CHAPITRE 4.

A.E.S.

(Advanced Encryption Standard)

http://math.univ-lyon1.fr/~roblot/masterpro.html

Histoire. En 1997, le NIST annonce la création d'un nouveau protocole de cryptographie à clé secrète nommé A.E.S. et lance un appel d'offre. En 1998, quinze protocoles candidats sont retenus et soumis aux critiques de la communauté cryptographique. En octobre 2000, le NIST annonce le choix du protocole **Rijndael** créé par J. Daemen et V. Rijmen. Ce protocole remplace D.E.S. comme standard du NIST (norme FIPS 197).

Bloc. Codage par blocs de 128 bits.

Clé. Clé de 128 (10 rondes), 192 (12 rondes) ou 256 bits (14 rondes).

Spécificités. Grande résistance à toutes les attaques connues ; très grande rapidité pour le cryptage et le décryptage ; utilise des méthodes de substitution-permutation et non les diagrammes de Feistel (ou généralisations) ; possède une véritable structure mathématique.

Les quatre étapes d'une ronde

A.E.S. opère sur des matrices 4×4 dont les entrées sont des mots de 8 bits. On découpe le message clair en 16 blocs de 8 bits et on remplit en allant de haut en bas et de gauche à droite.

SubBytes : chaque entrée est remplacé par un autre mot de 8 bits donné par un tableau de correspondance ;

ShiftRows : Les entrées sont décalées suivant un décalage circulaire à gauche d'un nombre de cases dépendant de la ligne ;

MixColumns : Chaque colonne est remplacée par une nouvelle colonne obtenue en transformant la colonne en un polynôme et en multipliant par un polynôme fixé ;

AddRoundKey : Chaque entrée est remplacée par le *ou exclusif* entre cette entrée et l'entrée correspondante dans une matrice 4×4 construit à partir de la **clé**.

Extensions de $\mathbb{F}_2$

Le corps $\mathbb{F}_2$. L'ensemble $\mathbb{F}_2 = \{0, 1\}$ des entiers modulo 2 est un corps (la multiplication correspond à $\wedge$ et l'addition à $\oplus$).

Polynômes irréductibles. Un polynôme $P(X) \in \mathbb{F}_2[X]$ et de degré ≥ 1 est **irréductible** s'il n'existe pas deux polynômes $P_1(X), P_2(X) \in \mathbb{F}_2[X]$, de degré ≥ 1, et tels que $P(X) = P_1(X)P_2(X)$.
Pour tout $d \geq 1$, il existe des polynômes irréductibles de degré d.

Anneaux quotients. Pour $P(X) \in \mathbb{F}_2[X]$ de degré $d \geq 1$, le quotient $\mathbb{F}_2[X]/(P(X))$ est l'ensemble des polynômes de degré $< d$ avec l'addition usuelle et pour la multiplication, on fait la multiplication usuelle et on prend le reste modulo P.

Les extensions de $\mathbb{F}_2$. Pour $P(X) \in \mathbb{F}_2[X]$ de degré $d \geq 1$ et **irréductible**, l'ensemble $\mathbb{F}_2[X]/(P(X))$ est un corps, noté $\mathbb{F}_{2^d}$. Sa **structure** ne dépend pas du choix du polynôme P, mais juste du degré d.

Exercice sur les extensions de $\mathbb{F}_2$

1. Trouver un polynôme $P_1(X) \in \mathbb{F}_2[X]$ de degré 3 et irréductible.
2. Construire la table d'addition du corps $\mathbb{F}_2[X]/P_1(X)$.
3. Construire la table de multiplication du corps $\mathbb{F}_2[X]/P_1(X)$.
4. Trouver un autre polynôme $P_2(X) \in \mathbb{F}_2[X]$ de degré 3 et irréductible.
5. Construire la table d'addition du corps $\mathbb{F}_2[X]/P_2(X)$.
6. Construire la table de multiplication du corps $\mathbb{F}_2[X]/P_2(X)$.
7. Montrer que l'application $X \mod P_1 \mapsto X^2 + 1 \mod P_2$ est un isomorphisme entre les deux corps.

Le corps A.E.S.

Représentation. Mots de 8 bits correspondent à des mots de deux chiffres hexadécimaux et à des polynômes de $\mathbb{F}_2$ de degré ≤ 7.

