Conception de Système Numérique

Modélisation VHDL de l'algorithme de déchiffrement AES

Table des matières

Table des figures

Liste des tableaux

1 Introduction - Chiffrement/Déchiffrement par bloc

Bob et Alice souhaitent garder secrète leur conversation vis-à-vis d'Eve jalouse. Ils décident donc de s'envoyer des messages chiffrés (cf. exemple de Table 1). Dans ce but, ils se basent sur la théorie de la cryptographie pour chiffrer/déchiffrer ces messages. Parmi les solutions existantes, ils choisissent un algorithme de chiffrement symétrique par bloc réputé mathématiquement inviolable : AES[1]. Dans le cas de l'AES, la taille des blocs de données est fixée à 16 octets soit 128 bits. La clé peut être néanmoins de taille 128 bits, 192 bits ou 256 bits.
L'objectif de ce projet est de développer en VHDL l'algorithme de déchiffrement AES avec une clé de 128 bits.

Table 1 – Message envoyé par Bob et reçu chiffré par Alice

Clé	2b 7e 15 16 28 ae d2 a6 ab f7 15 88 09 cf 4f 3c
Message	Resto en ville ?
Message en ASCII (Hexadecimal)	52 65 73 74 6f 20 65 6e 20 76 69 6c 6c 65 20 3f
Message chiffré (Hexadécimal)	d4 f1 25 f0 97 f7 ce e7 47 66 9b 78 30 56 ca a7
Message chiffré (ASCII)	Ôñ%ð÷ÎçGfx0VÊ§

2 Description de l'algorithme AES 128bits

L'algorithme AES se compose de 4 transformations élémentaires : AddRoundKey, SubBytes, ShiftRows et MixColumns détaillées dans la figure 1 pour le chiffrement ; AddRoundKey, InvSubBytes, InvShiftRows et InvMixColumns pour le déchiffrement. L'algorithme se déroule en 11 rondes : 1 ronde initiale suivie de 9 rondes exécutant les 4 fonctions et 1 dernière ronde ne comprenant pas l'appel à la fonction *MixColumns*. Le déchiffrement s'exécute dans l'ordre inverse de l'algorithme de chiffrement. Un bloc de données sur 16 octets (i.e. 128 bits) forme le message à chiffrer/déchiffrer en entrée de l'algorithme. Une clé ***secrète*** utilisée lors de la ronde initiale et dérivée ensuite dans les rondes suivantes constitue un paramètre de l'algorithme AES. Une fonction supplémentaire est nécessaire pour la génération des clés de ronde. Cette fonction est appelée *Key Expansion*.

Description des entrées / sorties
Dans le cadre de ce projet, vous développerez l'entité InvAES décrite dans la figure 2 pour déchiffrer les messages envoyés entre Bob et Alice selon l'algorithme de la figure 3.

L'entité comporte les entrées / sorties suivantes :
- Une entrée 'data_i' de 128 bits
- Une horloge 'clock_i'
- Un signal d'initialisation 'reset_i'
- Un signal 'start_i' indiquant la présence d'un message à chiffrer en entrée
- Une sortie 'data_o' sur 128 bits
- Un signal 'aes_on_o' indiquant que les calculs de déchiffrement sont en cours

Chronogramme du fonctionnement de l'entité InvAES
Le chronogramme de l'entité est donné dans la figure 4. Il n'inclut pas les contraintes de *timing* de l'horloge comme des relations entre signaux de commande et de donnée présents sur les bus. Les signaux évolueront de manière synchrone avec l'horloge.

