deux. Alors l'ordre du produit est égal au produit des ordres.

Structure des corps finis

- Théorème : les racines nièmes de l'unité dans un corps K forment un groupe multiplicatif. Si la caractéristique du corps K est nulle ou ne divise pas n, alors le groupe des racines nièmes de l'unité dans le corps des racines de X^n-1 sur le corps premier de K, est un groupe cyclique d'ordre n.
- Preuve : c'est un groupe car le produit de deux racines nièmes de l'unité est clairement une racine nième de l'unité. Pour l'inverse considérer pour un élément a : $(a^{-1})^n=(a^n)^{-1}=1$, l'inverse d'une racine nième de l'unité est une racine nième de l'unité.
- Si la caractéristique du corps est nulle ou ne divise pas n, alors dans le corps des racines de X^n-1 défini sur le corps premier de K, il y a exactement n racines nièmes de l'unité toutes distinctes car racines du polynôme X^n-1 qui a n racines qui sont bien toutes distinctes car une racine multiple serait aussi racine du polynôme dérivé nX^{n-1} (dont la seule racine puisque la caractéristique du corps est nulle ou ne divise pas n est 0, qui n'est pas racine nième de l'unité). Ainsi le groupe est dans ce cas d'ordre n
- Pour prouver qu'il est cyclique, on exhibe un élément d'ordre n

Structure des corps finis

Soit la décomposition de n en puissances premières $n=p_1^{n1}.p_2^{n2}\ldots p_k^{nk}$

Pour tout i tel que 1<=i<=k on peut toujours trouver un a_i tel que $a_i^{n/p_i} \neq 1$

Car le nombre de racines de $X^{n/p_i} - 1$ est au plus égal à n/p_i

On pose $m_i = n/p_i^{ni}$ et $b_i = a_i^{m_i}$ Les b_i sont d'ordre p_i^{ni}

car la puissance p_i^{ni} de b_i est $a_i^{n} = 1$: l'ordre de b_i divise donc p_i^{ni}

et la puissance p_i^{ni-1} de b_i est $a_i^{n/p_i} \neq 1$

Par conséquent les b_i ayant des ordres deux à deux premiers entre eux, leur produit $b=b_1.b_2\ldots b_n$ a pour ordre le produit des ordres (lemme), ainsi b est d'ordre n et est générateur du groupe. Une telle racine est appelée racine primitive de l'unité.

Corollaire : le sous groupe multiplicatif d'un corps fini est cyclique (théorème précédent appliqué au cas n=Card(K)-1 soit p^m -1 où p est la caractéristique de K et m sa dimension en tant que Z/pZ espace vectoriel)

Logarithmes discrets sur les corps finis

- Ce qui précède montre qu'il existe toujours dans un corps fini des racines primitives [Card(K)-1]ièmes de l'unité : soit α une de ces racines.
- Alors pour tout élément a non nul de K on sait trouver un entier L ($0<=L<=Card(K)-1$) tel que $\alpha^L=a$
- L est appelé logarithme en base α de a et noté $\log_\alpha(a)$
- Il résulte des définitions que étant donnés deux éléments a et b non nuls de K : $a.b=\alpha^{\log_\alpha(a)}.\alpha^{\log_\alpha(b)}=\alpha^{\log_\alpha(a)+\log_\alpha(b)}=\alpha^{\log_\alpha(ab)}$,
  Soit $\log_\alpha(a.b)=\log_\alpha(a)+\log_\alpha(b)$
- Dans les corps finis de taille modeste on peut ainsi tabuler $\log_\alpha$ et son inverse (l'exponentielle de base α) et s'en servir pour effectuer des multiplications
- On rappelle que le logarithme discret est en revanche un problème difficile dans les corps finis de taille importante.

Exemple du corps à 4 éléments F4

- Un seul polynôme irréductible de degré 2 : X^2+X+1 (c'est le seul, démonstration en TD), permet de construire F4 :
- $(Z/2Z[X])/(X^2+X+1)$ en tant que $Z/2Z$ espace vectoriel de dimension 2 dont la base est (X^0, X^1), donc constitué des polynômes de degré maximal 1 à coefficients dans $Z/2Z$, la multiplication étant effectuée modulo X^2+X+1, ou ce qui revient au même expressions polynomiales $Z/2Z(\alpha)$ où α est l'une des racines de X^2+X+1, l'autre étant $\alpha^2=\alpha+1$ que l'on peut noter β
- F4 contient donc les éléments 0, 1, α et $\alpha+1$ (vision espace vectoriel)
- C'est aussi le corps des racines du polynôme $X^4+X=X(X^3+X)=X(X+1)(X^2+X+1)$ constitué de 0 et des racines cubiques de l'unité (1, α et β). Les générateurs de F4* sont α et β tous deux utilisables pour faire des log.

Exemple du corps à 8 éléments F8

- Deux polynômes irréductibles X^3+X+1 et X^3+X^2+1 (ce sont les seuls possibles de degré 3, démonstration en TD), permettent l'un ou l'autre de construire F8 :
- $(Z/2Z[X])/(X^3+X+1)$ en tant que $Z/2Z$ espace vectoriel de dimension 3 dont la base est (X^0, X^1, X^2), donc constitué des polynômes de degré maximal 2 à coefficients dans $Z/2Z$, la multiplication étant effectuée modulo X^3+X+1, ou ce qui revient au même expressions polynomiales
  $Z/2Z(\gamma)$ où γ est l'une des racines de X^3+X+1.
- $(Z/2Z[X])/(X^3+X^2+1)$ en tant que $Z/2Z$ espace vectoriel de dimension 3 dont la base est (X^0, X^1, X^2), donc constitué des polynômes de degré maximal 2 à coefficients dans $Z/2Z$, la multiplication étant effectuée modulo X^3+X^2+1, ou ce qui revient au même expressions polynomiales
  $Z/2Z(\delta)$ où δ est l'une des racines de X^3+X^2+1.

Exemple du corps à 8 éléments F8

Cela donne donc une table d'addition

	0	**1**	**X**	**X+1**	**X^2**	**X^2+1**	**X^2+X**	**X^2+X+1**
0	0	1	X	X+1	X^2	X^2+1	X^2+X	X^2+X+1
1	1	0	X+1	X	X^2+1	X^2	X^2+X+1	X^2+X
X	X	X+1	0	1	X^2+X	X^2+X+1	X^2	X^2+1
X+1	X+1	X	1	0	X^2+X+1	X^2+X	X^2+1	X^2
X^2	X^2	X^2+1	X^2+X	X^2+X+1	0	1	X	X+1
X^2+1	X^2+1	X^2	X^2+X+1	X^2+X	1	0	X+1	X
X^2+X	X^2+X	X^2+X+1	X^2	X^2+1	X	X+1	0	1
X^2+X+1	X^2+X+1	X^2+X	X^2+1	X^2	X+1	X	1	0

(que l'on peut tout aussi valablement écrire en utilisant les mêmes expressions polynomiales de γ ou δ)