Exemple. On identifie

$$\begin{aligned}\{9A\} &= 1001\,1010 \\ &= 1\cdot X^7+0\cdot X^6+0\cdot X^5+1\cdot X^4+1\cdot X^3+0\cdot X^2+1\cdot X+0\end{aligned}$$

Corps A.E.S.. On travaille dans le quotient $\mathbb{F}_2[X]/R(X)$ où $R(X)$ est le polynôme de Rinjdael (irréductible sur $\mathbb{F}_2$)

$$R(X)=X^8+X^4+X^3+X+1$$

Exemple.

$$\begin{aligned}\{2A\}+\{37\} &= (X^5+X^3+X)+(X^5+X^4+X^2+X+1) \\ &= X^4+X^3+X^2+1=\{1D\} \\ \{2A\}\times\{37\} &= X^6+X^5+X^4+X^2+X+1=\{77\}\end{aligned}$$

Exercice sur le corps A.E.S.

1. Montrer que l'addition correspond au "ou exclusif" sur les mots binaires.
2. Calculer la transformation sur un mot de 8 bits correspondant à la multiplication par $\{00\}$, $\{01\}$, $\{02\}$.
3. En déduire une méthode efficace pour multiplier deux éléments du corps A.E.S.
4. Calculer $\{2A\} \times \{37\}$ par cet algorithme.
5. Calculer $\{48\} \times \{3F\}$ par cet algorithme.

L'étape **SubBytes**

Description. La S-boîte de A.E.S. est une permutation sur l'ensemble des mots de 8 bits. Elle est construite en utilisant une fonction algébrique sur les éléments du corps A.E.S.

Construction. La transformation est donnée pour $\{x\}$ dans le corps A.E.S. par $\{00\} \mapsto \{63\}$, et pour $\{x\}$ non nul par

$$\{x\} \mapsto A(\{x\}^{-1}) + \{63\}$$

où A l'application linéaire définie par $A(\{x\}) = \{y\}$ avec

$$y_i = x_i \oplus x_{i+4 \bmod 8} \oplus x_{i+5 \bmod 8} \oplus x_{i+6 \bmod 8} \oplus x_{i+7 \bmod 8}$$

(bits lus de droite à gauche)

Exercice. Calculer l'image de $\{02\}$ par la S-boîte.

Remarque. C'est la seule étape non-linéaire du protocole A.E.S.

L'étape **SubBytes** (suite)

Notation. La permutation de **SubBytes** est donnée par la S-boîte ci-dessous.

	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

Exemple. $\{A8\}$ est transformé en $\{C2\}$

L'étape **ShiftRows**

Transformation. La première ligne est reste inchangée, la deuxième ligne est décalé d'une case vers la gauche, la troisième de deux cases vers la gauche et la quatrième de trois cases vers la gauche

$$\begin{pmatrix} a_{0,0} & a_{0,1} & a_{0,2} & a_{0,3} \\ a_{1,0} & a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,0} & a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,0} & a_{3,1} & a_{3,2} & a_{3,3} \end{pmatrix} \mapsto \begin{pmatrix} a_{0,0} & a_{0,1} & a_{0,2} & a_{0,3} \\ a_{1,1} & a_{1,2} & a_{1,3} & a_{1,0} \\ a_{2,2} & a_{2,3} & a_{2,0} & a_{2,1} \\ a_{3,3} & a_{3,0} & a_{3,1} & a_{3,2} \end{pmatrix}$$

Exercice. Montrer que

2A 64 D5 CA E4 4C AA ED 1F 35 5A 37 94 4E F0 84

devient

2A 4C 5A 84 E4 35 F0 CA 1F 4E D5 ED 94 64 AA 37

L'étape **MixColumns**

Identification. Une colonne est identifiée avec un polynôme de degré ≤ 3 à coefficients dans le corps AES. (Pour simplifier, on écrit nos colonnes en lignes !)

Transformation.

$$^t(a_0 \quad a_1 \quad a_2 \quad a_3) \mapsto \{a_0\} + \{a_1\}T + \{a_2\}T^2 + \{a_3\}T^3$$

On multiplie par $\{03\}T^3 + \{01\}T^2 + \{01\}T + \{02\}$ et on réduit modulo $\{01\}T^4 + \{01\}$:

$$\begin{aligned}(\{a_3\}T^3+\{a_2\}T^2+\{a_1\}T+\{a_0\})(\{03\}T^3+\{01\}T^2+\{01\}T+\{02\}) \\ = Q(X)\big(\{01\}T^4 + \{01\}\big) + \{a'_3\}T^3 + \{a'_2\}T^2 + \{a'_1\}T + \{a'_0\}\end{aligned}$$