1. Advanced Encryption Standard

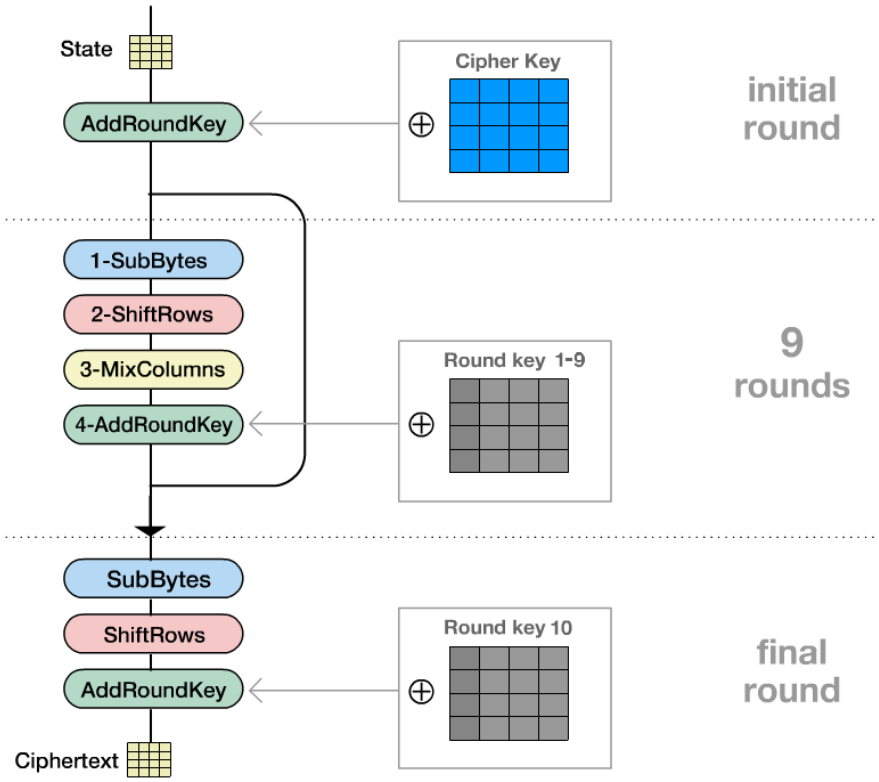

Figure 1 – Chiffrement AES 128bits

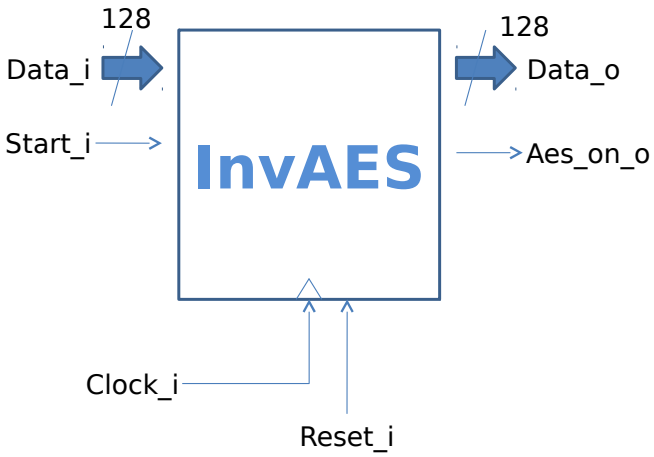

Figure 2 – Entrées / Sorties de l'entité InvAES

```
InvCipher(byte in[4*Nb], byte out[4*Nb], word w[Nb*(Nr+1)])
begin
   byte  state[4,Nb]

   state = in

   AddRoundKey(state, w[Nr*Nb, (Nr+1)*Nb-1])

   for round = Nr-1 step -1 downto 1
      InvShiftRows(state)
      InvSubBytes(state)
      AddRoundKey(state, w[round*Nb, (round+1)*Nb-1])
      InvMixColumns(state)
   end for

   InvShiftRows(state)
   InvSubBytes(state)
   AddRoundKey(state, w[0, Nb-1])

   out = state
end
```

Figure 3 – Algorithme de déchiffrement

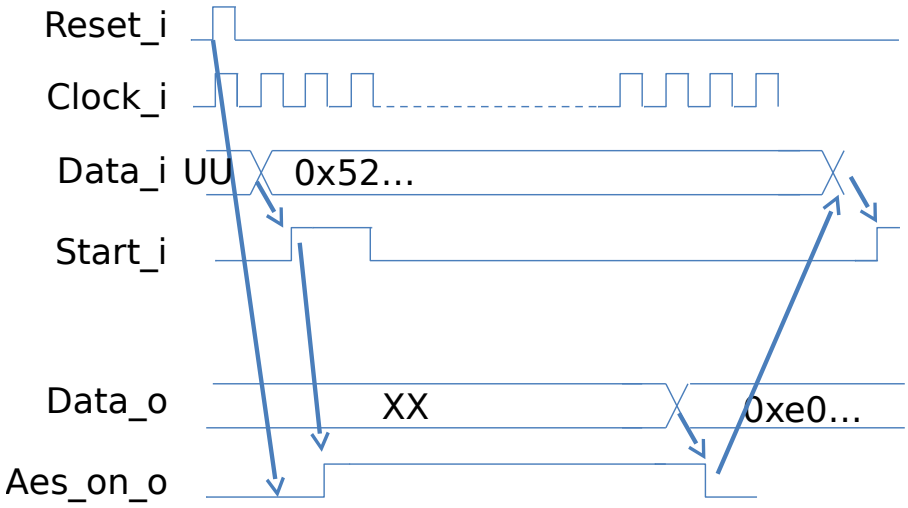

Figure 4 – Evolution des signaux de l'entité InvAES

2.1 Formalisme et notation

Pour être en adéquation avec la norme, vous utiliserez les notations suivantes :
— La numérotation des indices de la figure 5
— La représentation des octets (cf. figure 6)
— Un état peut également être considéré comme un tableau de colonnes, chaque colonne comprenant 4 octets soit un mot (word) de 32 bits (cf. figure 7)

Input bit sequence	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	...
Byte number	0								1								2								...
Bit numbers in byte	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	...