Exemple du corps à 8 éléments F8

Cela donne en revanche une table de multiplication modulo X^3+X+1

	0	**1**	**γ**	**γ+1**	**γ²**	**γ²+1**	**γ²+γ**	**γ²+γ+1**
0	0	0	0	0	0	0	0	0
1	0	1	γ	γ+1	γ²	γ²+1	γ²+γ	γ²+γ+1
γ	0	γ	γ²	γ²+γ	γ+1	1	γ²+γ+1	γ²+1
γ+1	0	γ+1	γ²+γ	γ²+1	γ²+γ+1	γ²	1	γ
γ²	0	γ²	γ+1	γ²+γ+1	γ²+γ	γ	γ²+1	1
γ²+1	0	γ²+1	1	γ²	γ	γ²+γ+1	γ+1	γ²+γ
γ²+γ	0	γ²+γ	γ²+γ+1	1	γ²+1	γ+1	γ	γ²
γ²+γ+1	0	γ²+γ+1	γ²+1	γ	1	γ²+γ	γ²	γ+1

(ici écrite en explicitant le fait qu'il s'agit d'expressions polynomiales de γ)

Exemple du corps à 8 éléments F8

Et une autre table de multiplication modulo X^3+X^2+1

	0	**1**	**δ**	**δ+1**	**δ²**	**δ²+1**	**δ²+δ**	**δ²+δ+1**
0	0	0	0	0	0	0	0	0
1	0	1	δ	δ+1	δ²	δ²+1	δ²+δ	δ²+δ+1
δ	0	δ	δ²	δ²+δ	δ²+1	δ²+δ+1	1	δ+1
δ+1	0	δ+1	δ²+δ	δ²+1	1	δ	δ²+δ+1	δ²
δ²	0	δ²	δ²+1	1	δ²+δ+1	δ+1	δ	δ²+δ
δ²+1	0	δ²+1	δ²+δ+1	δ	δ+1	δ²+δ	δ²	1
δ²+δ	0	δ²+δ	1	δ²+δ+1	δ	δ²	δ+1	δ²+1
δ²+δ+1	0	δ²+δ+1	δ+1	δ²	δ²+δ	1	δ²+1	δ

(ici écrite en explicitant le fait qu'il s'agit d'expressions polynomiales de δ)

Exemple du corps à 8 éléments F8

- Mais F8 est « le » corps des racines de X^8-X (ou X^8+X) qui d'ailleurs vaut $X(X+1)(X^3+X+1)(X^3+X^2+1)$ constitué de 0 et des 7 racines $7^{èmes}$ de l'unité (dont 1) toutes distinctes.
- Noter incidemment que les éléments α et β de F4 n'appartiennent pas à F8 car $\alpha^3=\beta^3=1$ donc $\alpha^7=\alpha$ et $\beta^7=\beta$ tous deux différents de 1
- Les maths nous affirment donc que les constructions sont isomorphes (un simple changement de nom doit transformer une table de multiplication en l'autre en laissant stable la table d'addition)… l'isomorphisme n'étant pas en évidence…
- Mais ici encore les maths vont nous sortir d'affaire…

Exemple du corps à 8 éléments F8

- Car on connaît déjà un automorphisme : Frobenius (élévation au carré). En effet pour tout couple d'éléments $(\xi+\psi)^2=\xi^2+\psi^2$ et bien évidemment $(\xi.\psi)^2=\xi^2.\psi^2$
- Il est facile de voir (par exemple) que Frobenius effectue les deux permutations circulaires
  $\gamma->\gamma^2->\gamma^2+\gamma->\gamma$
  $\gamma+1->\gamma^2+1->\gamma^2+\gamma+1->\gamma+1$
- Frobenius au carré est un autre automorphisme qui effectue donc les permutations
  $\gamma->\gamma^2+\gamma->\gamma^2->\gamma$
  $\gamma+1->\gamma^2+\gamma+1->\gamma^2+1->\gamma+1$
- Frobenius au cube est l'identité car les éléments de F8 sont racines de X^8-X

Exemple du corps à 8 éléments F8

- Pour trouver l'isomorphisme des deux constructions de F8, on peut s'inspirer de ce qui précède pour faire correspondre les éléments exprimés dans « la base δ » et ceux exprimés dans « la base γ »
- Or le sous groupe multiplicatif des F8 étant d'ordre 7, tout élément de F8* différent de 1 (et donc en particulier γ ou δ) est générateur de ce groupe. Les éléments différents de 0 peuvent donc être exprimés comme combinaisons linéaires (par exemple) de γ et γ^2 (vision espace vectoriel) ou comme puissances de γ (vision génération du groupe multiplicatif)
  $\gamma(=\gamma)->\gamma^2(=\gamma^2)->\gamma^3(=\gamma+1)->\gamma^4(=\gamma^2+\gamma)->\gamma^5(=\gamma^2+\gamma+1)->\gamma^6(=\gamma^2+1)$
- De même
  $\delta(=\delta)->\delta^2(=\delta^2)->\delta^3(=\delta^2+1)->\delta^4(=\delta^2+\delta+1)->\delta^5(=\delta+1)->\delta^6(=\delta^2+\delta)$
- γ^7 ou δ^7 valent 1 car sont racines 7èmes de l'unité

Exemple du corps à 8 éléments F8

- Or grâce à Frobenius on sait que si γ est une racine de X^3+X+1, les deux autres sont γ^2 et γ^4 et que par conséquent γ^3, γ^5 et γ^6 sont donc les trois racines de X^3+X^2+1
- Cela est facile à vérifier directement car par exemple $\gamma^9=\gamma^2$, $\gamma^6=\gamma^2+1$ donc $\gamma^9+\gamma^6+1=0$
- On a donc trois isomorphismes possibles
  $\delta \to \gamma^3=\gamma+1$ donc $\delta^2 \to \gamma^6=\gamma^2+1$ et $\delta^4 \to \gamma^{12}=\gamma^5=\gamma^2+\gamma+1$
  $\delta \to \gamma^5=\gamma^2+\gamma+1$ donc $\delta^2 \to \gamma^{10}=\gamma^3=\gamma+1$ et $\delta^4 \to \gamma^{20}=\gamma^6=\gamma^2+1$
  $\delta \to \gamma^6=\gamma^2+1$ donc $\delta^2 \to \gamma^{12}=\gamma^5=\gamma^2+\gamma+1$ et $\delta^4 \to \gamma^{24}=\gamma^3=\gamma+1$
- Parmi ces trois isomorphismes l'un est l'identité (mais il n'y a aucun moyen de savoir lequel, cela correspond à l'arbitraire de la racine appelée γ ou δ) les deux autres sont Frobenius et Frobenius au carré.