Puis on retransforme en colonne :

$$\{a'_0\} + \{a'_1\}T + \{a'_2\}T^2 + \{a'_3\}T^3 \mapsto {}^t(a'_0 \quad a'_1 \quad a'_2 \quad a'_3)$$

Exercice sur l'étape **MixColumns**

Montrer que l'étape **MixColumns** revient à multiplier la colonne par la matrice suivante à coefficients dans le corps A.E.S.

$$\begin{pmatrix} \{02\} & \{03\} & \{01\} & \{01\} \\ \{01\} & \{02\} & \{03\} & \{01\} \\ \{01\} & \{01\} & \{02\} & \{03\} \\ \{03\} & \{01\} & \{01\} & \{02\} \end{pmatrix}$$

L'étape **AddRoundKey**

Construction des sous-clés. à chaque ronde, une matrice 4×4 à coefficients dans le corps A.E.S. est construite et est ajoutée à la matrice.

$$\begin{pmatrix} a_{0,0} & a_{0,1} & a_{0,2} & a_{0,3} \\ a_{1,0} & a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,0} & a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,0} & a_{3,1} & a_{3,2} & a_{3,3} \end{pmatrix} \oplus \begin{pmatrix} k_{0,0} & k_{0,1} & k_{0,2} & k_{0,3} \\ k_{1,0} & k_{1,1} & k_{1,2} & k_{1,3} \\ k_{2,0} & k_{2,1} & k_{2,2} & k_{2,3} \\ k_{3,0} & k_{3,1} & k_{3,2} & k_{3,3} \end{pmatrix}$$

$$\mapsto \begin{pmatrix} b_{0,0} & b_{0,1} & b_{0,2} & b_{0,3} \\ b_{1,0} & b_{1,1} & b_{1,2} & b_{1,3} \\ b_{2,0} & b_{2,1} & b_{2,2} & b_{2,3} \\ b_{3,0} & b_{3,1} & b_{3,2} & b_{3,3} \end{pmatrix}$$

Remarque. C'est la seule partie du protocole qui utilise la clé.

Construction des sous-clés

Transformations. On travaille sur des vecteurs de 4 mots de 8 bits. On utilise la S-boîte de **SubBytes**, fonction `SubWord` ; la fonction `RotWord` qui transforme (a_0, a_1, a_2, a_3) en (a_1, a_2, a_3, a_0) (utilisée par **ShiftRows**) et les constantes $\texttt{Rcst}_i = (X^{i-1}, 0, 0, 0)$

Exercice. Calculer $\texttt{Rcst}_i$ pour $i = 1, 2, 3, \ldots, 10$.

Expansion. On prend une matrice de 4 lignes et de colonnes égal au nombre de sous-clés à engendrer. On met la clé dans les colonnes C_i pour $i = 1, \ldots, N_k$ colonnes avec $N_k = 4$, 6 ou 8 (pour une clé de 128, 196 ou 256 bits). Puis, pour $i > N_k$, on fait $C_i = D_i \oplus C_{i-N_k}$ avec $D_i = C_{i-1}$ si N_k ne divise pas $i - 1$, et si N_k divise $i - 1$

$$D_i = \texttt{SubWord}(\texttt{RotWord}(C_{i-1})) \oplus \texttt{Rcst}_{(i-1)/N_k}$$

Exercice. Pour $N_k = 4$, calculer l'expression des colonnes C_i, $i = 5, ..., 12$, en fonction des colonnes C_1, C_2, C_3, C_4 et des $\texttt{Rcst}_i$.

Résultats de cryptanalyse contre A.E.S.

Depuis juin 2003, le gouvernement américain a annoncé que A.E.S. peut être utilisé pour crypter les informations classifiées :
« *La conception et la résistance des clés A.E.S. de différentes tailles (128, 192 ou 256 bits) sont suffisantes pour protéger les informations classées au niveau SECRET. Les informations classées au niveau TOP SECRET doivent utiliser des clés de longueur 192 ou 256 bits.* »

Recherche exhaustive. On essaie toutes les clés possibles. Pour les plus courtes, il faut en tester 2^{128}, soit environ $700\,000\,000\,000$ fois l'âge de l'univers pour un test de $1\,000\,000\,000$ clés par seconde. Pour les plus longues, il faut en tester 2^{256}, soit environ $2 \cdot 10^{50}$ fois l'âge de l'univers pour un test de $1\,000\,000\,000$ clés par seconde.

Autres attaques. Toutes les attaques efficaces contre A.E.S. sont des attaques contre de mauvaises implémentations logicielles ou matérielles. Il existe des attaques par relations quadratiques, mais qui sont infructueuses à l'heure actuelle.