Figure 5 – Numérotation des vecteurs de bits

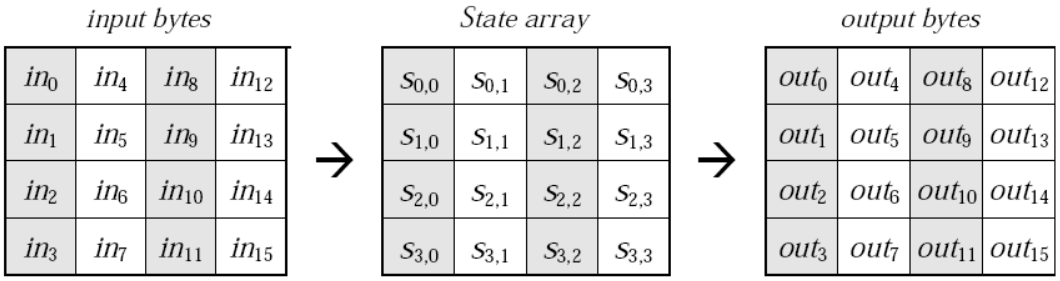

Figure 6 – Représentation de la matrice d'état de l'AES

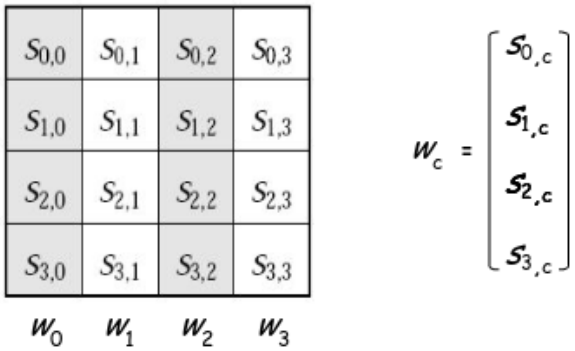

Figure 7 – Représentation d'une colonne de la matrice d'état

2.2 La transformation InvAddRoundKey

la fonction InvAddRoundKey ajoute la clef de ronde courante (Ronde 10 à Ronde 0) à l'état ; l'addition étant prise au sens ou-exclusif, elle est équivalente à la fonction AddRoundKey. Par conséquent, la fonction booléenne XOR est appliquée bit à bit entre les octets de l'état et les octets de la clef de ronde. La figure 8 montre l'application de la fonction. A noter que la clef de la ronde 0 est la clef de chiffrement alors que les clefs des rondes suivantes sont issues d'un processus de diversification des clefs dénommé 'Key Expansion'. Pour le projet, l'ensemble des clefs sera disponible à partir d'une mémoire adressable de $0x0$ à $0xA$ et compilé dans la librairie ***AESLibrary*** fournie.

2.3 La transformation InvShiftRows

La fonction InvShiftRows effectue une permutation cyclique (i.e. rotation) des octets des lignes de l'état. Le décalage des octets correspond à l'indice de la ligne considérée ($0 \leq r < 4$). Ainsi,

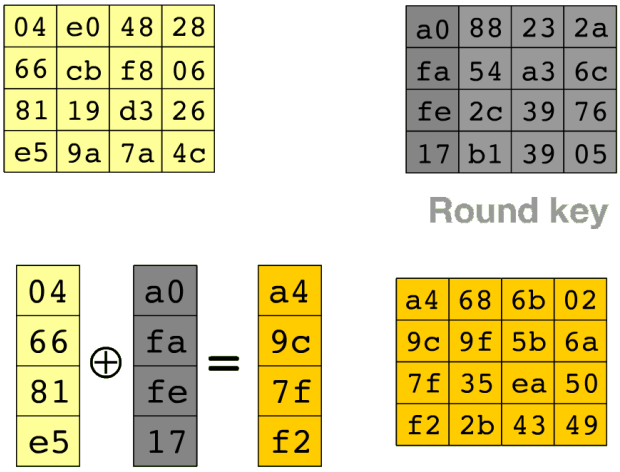

Figure 8 – Calcul de la fonction AddRoundKey

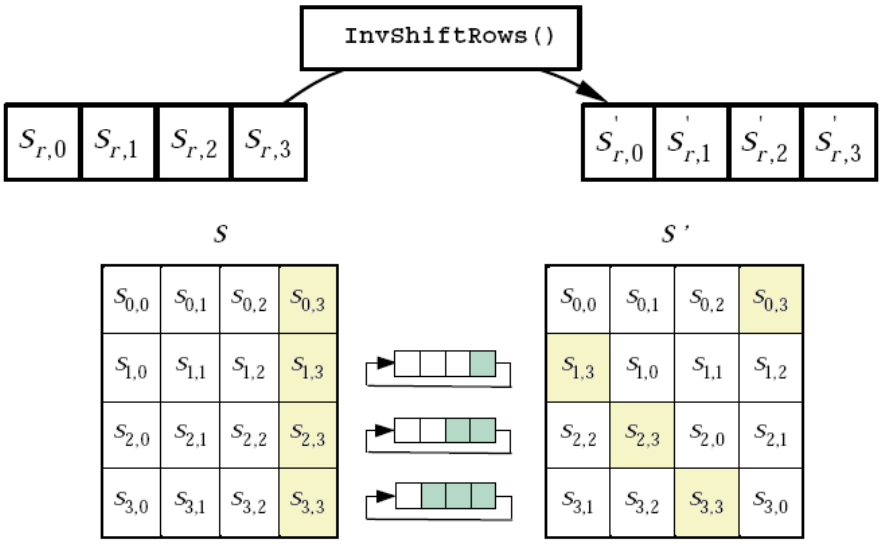

Figure 9 – Illustration de la fonction InvShiftRows

dans l'hypothèse ou $S_{1,x} = \{0x23, 0xeb, 0x5f, 0x99\}$, l'application de la fonction donnera $S'_{1,x} = \{0x99, 0x23, 0xeb, 0x5f\}$. Une illustration de la fonctionnalité est détaillée dans la Figure 9.

2.4 La transformation InvSubBytes

La fonction InvSubBytes consiste en une transformation non linéaire appliquée à tous les octets de l'état en utilisant une table de substitution appelée S-Box (cf. Figure 10). Vous implanterez la S-Box de la figure 11 sous la forme d'une mémoire (i.e. un tableau en VHDL) lors du développement de ce projet.
Pour exemple, soit $S_{2,1} = \{0xED\}$, l'application de la fonction InvSubBytes donnera l'écriture de $S'_{2,1} = \{0x53\}$ en sortie.