Exemple du corps à 8 éléments F8

- Pour les sceptiques : prendre n'importe quelle opération de la table de multiplication avec les δ, par exemple : $\delta^2*\delta=\delta^2+1$
- Transformer en γ par l'un des isomorphismes
  $\delta->\gamma^3=\gamma+1$, $\delta^2->\gamma^6=\gamma^2+1$, $\delta^2+1->\gamma^6+1=\gamma^2$
- Vérifier dans la table sur les γ, que l'on a bien $(\gamma+1)(\gamma^2+1)=\gamma^2$
- …

Exemple du corps à 16 éléments F16

- F16 peut être construit comme espace vectoriel de dimension 4 sur F2 à partir de l'un des trois polynômes irréductibles de degré 4 identifiés en TD : X^4+X+1, X^4+X^3+1 et $X^4+X^3+X^2+X+1$
- F16 est donc constitué des racines de $X^{16}+X$ soit 0 et les 15 racines $15^{èmes}$ de l'unité
- Parmi ces racines $15^{èmes}$ de l'unité il y a les racines cubiques de l'unité, éléments de F4 donc inclus dans F16
- $X^{16}+X = X(X+1)(X^2+X+1)(X^4+X+1)(X^4+X^3+1)(X^4+X^3+X^2+X+1)$ donc F16 contient 0, 1, α et β (éléments de F4) ainsi que les 3*4 racines des polynômes de degré 4 permettant de construire F16
- Deux constructions quelconques peuvent être mises en correspondance par 4 isomorphismes (puissances de Frobenius de 0 à 3)
- Mais F16 peut donc aussi être construit comme extension de F4…

Exemple du corps à 16 éléments F16

- Pour construire F16 comme extension de dimension 2 de F4 au lieu d'extension de dimension 4 de F2, il faut des polynômes unitaires irréductibles de degré 2 de F4[X]
- Les polynômes unitaires irréductibles de degré 1 de F4[X] sont X, X+1, X+α et X+β
- Un polynôme unitaire irréductible de degré 2 doit avoir son coefficient de X^2 égal à 1 et son coefficient de X^0 non nul, reste donc 12 polynômes candidats dont il faut exclure les 6 produits de X+1, X+α et X+β
- Reste donc $X^2+X+\alpha$, $X^2+X+\beta$, $X^2+\alpha X+1$, $X^2+\beta X+1$, $X^2+\alpha X+\alpha$, $X^2+\beta X+\beta$
- On vérifie facilement que l'un quelconque est bien irréductible car n'admet pas de racine dans F4 (rappel $\alpha^2=\alpha+1=\beta$, $\beta^2=\beta+1=\alpha$ donc $\alpha+\beta=\alpha.\beta=1$)

Exemple du corps à 16 éléments F16

- On vérifie aussi facilement que le produit de X, X+1, X^2+X+1 et des 6 polynômes générateurs vaut $X^{16}+1$, donc les éléments de F16 sont 0, 1, α, β et les 6*2 racines des polynômes générateurs.
- Désignant par Γ une racine de $X^2+X+\alpha$, les éléments de F16 sont de la forme $a\Gamma+b$ où a et b sont éléments de F4 (vision espace vectoriel de dimension 2 sur F4)
- Attention cette fois, à l'exception des racines de X^2+X+1, ce n'est pas l'élévation au carré mais à la puissance 4 qui fait passer d'une racine à l'autre, la seconde racine de $X^2+X+\alpha$ est Γ^4 (rappel $\alpha^4=\alpha$)
- Entre deux constructions quelconques existent deux isomorphismes naturels (obtenus par mises en correspondance des racines de polynôme de construction)
- Avec un peu de calcul on trouve dans F16* des éléments d'ordre 1, 3, 5 et 15

Le successeur du DES : AES

- Conscient de la faiblesse potentielle du DES le NIST Américain (National Institute for Standards and Technologies) lance en 1997 un appel d'offres pour élaborer un nouveau standard : l'Advanced Encryption System AES
- Le 2 Octobre 2000, l'algorithme retenu par le NIST est le Rijndael (prononcer «Rain Doll») conçu par deux belges, Joan Daemen et Vincent Rijmen.
- Le 26 Novembre 2001, le nouveau standard est publié en tant que Federal Information Processing Standard (FIPS)
- L'algorithme traite l'entrée par blocs de 128 bits avec une clé de longueur 128, 192 ou 256 bits

AES : Conventions (1/3)

- Le bloc de 128 bits est considéré comme un séquence de 16 octets avec les conventions usuelles (bit de poids fort en premier) puis recopié dans un tableau 4*4 («état») avec les conventions suivantes :

B0	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12	B13	B14	B15

b7	b6	b5	b4	b3	b2	b1	b0

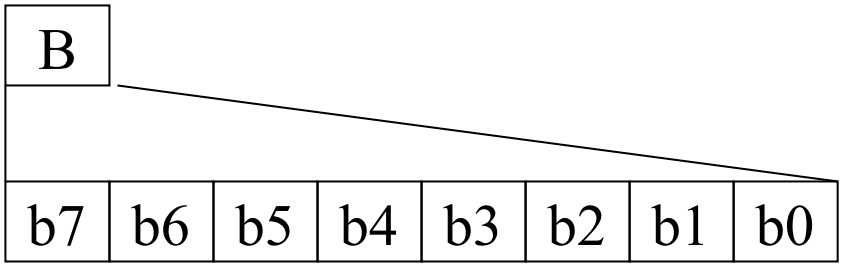
$$B0 = \sum_{i=0}^{7} bi * 2^i$$

Exemple : 10011101 = {9D}

B0	B4	B8	B12
B1	B5	B9	B13
B2	B6	B10	B14
B3	B7	B11	B15

AES : Conventions (2/3)

- AES manipule les octets comme des polynômes de degré <=7 dont les coefficients sont les bits



$$B \Leftrightarrow \sum_{i=0}^{7} bi.x^{i}$$

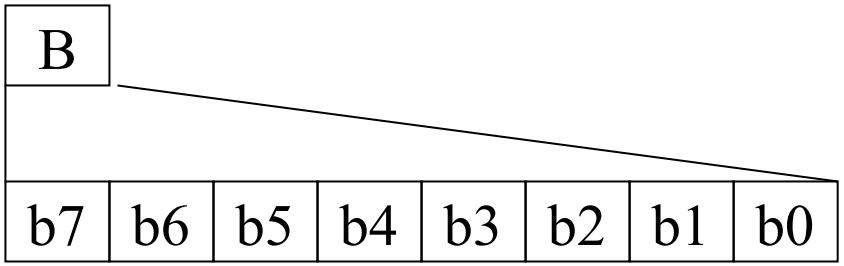
Exemple : {9D} <=> 10011101 <=> $x^7+x^4+x^3+x^2+1$

L'addition de deux octets est alors l'addition modulo 2 des coefficients (équivalent au XOR bit à bit) :

$$\{57\} \oplus \{83\} = ?$$

AES : Conventions (2/3)

- AES manipule les octets comme des polynômes de degré <=7 dont les coefficients sont les bits



$$B \Leftrightarrow \sum_{i=0}^{7} bi.x^i$$

Exemple : {9D} <=> 10011101 <=> $x^7+x^4+x^3+x^2+1$

L'addition de deux octets est alors l'addition modulo 2 des coefficients (équivalent au XOR bit à bit) :

$$\{57\} \oplus \{83\} = 01010111 \oplus 10000011 = 11010100 = \{D4\}$$

AES : Conventions (3/3)

- La multiplication de deux octets est la multiplication polynomiale de leurs polynômes représentatifs, modulo un polynôme *irréductible* de degré 8 :

  $m(x) = x^8 + x^4 + x^3 + x + 1$ ou {01}{1B} en hexa

- Ainsi le résultat reste un polynôme de degré <=7
- Contrairement à l'addition, il n'existe pas d'opération simple au niveau des octets correspondant à cette multiplication