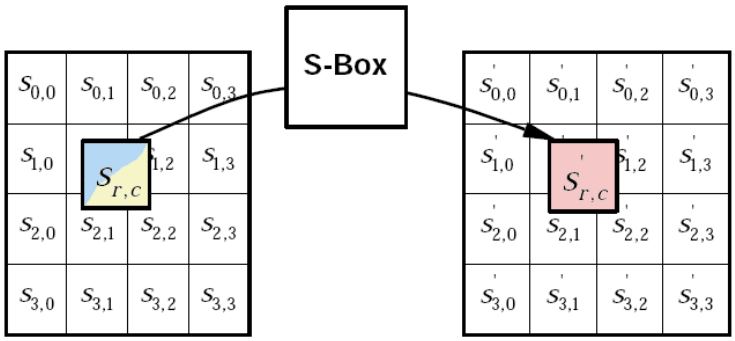

FIGURE 10 – Principe de la fonction InvSubBytes

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

x

FIGURE 11 – Table de substitution utilisé pour le projet

2.5 La transformation InvMixColumns

La fonction InvMixColumns applique une transformation colonne après colonne à un état. Cette transformation linéaire d'un produit matriciel utilisant les 4 octets d'une colonne (cf. Figure 12). Les colonnes sont traitées comme des polynômes dans $\mathrm{GF}(2^8)$ [2] et multipliées modulo x^4+1 (noté $\otimes$) avec les polynômes fixes de la Figure 12. Ces opérations réalisées dans le champs de Gallois sont calculées pour les additions à l'aide d'une fonction XOR.

$$\begin{bmatrix} s'_{0,c} \\ s'_{1,c} \\ s'_{2,c} \\ s'_{3,c} \end{bmatrix} = \begin{bmatrix} 0e & 0b & 0d & 09 \\ 09 & 0e & 0b & 0d \\ 0d & 09 & 0e & 0b \\ 0b & 0d & 09 & 0e \end{bmatrix} \begin{bmatrix} s_{0,c} \\ s_{1,c} \\ s_{2,c} \\ s_{3,c} \end{bmatrix}$$

$$s'_{0,c} = (\{0e\} \bullet s_{0,c}) \oplus (\{0b\} \bullet s_{1,c}) \oplus (\{0d\} \bullet s_{2,c}) \oplus (\{09\} \bullet s_{3,c})$$
$$s'_{1,c} = (\{09\} \bullet s_{0,c}) \oplus (\{0e\} \bullet s_{1,c}) \oplus (\{0b\} \bullet s_{2,c}) \oplus (\{0d\} \bullet s_{3,c})$$
$$s'_{2,c} = (\{0d\} \bullet s_{0,c}) \oplus (\{09\} \bullet s_{1,c}) \oplus (\{0e\} \bullet s_{2,c}) \oplus (\{0b\} \bullet s_{3,c})$$
$$s'_{3,c} = (\{0b\} \bullet s_{0,c}) \oplus (\{0d\} \bullet s_{1,c}) \oplus (\{09\} \bullet s_{2,c}) \oplus (\{0e\} \bullet s_{3,c})$$

FIGURE 12 – Produit matriciel de la fonction InvMixColumns

Illustrons la multiplication sur 2 exemples :

— Soit $S_{0,c} = 0xD4 = b'11010100$, $\{02\} \otimes S_{0,c}$ s'écrit sous la forme polynomiale :

$$(x^7 + x^6 + x^4 + x^2) \cdot x = x^8 + x^7 + x^5 + x^3$$

2. Galois Field ou champs de Galois de 2^8 = corps commutatif fini de cardinal 256

A la lecture de *Cryptography and Network Security* [1], la multiplication polynômiale par x peut être implanté à l'aide d'un décalage à gauche suivi d'un ou-exclusif avec la valeur b'100011011 conditionné par le bit de poids fort du polynôme. Ainsi nous écrivons l'opération telle que :

$$\begin{aligned}
\{02\} \otimes S_{0,c} &= (\{02\} \odot S_{0,c}) \ mod \ b'100011011 && (1)\\
&= shiftleft(b'11010100) \ xor \ b'100011011 \ (0xD4_7 = 1 \Rightarrow ou-exclusif) && (2)\\
&= b'110101000 \ xor \ b'100011011 && (3)\\
&= b'10110011 = 0xB3 && (4)
\end{aligned}$$

— Soit $S_{0,c} = 0x04 = b'00000100$, $\{02\} \otimes S_{0,c}$ s'écrit sous la forme polynomiale :
$$(x^2) \cdot x = x^3$$
idem, nous écrivons l'opération telle que :

$$\begin{aligned}
\{02\} \otimes S_{0,c} &= (\{02\} \cdot S_{0,c}) \ mod \ b'100011011 && (5)\\
&= shiftleft(b'00000100) && (6)\\
&= b'00001000 = 0x08 && (7)
\end{aligned}$$

Soit $W_2 = \{0x14, 0xE5, 0xFF, 0x00\}$, la sortie de la fonction InvMixColumns pour $S'_{0,2}$ sera :

$$\begin{aligned}
S'_{0,2} &= (\{0xE\} \otimes S_{0,2}) + (\{0xB\} \otimes S_{1,2}) + (\{0xD\} \otimes S_{2,2}) + (\{0x9\} \otimes S_{3,2}) && (8)\\
&= (\{b'1110\} \otimes S_{0,2}) \ xor \ (\{b'1011\} \otimes S_{1,2}) \ xor \ (\{b'1101\} \otimes S_{2,2}) \ xor \ (\{b'1001\} \otimes S_{3,2}) && (9)
\end{aligned}$$

Or

$$\begin{aligned}
(\{b'1001\} \otimes S_{3,2}) &= (\{b'1000 \ xor \ b'0001\} \otimes S_{3,2}) && (10)\\
&= (\{08\} \otimes S_{3,2} \ xor \ \{01\} \otimes S_{3,2}) && (11)\\
&= (\{2^3\} \otimes S_{3,2} \ xor \ S_{3,2}) && (12)\\
&= (\{02\} \otimes (\{02\} \otimes (\{02\} \otimes S_{3,2}))) \ xor \ S_{3,2}) && (13)\\
&= ..... && (14)
\end{aligned}$$

Par conséquent, le calcul successif des puissances de 2 des octets contenus dans la colonne permet d'effectuer toutes les opérations pour le calcul de la matrice inverse de la fonction MixColumns.
Avec $\oplus$ (i.e. xor) la fonction booléenne ou-exclusif définit selon :

XOR		
0	0	0
0	1	1
1	0	1
1	1	0

$X \oplus 0 = X$
$X \oplus 1 = not(X)$
$X \oplus X = 0$
$X \oplus not(X) = 1$
$X \oplus a \oplus X = a$

Figure 13 – Fonction Ou-exclusif

Notons également qu'une autre solution peut être implantée sous la forme de tables de substitution pré-calculées pour les multiplications par 0x9, 0xB, 0xD et 0xE.

2.6 Architecture globale de InvAES

L'architecture complète de l'InvAES est décrite dans la figure 14.
Elle contient :

— une machine d'états (ou Finite State Machine (FSM)) pilotant les signaux de contrôle de l'entité InvAES

— l'entité *KeyExpansion_ table* contenant toutes les clefs de rondes issues du standard NIST [2]
— un compteur *Counter* piloté par la FSM pour fixer l'adresse de la clef de ronde courante
— un composant *InvAESRound* intégrant les fonctions (AddRoundKey, InvShiftRows, InvSubBytes et InvMixColumns) pour le calcul d'une ronde
— un registre pour la sauvegarde du résultat du déchiffrement
— un multiplexeur pour choisir entre le message à déchiffrer en début de l'algorithme et le résultat intermédiaire issu du calcul d'une ronde

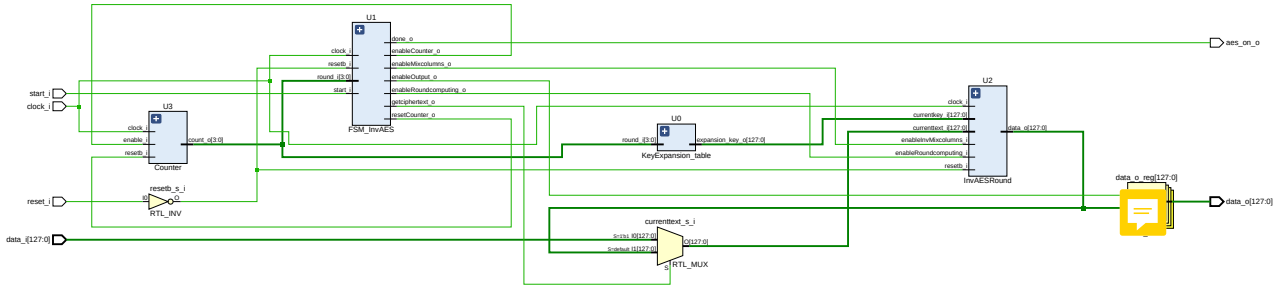

Figure 14 – Architecture globale de l'AES

3 Organisation du travail

3.1 Planning

Vous disposez de 5 séances pour modéliser l'entité InvAES en VHDL. Chacune des séances sera dédiée à la réalisation d'une composante de l'entité et sa validation. Il est par conséquent important de terminer cette composante avant le début de la séance suivante. Le découpage des séances est proposé comme suit :

1. Lecture et compréhension du sujet / Conception et test de la S-BOX pour la fonction InvSubBytes
2. Conception et test des modules *InvShiftRows* et *AddRoundKey*
3. Conception et test de la fonction *InvMixColumns*
4. Conception et test de la machine d'états (FSM) régissant le déchiffrement et du compteur
5. Suite de la conception de la FSM et intégration de tous les éléments dans l'entité InvAES (Top level) pour validation complète

Afin de coller à la réalité d'un projet industriel, le planning de la figure 15 décrit l'évolution que doit suivre votre travail. Ainsi un bilan d'avancement du projet en pourcentage sera demandé pour chacune des séances.

3.2 Contraintes de développement

Le projet sera développé à l'aide de l'outil Mentor Graphics ModelSim. Les fichiers de description VHDL (xxx.vhd) et de test (xxx_tb.vhd) seront enregistrés dans les répertoires nommés "sources" et "bench" respectivement. Les bibliothèques associées seront nommées "lib_sources " et "lib_bench" et créées dans un répertoire nommé "lib". Un script automatisant la compilation vous sera demandé.
De plus, et afin de disposer d'un code VHDL lisible, une attention toute particulière sera apportée à l'écriture du code. Ainsi certaines règles devront être respectées :

1. Une architecture associée à une entité doit se trouver dans le même fichier VHDL. Le nom du fichier correspond au nom de l'entité.
2. Le nom de l'architecture reprend le nom de l'entité complété du suffixe "_arch".
3. Pour les machines d'états précisez si le modèle d'architecture est Mealy ou Moore. Exemple : "FSM_arch_Moore".
4. Les signaux entrant d'une entité doivent être complétés par le suffixe "_i"