AES : Le corps fini GF(2^8)

- Dûment muni de ces opérations, l'ensemble des octets a une structure de corps fini ou corps de Galois (Galois Field) à 2^8 éléments noté GF(2^8)
- En particulier tout élément non nul a un inverse ce qui est conséquence du fait que le polynôme m est irréductible c'est-à-dire « premier » (on montre ci-après : Algorithme d'Euclide, qu'un élément est inversible modulo un autre si et seulement si ils sont premiers entre eux)
- On démontre que tout corps fini est isomorphe au corps GF(p^m) des polynômes de degré m-1 à coefficients entiers modulo p (premier), la multiplication étant modulo un polynôme irréductible de degré m si m>1

AES : Propriétés des corps finis

- Dans $GF(p^m)$, p est la caractéristique du corps, p^m est sa cardinalité
- GF(p) est le corps des entiers modulo p souvent noté Z/pZ
- Pour tout élément u de $GF(p^m)$, on a : $\underbrace{u + u + \ldots + u}_{p} = 0$

- En particulier dans $GF(2^8)$ on a pour tout élément u +u=0 ce qui signifie qu'additionner et soustraire sont équivalents (pas de risque de fautes de signe !)

AES : Exemples de calculs dans GF(2^8) : Produits

Exercice : Effectuer dans GF(2^8) la multiplication :

$$\{19\} \bullet \{3F\}$$

On rappelle que le polynôme modulo est m={01}{1B}

AES : Exemples de calculs dans GF(2^8) : Produits

Soit à effectuer la multiplication notée $\{19\} \bullet \{3F\}$

$$\{19\} \bullet \{3F\} = 00011001 \bullet 00111111 \Leftrightarrow$$

$$\left(x^4 + x^3 + 1\right)\left(x^5 + x^4 + x^3 + x^2 + x + 1\right) = x^9 + x^5 + x^4 + x^2 + x + 1$$

Pour prendre le modulo $m(x) = x^8 + x^4 + x^3 + x + 1$

Il faut soustraire $x.m(x) = x^9 + x^5 + x^4 + x^2 + x$

Conclusion $\{19\} \bullet \{3F\} = \{01\}$

AES : Exemples de calculs dans GF(2^8) : Division Euclidienne

Exercice : Effectuer la division Euclidienne de m={01}{1B} par {19} (trouver le quotient et le reste par division polynomiale)

AES : Exemples de calculs dans GF(2^8) : Division Euclidienne

Dividende
m={01}{1B}

$x^8 + x^4 + x^3 + x + 1$ | $x^4 + x^3 + 1$ — Diviseur {19}

$x^8 + x^7 + x^4$ | $x^4 + x^3 + x^2 + x + 1$

$x^7 + x^3 + x + 1$

$x^7 + x^6 + x^3$

Quotient 00011111
soit {1F}

$x^6 + x + 1$

$x^6 + x^5 + x^2$

$x^5 + x^2 + x + 1$

$x^5 + x^4 + x$

$m = \{1F\} \bullet \{19\} + \{0C\}$

$x^4 + x^2 + 1$

$x^4 + x^3 + 1$

$x^3 + x^2$ ←

Reste 00001100
soit {0C}

AES : Algorithme d'Euclide étendu dans un corps fini

Pour déterminer le pgcd de deux éléments a et b dans GF(p^m) :

- Tout diviseur de a et b divise a mod b = a - qb, par conséquent : g=pgcd(a,b)=pgcd(b,a mod b) => Algorithme d'Euclide
- Par divisions successives on construit une suite de restes strictement décroissante. Le dernier reste non nul est g=pgcd
- On a donc à l'avant-dernière étape $a_n=q_nb_n+g$ et à l'étape d'avant $a_{n-1}=q_{n-1}b_{n-1}+r_{n-1}$ (avec $a_n=b_{n-1}$ et $b_n=r_{n-1}$).
  En reportant dans la première : $b_{n-1}=q_n(a_{n-1}-q_{n-1}b_{n-1})+g$
- Par récurrence, on peut donc à toute étape exprimer g comme combinaison linéaire de a_i et b_i, donc en particulier trouver u et v tels que g=au+bv (identité de Bezout) que l'on détermine donc en « remontant » toutes les divisions euclidiennes

AES : Recherche de l'inverse d'un élément d'un corps fini (1/2)

- Ce qui précède montre que si a et b sont premiers entre eux, alors on peut trouver u et v vérifiant au+bv=1,
  donc a possède un inverse modulo b qui est u mod b (et b possède un inverse modulo a qui est v mod a)
- Réciproquement si on peut inverser a modulo b il existe u tel que au=1 mod b soit au=1+kb.
  Un diviseur de a et b divise par conséquent a-kb=1, donc a et b sont premiers entre eux
- Par conséquent a possède un inverse modulo b (et b possède un inverse modulo a) <=> a et b premiers entre eux
- Inversion d'un élément a de GF(2^8) : par algorithme d'Euclide étendu entre a et le polynôme irréductible m(x)

AES : Recherche de l'inverse d'un élément d'un corps fini (2/2)

- Exercice : Utiliser l'algorithme d'Euclide étendu pour inverser l'élément {19} de GF(2^8)
- On rappelle que le polynôme modulo est m={01}{1B} et que la première division de l'algorithme est par conséquent {01}{1B} / {19} qui vient d'être effectué à titre d'exercice

AES : Recherche de l'inverse d'un élément d'un corps fini (2/2)

- Soit à inverser l'élément {19} de GF(2^8)
- La première étape ci-avant montre que $m = \{1F\} \bullet \{19\} + \{0C\}$
- Deuxième étape : Dividende {19}

$x^4 + x^3 + 1$	$x^3 + x^2$ Diviseur
$x^4 + x^3$	{0C}
	x
1	$\boxed{\{19\} = \{02\} \bullet \{0C\} + \{01\}}$

- D'où :

$$\{19\} + \{02\} \bullet (m + \{1F\} \bullet \{19\}) = \{01\}$$

$$\{19\} \bullet (\{01\} + \{02\} \bullet \{1F\}) = \{01\}$$

$$\{02\} \bullet \{1F\} \Leftrightarrow x(x^4 + x^3 + x^2 + x + 1)$$

$$x^5 + x^4 + x^3 + x^2 + x \Leftrightarrow 00111110 = \{3E\}$$

$\boxed{\{19\}^{-1} = \{01\} + \{3E\} = \{3F\}}$ Identité vérifiée plus haut

Une astuce pour calculer dans $GF(2^8)$: logarithmes discrets

- On cherche un générateur du groupe multiplicatif $GF(2^8)^*$: avec le polynôme modulo de Rijndael {03} est un tel générateur : les puissances successives de {03} parcourent les 255 éléments de $GF(2^8)^*$ de sorte que $\{03\}^{255} = \{01\}$
- On dresse alors la table des $\{03\}^i$, et son inverse qui représente le logarithme discret à base {03}
- Cela est possible du fait de que $GF(2^8)$ est un corps de taille modeste (le calcul du logarithme dans un corps de grande taille est très difficile : cf. ci-après)

Une astuce pour calculer dans GF(2^8) : logarithmes discrets

- Table des {03}^CL :