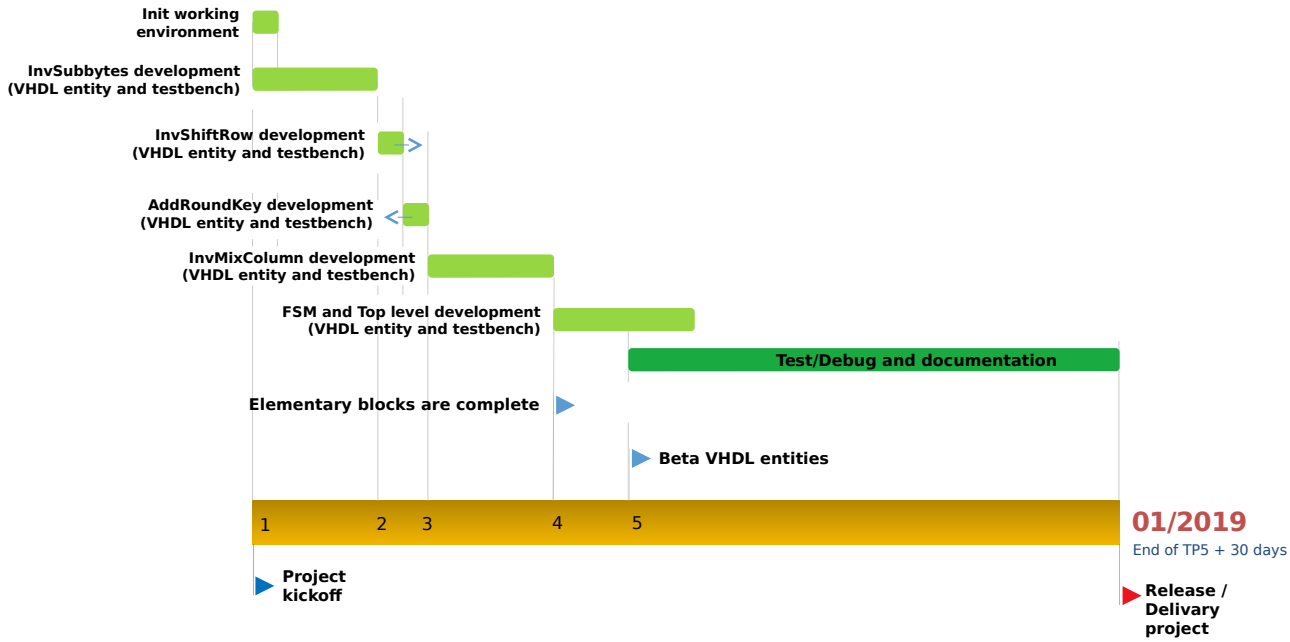

Figure 15 – Représentation Gantt du projet

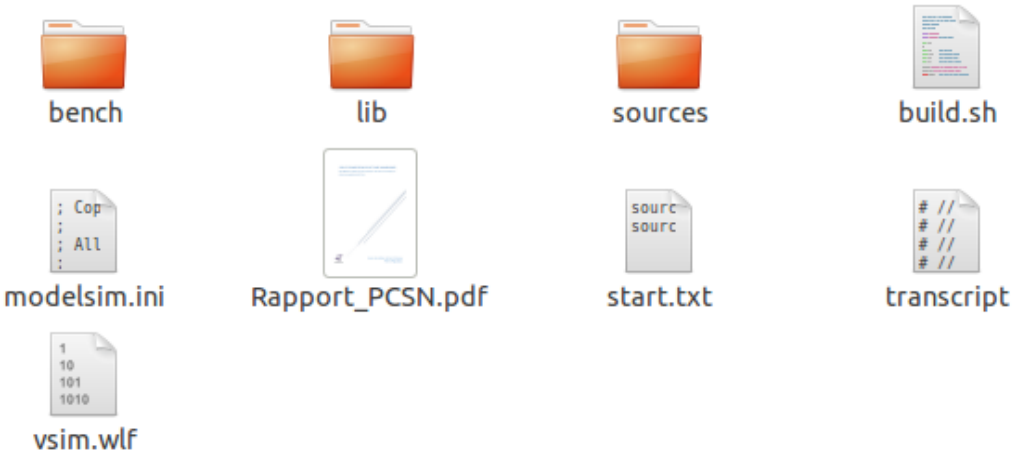

Figure 16 – Organisation des répertoires de travail

5. Les signaux sortant d'une entité doivent être complétés par le suffixe "_o"
6. Les signaux internes d'une architecture doivent être complétés par le suffixe "_s"
7. Les commentaires sont "obligatoires"

3.3 Validation du fonctionnement

A titre d'évaluation du bon fonctionnement de votre développement, les états intermédiaires après chaque étape de calcul de l'AES pour le chiffrement puis du déchiffrement du message "Resto ce soir ?" avec la clé "2b 7e 15 16 28 ae d2 a6 ab f7 15 88 09 cf 4f 3c" vous sont listés ci-dessous. Vous pourrez également vous aider de l'Appendix B de la norme FIPS [2]
avec le message chiffré $0x3925841d02dc09fbdc118597196a0b32$
donnant le message en clair $0x3243f6a8885a308d313198a2e0370734$.

```
Plain text : (Hex) 52 65 73 74 6f 20 65 6e 20 76 69 6c 6c 65 20 3f
(ASCII) Resto en ville ?
```