	0	**10**	**20**	**30**	**40**	**50**	**60**	**70**	**80**	**90**	**100**	**110**	**120**	**130**	**140**	**150**	**160**	**170**	**180**	**190**	**200**	**210**	**220**	**230**	**240**	**250**
0	01	72	D8	66	6A	04	D3	4D	83	B3	10	61	2F	3A	FA	40	9F	BC	E8	C5	1B	4A	C6	8D	39	6C
1	03	96	73	AA	BE	0C	6E	D7	9E	CE	30	A3	71	4E	15	C0	BA	DF	23	54	2D	DE	51	8C	4B	B4
2	05	A1	95	E5	D9	14	B2	62	B9	49	50	FE	93	D2	3F	5B	D5	7A	65	FC	77	79	F3	8F	DD	C7
3	0F	F8	A4	34	70	3C	CD	A6	D0	DB	F0	19	AE	6D	41	ED	64	8E	AF	1F	99	8B	0E	8A	7C	52
4	11	13	F7	5C	90	44	4C	F1	6B	76	0B	2B	E9	B7	C3	2C	AC	89	EA	21	B0	86	12	85	84	F6
5	33	35	02	E4	AB	CC	D4	08	BD	9A	1D	7D	20	C2	5E	74	EF	80	25	63	CB	91	36	94	97	01
6	55	5F	06	37	E6	4F	67	18	DC	B5	27	87	60	5D	E2	9C	2A	9B	6F	A5	46	A8	5A	A7	A2	03
7	FF	E1	0A	59	31	D1	A9	28	7F	C4	69	92	A0	E7	3D	BF	7E	B6	B1	F4	CA	E3	EE	F2	FD	05
8	1A	38	1E	EB	53	68	E0	78	81	57	BB	AD	FB	32	47	DA	82	C1	C8	07	45	3E	29	0D	1C	0F
9	2E	48	22	26	F5	B8	3B	88	98	F9	D6	EC	16	56	C9	75	9D	58	43	09	CF	42	7B	17	24	11

Une astuce pour calculer dans GF(2^8) : logarithmes discrets

- Table des $\log_{\{03\}}$(CL) (valeurs en décimal) :

0	**0**	**10**	**20**	**30**	**40**	**50**	**60**	**70**	**80**	**90**	**A0**	**B0**	**C0**	**D0**	**E0**	**F0**
0		100	125	101	150	102	126	43	175	44	127	204	151	83	68	103
1	0	4	194	47	143	221	110	121	88	215	12	187	178	57	17	74
2	25	224	29	138	219	253	72	10	168	117	246	62	135	132	146	237
3	1	14	181	5	189	48	195	21	80	122	111	90	144	60	217	222
4	50	52	249	33	54	191	163	155	244	235	23	251	97	65	35	197
5	2	141	185	15	208	6	182	159	234	22	196	96	190	162	32	49
6	26	129	39	225	206	139	30	94	214	11	73	177	220	109	46	254
7	198	239	106	36	148	98	66	202	116	245	236	134	252	71	137	24
8	75	76	77	18	19	179	58	78	79	89	216	59	188	20	180	13
9	199	113	228	240	92	37	107	212	174	203	67	82	149	42	124	99
A	27	8	166	130	210	226	40	172	233	95	31	161	207	158	184	140
B	104	200	114	69	241	152	84	229	213	176	45	108	205	93	38	128
C	51	248	154	53	64	34	250	243	231	156	164	170	55	86	119	192
D	238	105	201	147	70	136	133	115	230	169	118	85	63	242	153	247
E	223	28	9	218	131	145	61	167	173	81	123	41	91	211	227	112
F	3	193	120	142	56	16	186	87	232	160	183	157	209	171	165	7

Une astuce pour calculer dans GF(2^8) : logarithmes discrets

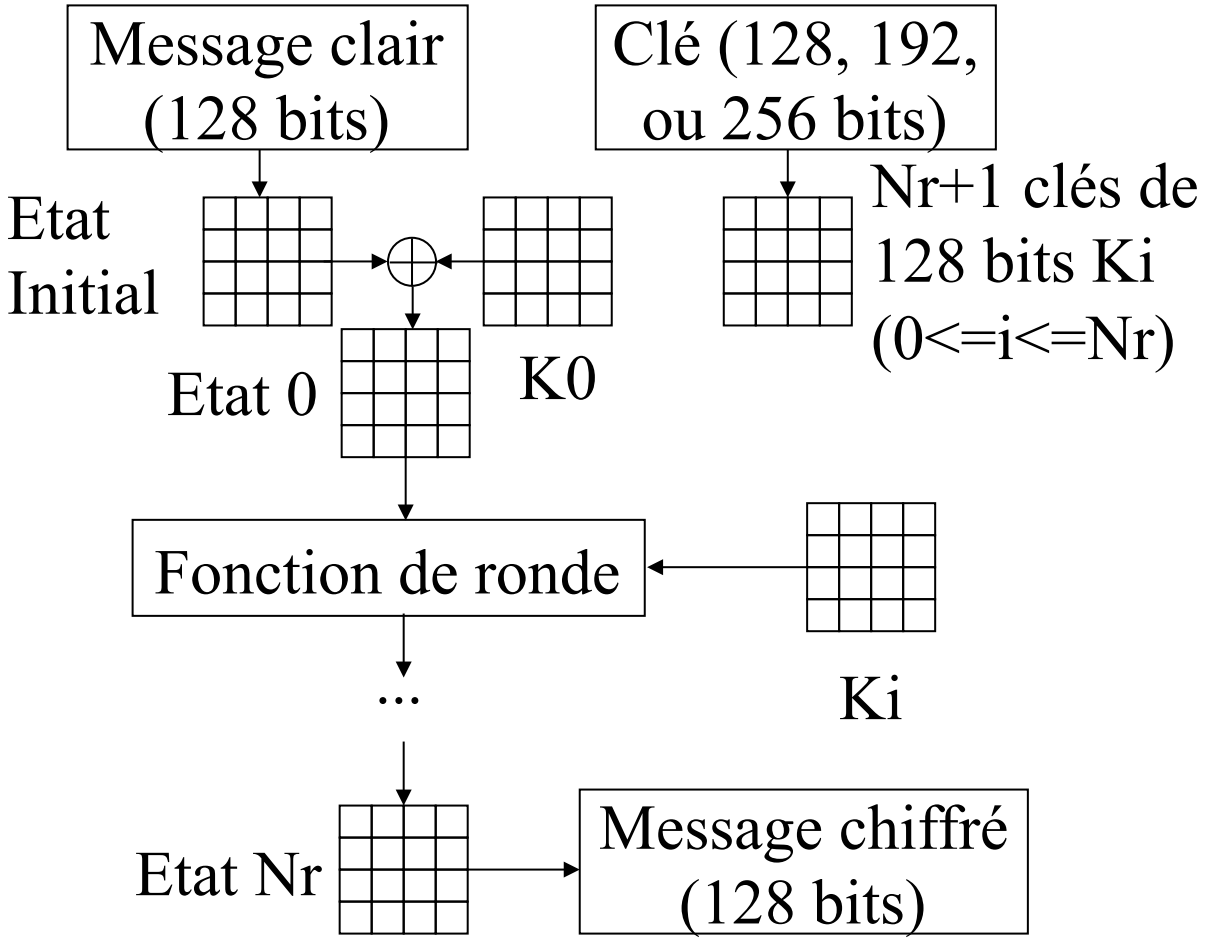
- Soit à effectuer $\{19\} \bullet \{3F\}$
- $\log_{\{03\}}(\{19\}) = 113$, $\log_{\{03\}}(\{3F\}) = 142$