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

```
SubBytes : 36 ea ea ff 7e 2b 0f 22 29 e3 aa c0 bf 2d 43 b2
ShiftRows : 36 2b aa b2 7e e3 43 ff 29 2d ea 22 bf ea 0f c0
MixColumns : 09 37 9f a4 7e 99 01 c7 ed 74 ad f8 8f a1 10 a4
ComputeKey : ac 77 66 f3 19 fa dc 21 28 d1 29 41 57 5c 00 6e
AddRoundKey : a5 40 f9 57 67 63 dd e6 c5 a5 84 b9 d8 fd 10 ca
Round 10
SubBytes : 06 09 99 5b 85 fb c1 8e a6 06 5f 56 61 54 ca 74
ShiftRows : 06 fb 5f 74 85 06 ca 5b a6 54 99 8e 61 09 c1 56
ComputeKey : d0 14 f9 a8 c9 ee 25 89 e1 3f 0c c8 b6 63 0c a6
AddRoundKey : d6 ef a6 dc 4c e8 ef d2 47 6b 95 46 d7 6a cd f0
GetCiphertext : d6 ef a6 dc 4c e8 ef d2 47 6b 95 46 d7 6a cd f0
Cipher text at the end: (Hex) d6 ef a6 dc 4c e8 ef d2 47 6b 95 46 d7 6a cd f0
Cipher text to decipher: (Hex) d6 ef a6 dc 4c e8 ef d2 47 6b 95 46 d7 6a cd f0

SetCiphertext : d6 ef a6 dc 4c e8 ef d2 47 6b 95 46 d7 6a cd f0
InitKey : 2b 7e 15 16 28 ae d2 a6 ab f7 15 88 09 cf 4f 3c
KeyExpansion (round 0): 2b 7e 15 16 28 ae d2 a6 ab f7 15 88 09 cf 4f 3c
KeyExpansion (round 1): a0 fa fe 17 88 54 2c b1 23 a3 39 39 2a 6c 76 05
KeyExpansion (round 2): f2 c2 95 f2 7a 96 b9 43 59 35 80 7a 73 59 f6 7f
KeyExpansion (round 3): 3d 80 47 7d 47 16 fe 3e 1e 23 7e 44 6d 7a 88 3b
KeyExpansion (round 4): ef 44 a5 41 a8 52 5b 7f b6 71 25 3b db 0b ad 00
KeyExpansion (round 5): d4 d1 c6 f8 7c 83 9d 87 ca f2 b8 bc 11 f9 15 bc
KeyExpansion (round 6): 6d 88 a3 7a 11 0b 3e fd db f9 86 41 ca 00 93 fd
KeyExpansion (round 7): 4e 54 f7 0e 5f 5f c9 f3 84 a6 4f b2 4e a6 dc 4f
KeyExpansion (round 8): ea d2 73 21 b5 8d ba d2 31 2b f5 60 7f 8d 29 2f
KeyExpansion (round 9): ac 77 66 f3 19 fa dc 21 28 d1 29 41 57 5c 00 6e
KeyExpansion (round 10): d0 14 f9 a8 c9 ee 25 89 e1 3f 0c c8 b6 63 0c a6
Round 10
AddRoundKey : 06 fb 5f 74 85 06 ca 5b a6 54 99 8e 61 09 c1 56
Round 9
InvShiftRows : 06 09 99 5b 85 fb c1 8e a6 06 5f 56 61 54 ca 74
InvSubBytes : a5 40 f9 57 67 63 dd e6 c5 a5 84 b9 d8 fd 10 ca
AddRoundKey : 09 37 9f a4 7e 99 01 c7 ed 74 ad f8 8f a1 10 a4
InvMixColumns : 36 2b aa b2 7e e3 43 ff 29 2d ea 22 bf ea 0f c0
Round 8
InvShiftRows : 36 ea ea ff 7e 2b 0f 22 29 e3 aa c0 bf 2d 43 b2
InvSubBytes : 24 bb bb 7d 8a 0b fb 94 4c 4d 62 1f f4 fa 64 3e
AddRoundKey : ce 69 c8 5c 3f 86 41 46 7d 66 97 7f 8b 77 4d 11
InvMixColumns : 33 54 53 07 8c 07 95 a0 e4 d1 f3 35 8a 57 17 6a
Round 7
InvShiftRows : 33 57 f3 a0 8c 54 17 35 e4 07 53 6a 8a d1 95 07
InvSubBytes : 66 da 7e 47 f0 fd 87 d9 ae 38 50 58 cf 51 ad 38
AddRoundKey : 28 8e 89 49 af a2 4e 2a 2a 9e 1f ea 81 f7 71 77
InvMixColumns : b6 ca db c1 10 7b 23 21 f2 33 45 c5 5d 0b 4d 6b
Round 6
InvShiftRows : b6 0b 45 21 10 ca 4d c5 f2 7b db 6b 5d 33 23 c1
InvSubBytes : 79 9e 68 7b 7c 10 65 07 04 03 9f 05 8d 66 32 dd
AddRoundKey : 14 16 cb 01 6d 1b 5b fa df fa 19 44 47 66 a1 20
InvMixColumns : 93 39 c7 a5 6c 07 ef 53 35 7c 03 32 67 27 da 3a
Round 5
InvShiftRows : 93 27 03 53 6c 39 da 32 35 07 c7 3a 67 7c ef a5
InvSubBytes : 22 3d d5 50 b8 5b 7a a1 d9 38 31 a2 0a 01 61 29
AddRoundKey : f6 ec 13 a8 c4 d8 e7 26 13 ca 89 1e 1b f8 74 95
```

```
InvMixColumns : a5 dc 19 c1 1f 1c 9d 43 ec 39 ea 71 73 46 18 2f
Round 4
InvShiftRows : a5 46 ea 43 1f dc 18 71 ec 1c 19 2f 73 39 9d c1
InvSubBytes : 29 98 bb 64 cb 93 34 2c 83 c4 8e 4e 8f 5b 75 dd
AddRoundKey : c6 dc 1e 25 63 c1 6f 53 35 b5 ab 75 54 50 d8 dd
InvMixColumns : 8d b8 17 03 0e fa 25 4f f8 3c da 40 53 50 dd df
Round 3
InvShiftRows : 8d 50 da 4f 0e b8 dd 40 f8 fa 17 df 53 3c 25 03
InvSubBytes : b4 6c 7a 92 d7 9a c9 72 e1 14 87 ef 50 6d c2 d5
AddRoundKey : 89 ec 3d ef 90 8c 37 4c ff 37 f9 ab 3d 17 4a ee
InvMixColumns : dd 21 1c 57 70 be 19 b0 4a d0 63 63 3c f6 4c 08
Round 2
InvShiftRows : dd f6 63 b0 70 21 4c 63 4a be 1c 08 3c d0 19 57
InvSubBytes : c9 d6 00 fc d0 7b 5d 00 5c 5a c4 bf 6d 60 8e da
AddRoundKey : 3b 14 95 0e aa ed e4 43 05 6f 44 c5 1e 39 78 a5
InvMixColumns : 88 06 55 6f a6 d0 33 a5 3c 55 b0 32 b8 96 31 e5
Round 1
InvShiftRows : 88 96 b0 a5 a6 06 31 32 3c d0 55 e5 b8 55 33 6f
InvSubBytes : 97 35 fc 29 c5 a5 2e a1 6d 60 ed 2a 9a ed 66 06
AddRoundKey : 37 cf 02 3e 4d f1 02 10 4e c3 d4 13 b0 81 10 03
InvMixColumns : b6 19 10 7b a0 0c a8 aa 3d ac 33 e8 4d af a9 69
Round 0
InvShiftRows : b6 af 33 aa a0 19 a9 e8 3d 0c 10 69 4d ac a8 7b
InvSubBytes : 79 1b 66 62 47 8e b7 c8 8b 81 7c e4 65 aa 6f 03
AddRoundKey : 52 65 73 74 6f 20 65 6e 20 76 69 6c 6c 65 20 3f
Getplaintext : 52 65 73 74 6f 20 65 6e 20 76 69 6c 6c 65 20 3f
Obtained plain text : (Hex) 52 65 73 74 6f 20 65 6e 20 76 69 6c 6c 65 20 3f
(ASCII) Resto en ville ?
```