  $\{19\} \bullet \{3F\} = \{03\}^{113} \bullet \{03\}^{142} = \{03\}^{255} = \{01\}$
- Soit à rechercher l'inverse de $\{19\}$
- Le $\log_{\{03\}}$ de l'inverse doit valoir 255-113=142
- On recherche $\{03\}^{142}$ dans la table (142 = 0x8E)
- L'inverse vaut $\{3F\}$

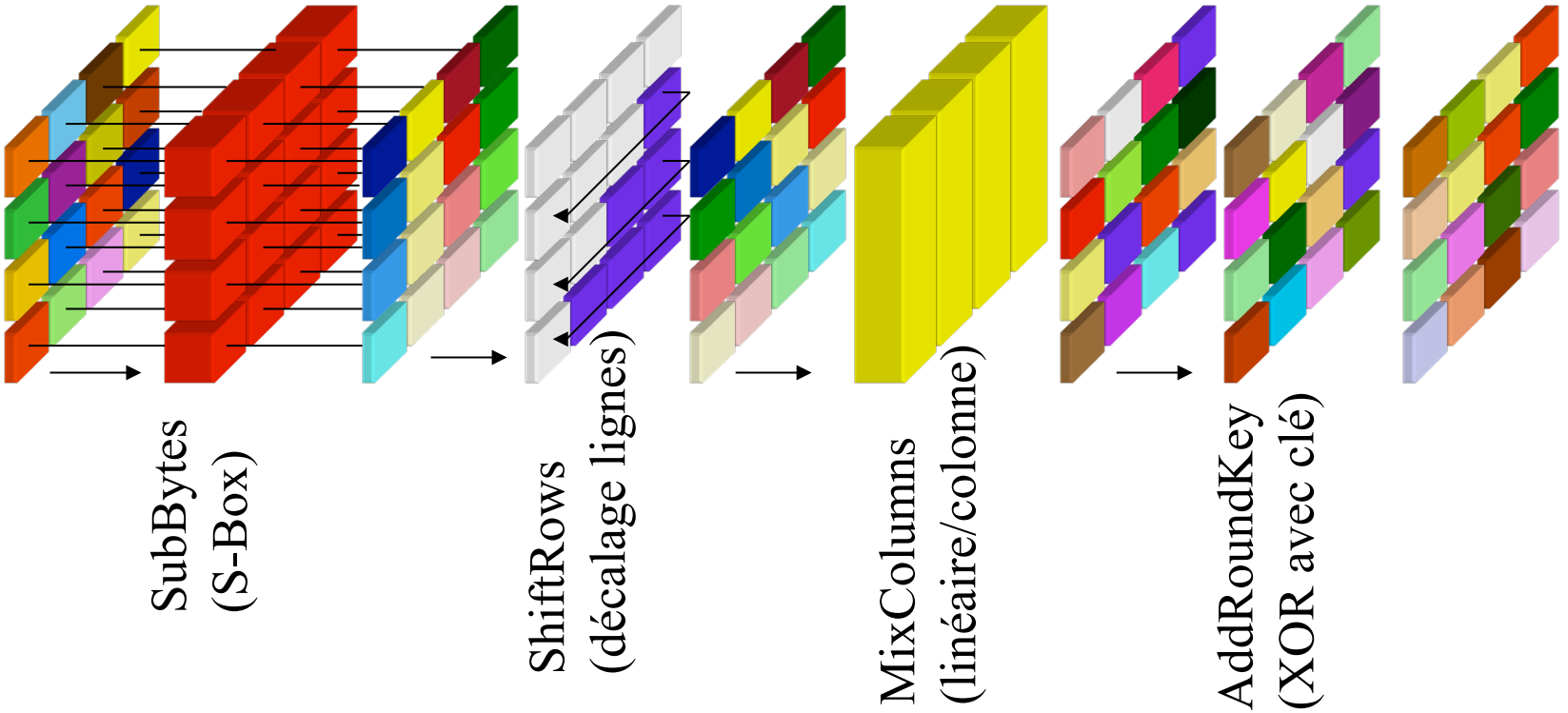
AES : Présentation de l'algorithme

- Nr Rondes

Clé	Nr
128 bits	10
192 bits	12
256 bits	14



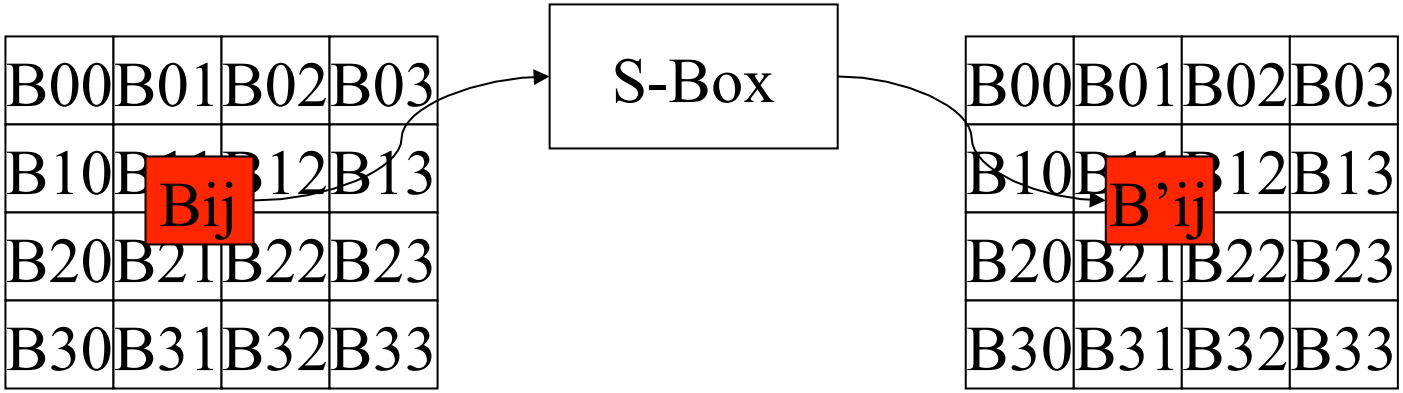
AES : Fonction de ronde



- Exception : la dernière ronde ne comporte pas de MixColumns

AES : SubBytes

- La transformation Subbytes opère sur la matrice d'états octet par octet en appliquant une S-Box :



- Prendre l'inverse multiplicatif (dans GF(2^8)) puis remplacer le bit i de l'octet par (c_i : bit i de {63}) :

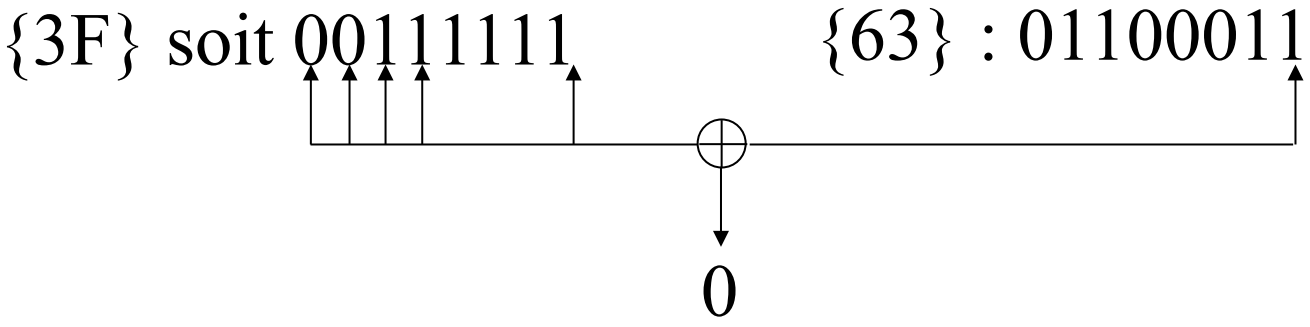
$$b_i' = b_i \oplus b_{(i+4)\bmod 8} \oplus b_{(i+5)\bmod 8} \oplus b_{(i+6)\bmod 8} \oplus b_{(i+7)\bmod 8} \oplus c_i$$

- Nota : pour l'octet 00 qui n'a pas d'inverse on substitue 00 et on applique la seconde étape : le substitué de 00 vaut donc 63

AES : SubBytes : Exemple

- Calcul du bit 0 de l'octet substitué à {19} :

  Inverse de {19} :



- Idem pour chaque bit : résultat {D4}
- Le résultat de la S-Box sur chaque octet de {00} à {FF} peut être précalculé et placé dans une table.

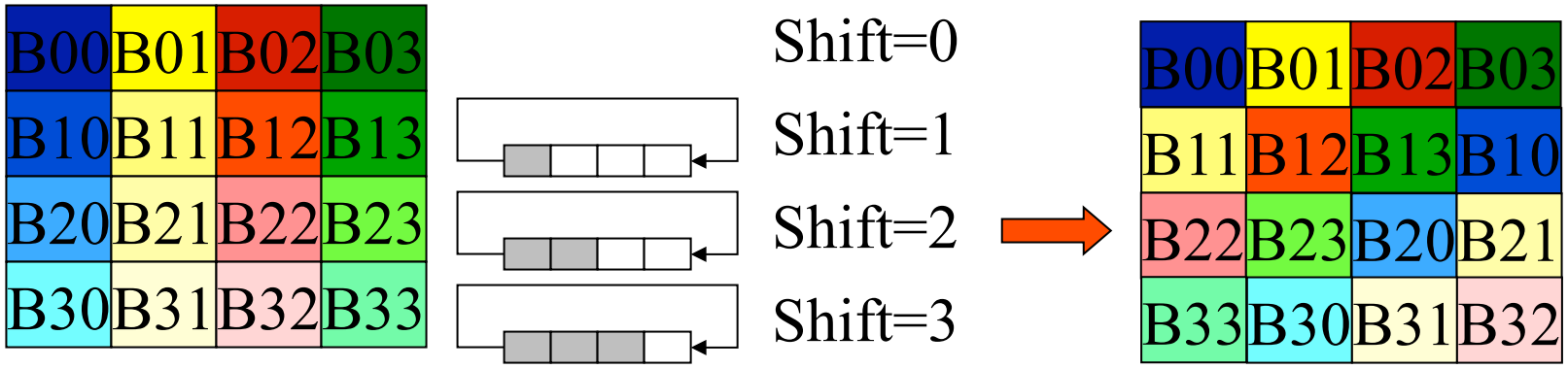
AES : SubBytes : La S-Box

- Transformée de l'octet {LC} :

	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

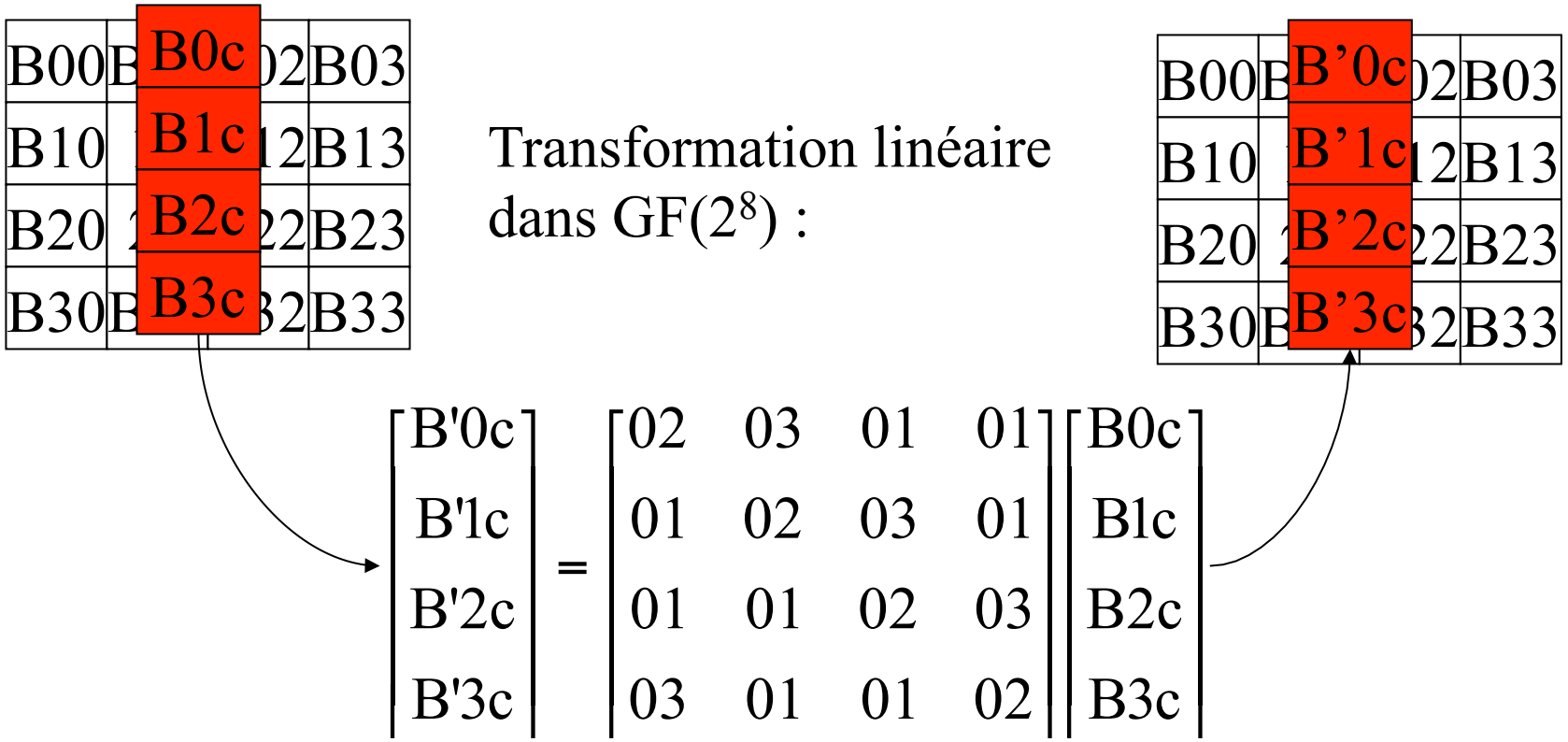
AES : ShiftRows

- La transformation ShiftRows opère sur la matrice d'états ligne à ligne en effectuant des shifts cycliques à gauche :