La simulation de InvAES pour le déchiffrement du message de Bob ainsi que la réponse d'Alice (à trouver) est donnée dans la figure 17 ci-dessous.

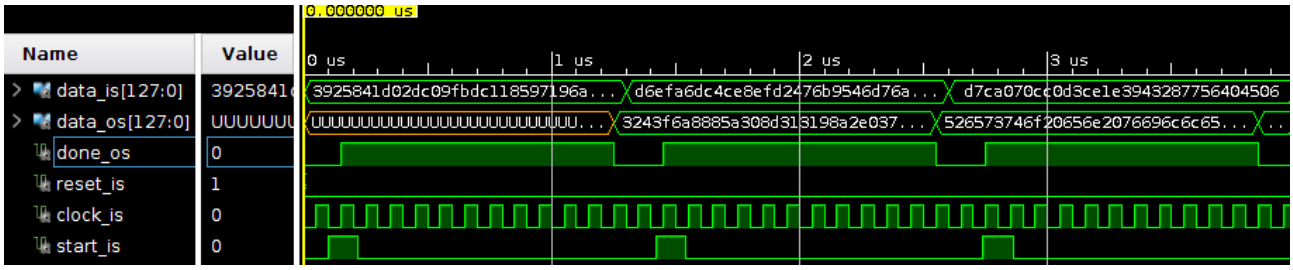

Figure 17 – Simulation de trois déchiffrements

3.4 Livrables

La note sera composée du PV de réception du projet complet. Le PV de réception sera validé après l'envoi par l'élève d'un fichier compressé (.zip ou .tar) à la date prévue par le Gantt. Il sera constitué :

1. Un rapport au format pdf contenant la description de votre entité InvAES et le chronogramme résultant de sa simulation
2. La description de la machine d'états gérant le déchiffrement
3. Les chronogrammes (et leur interprétation) issus de la simulation des éléments constituant InvAES
4. La description des points bloquant et les solutions envisagées

5. Les codes VHDL répartis dans les répertoires "sources" et "bench"
6. Le script de compilation de ces codes VHDL

La notation sera réalisée selon le barème suivant :

Correction PCSN (ISMIN_EI17)		Modules						Règles d'écritures	Consignes VHDL		Rapport		
		InvSubBytes	InvShiftRows	AddRoundkey	InvMixColumn	InvAES_FSM	Top		Script	Organisation	Contenu	Orthographe	
Nom	Prénom	1 pts	1 pts	1 pts	3 pts	3 pts	2 pts	5 pts	1 pts	3 pts	7 pts	3 pts	Note / 30

Figure 18 – Notation du projet PCSN

Note 1 : Toute ressemblance avec un projet existant ou copié sur un autre élève sera sanctionnée d'un 0/20

Note 2 : Il n'y a pas de rattrapage pour cette UP

Références

[1] W. Stallings, *Cryptography and Network Security : Principles and Practice.* Upper Saddle River, NJ, USA : Prentice Hall Press, 5th ed., 2010.

[2] NIST, "Fips-197, announcing the advanced encryption standard (aes),"