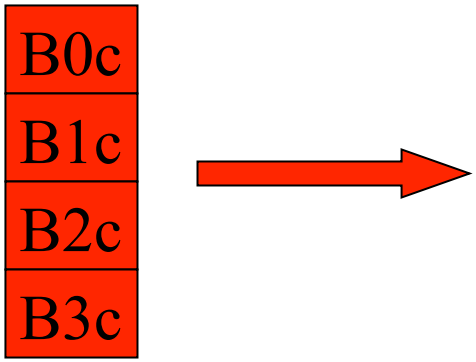
AES : MixColumns (1/3)

- MixColumns opère colonne par colonne :



AES : MixColumns (2/3)

- MixColumns peut également être décrite en considérant la colonne comme polynôme de degré 3 à coefficients dans GF(2^8) :



$$B3c.x^3 + B2c.x^2 + B1c.x + B0c$$

- MixColumns est alors équivalente à la multiplication modulo x^4+1 de ce polynôme par le polynôme :
  $a(x) = \{03\}.x^3 + \{01\}.x^2 + \{01\}.x + \{02\}$

AES : MixColumns (3/3)

- En effet, le terme de degré 0 du résultat est la somme des termes de degrés 0 et 4 du produit :

$$(B3c.x^3+B2c.x^2+B1c.x+B0c)\ (\{03\}.x^3+\{01\}.x^2+\{01\}.x+\{02\})$$

car l'élimination d'un terme $A.x^4$ par le modulo s'effectue en ajoutant $A.(x^4+1)$

D'où $B'0c = \{02\} \bullet B0c \oplus \{03\} \bullet B1c \oplus \{01\} \bullet B2c \oplus \{01\} \bullet B3c$

Idem pour les autres degrés. Ainsi l'inverse de MixColumns sera la multiplication par l'inverse modulo x^4+1 de a(x), s'il existe (x^4+1 non irréductible)

AES : MixColumns : Exemple

- La colonne à mixer est représentée par le polynôme $(\{30\}.x^3+ \{5D\}.x^2+ \{BF\}.x+ \{D4\})$
- $\log_{\{03\}}(\{D4\})=65$, $\log_{\{03\}}(\{02\})=25$ d'où :

$$\{02\} \bullet \{D4\} = \{03\}^{90} = \{B3\}$$

- $\log_{\{03\}}(\{BF\})=157$, $\log_{\{03\}}(\{03\})=1$ d'où :

$$\{03\} \bullet \{BF\} = \{03\}^{158} = \{DA\}$$

- Soit finalement :

$$B'0c = \{B3\} \oplus \{DA\} \oplus \{5D\} \oplus \{30\} = \{04\}$$

- Idem pour les autres éléments de la colonne

AES : AddRoundKey

- AddRoundKey est le simple XOR bit à bit de la matrice d'état avec une matrice de 4*4 Octets fabriquée à partir de la clé de chiffrement pour la ronde en cours.
- Si le nombre de rondes est Nr il faut donc Nr+1 telles matrices, l'algorithme commençant par une addition de clé initiale (Rappel : Nr dépend de la taille de la clé : 128, 192 ou 256)
- La fabrication de ces Nr+1 clés est l'algorithme d'expansion des clés décrit ci-après

AES : Expansion des clés (1/3)

- Manipule des mots de 32 bits.
- Clé de l'addition initiale : 4 (premiers) mots de la clé de chiffrement notés w[0] à w[3] rangés comme le message (en colonne du haut vers le bas).
- Selon la clé (128,192 ou 256), Nr = 10, 12 ou 14 => on doit obtenir au total 44, 52 ou 60 mots de 32 bits
- Clé de la ronde i : mots numérotés de w[4*i] à w[4*i+3] rangés dans une matrice de 4*4 octets suivant les même conventions

AES : Expansion des clés (2/3)

- La clé de chiffrement est constituée des Nk premiers mots (Nk=4, 6 ou 8 pour AES 128, 192 ou 256)
- En général pour i >= Nk $w[i] = w[i-1] \oplus w[i-Nk]$
- sauf si i est multiple de Nk où w[i-1] subit préalablement les opérations RotWord, SubWord et XOR avec une constante notée Rcon[i/Nk]
- Autre exception pour l'AES 256 seulement (Nk=8) : si i-4 est multiple de 8, w[i-1] subit un Subword (les opérations précédentes restant applicables si i est multiple de 8)

AES : Expansion des clés (3/3)

- Rotword : Shift cyclique gauche : Transforme un mot de 32 bits [B0,B1,B2,B3] en [B1,B2,B3,B0]
- Subword : Opère octet par octet en appliquant la même S-Box que SubBytes
- Rcon[i] est le mot de 32 bits représenté par $[x^{i-1},\{00\},\{00\},\{00\}]$
- Par exemple, pour Rcon[7] utilisé pour w[7Nk] l'octet représenté par x^6 est 01000000 soit {40} et Rcon[7]=40000000
- Si i-1>7, il faut faire un recalage modulo m(x)

AES : Expansion des clés : Exemple (1/2)

- En AES 128 si la clé vaut
  2B 7E 15 16 28 AE D2 A6 AB F7 15 88 09 CF 4F 3C

La clé utilisée pour l'addition initiale est :

2B	28	AB	09
7E	AE	F7	CF
15	D2	15	4F
16	A6	88	3C

- Les mots w[0] à w[3] sont ceux que l'on lit en colonnes de haut en bas et de gauche à droite

AES : Expansion des clés : Exemple (2/2)

- Pour fabriquer w[4] qui sera la première colonne de la clé de la première ronde, il faut appliquer RotWord, SubWord et XOR avec Rcon[1] sur 09CF4F3C puis faire un XOR du résultat avec 2B7E1516
- Après RotWord on a CF4F3C09
- Après SubWord on a 8A84EB01 (voir la S-Box)
- Rcon[1] vaut 01000000 donc après XOR avec Rcon[1] on a 8B84EB01
- Finalement

$$w[4] = 8B84EB01 \oplus 2B7E1516 = A0FAFE17$$

AES : Inversion

- Les opérations SubBytes, ShiftRows, MixColumns et AddRoundKey sont inversibles => il suffit de les appliquer dans l'ordre inverse
- SubBytes : il faut construire la S-Box inverse
- ShiftRows : l'inverse est obtenue par des shifts cyclique à droite
- AddRoundKey : est sa propre inverse
- Pour prouver l'inversibilité de MixColumns on montre que l'inverse modulo x^4+1 de $\{03\}x^3+\{01\}x^2+\{01\}x+\{02\}$ existe et vaut $\{0B\}x^3+\{0D\}x^2+\{09\}x+\{0E\}$