Advanced Encryption Standard (AES)

1. Efectes de les funcions elementals:

   (a) Canviem la funció **ByteSub** per la identitat, i.e. **ByteSub(x)=x**.

   Sigui M_i igual a M excepte en el bit i; M_j igual a M excepte en el bit j; M_{ij} és igual a M excepte en els bits i, j; C_i el resultat de xifrar M_i amb la clau K; C_j el resultat de xifrar M_j amb la clau K; C_{ij} el resultat de xifrar M_{ij} amb la clau K:

   $M=$
15	33	7e	b3
97	1c	6d	ea
c4	c2	1b	3b
ef	8b	2e	95

   $M_i=$
15	33	7e	b3
97	1c	6d	ea
c4	**82**	1b	3b
ef	8b	2e	95

   $M_j=$
15	33	7e	**93**
97	1c	6d	ea
c4	c2	1b	3b
ef	8b	2e	95

   $M_{ij}=$
15	33	7e	**93**
97	1c	6d	ea
c4	**82**	1b	3b
ef	8b	2e	95

   $C=$
ae	99	2e	5c
29	c0	ab	16
8d	74	01	a2
91	19	99	2e

   $C_i=$
ae	99	**6e**	5c
29	**00**	ab	16
0d	74	01	a2
91	19	99	**6e**

   $C_j=$
ae	99	2e	**5a**
29	c0	**a3**	16
8d	**7f**	01	a2
9e	19	99	26

   $C_{ij}=$
ae	99	**6e**	**5a**
29	**00**	**a3**	16
0d	**7f**	01	a2
9e	19	99	**6e**

   Feu un programa per comprobar que $C = C_i \oplus C_j \oplus C_{ij}$ per qualsevol i, j, i que això no pasa si agafen la funció **ByteSub** original.

   $C=$
2a	9a	7c	9c
56	9f	36	76
e1	34	6e	ec
4e	63	c8	60

   $C_i=$
67	84	1b	ac
22	43	bd	e7
73	52	ed	5c
82	ff	1d	b3

   $C_j=$
0e	95	9c	0d
ee	98	3f	f2
81	0a	b5	e2
2e	13	59	d4

   $C_{ij}=$
55	d1	61	74
ef	62	72	0e
bb	e1	ea	9d
d5	d0	b7	ea

   Noteu que si $M = 0$, llavors M_i és el missatge que té tot de 0's excepte un 1 a la posició i i si sabem el valor de C, C_i i C_j llavors podem calcular fàcilment C_{ij} correponent al missatge que té tot de 0's excepte a les posicions i i j.

   Doneu una forma senzilla de calcular el criptograma correponent al missatge que té tot de 0's excepte a les posicions i, j, k i l.

   (b) Canviem la funció **ShiftRows** per la identitat. Quins efectes té aquest canvi al xifrar un bloc? (Xifreu diferents M i els corresponents M_i amb la mateixa clau K i compareu C amb C_i.)

   (c) Canviem la funció **MixColumns** per la identitat. Quins efectes té aquest canvi al xifrar un bloc? (Xifreu diferents M i els corresponents M_i amb la mateixa clau K i compareu C amb C_i.)

2. Propagació de canvis: Amb un missatge M de 128 bits i una clau K de 128 bits qualssevol feu una estadística dels bits que canvien a la sortida quan modifiqueu un bit de M:

   (a) histograma del nombre total de bits que canvien amb cada modificació,

   (b) histograma de les posicions que canvien amb cada modificació.

   Feu el mateix si modifiqueu un bit de K.

Referències

Federal Information Processing Standards Publication (FIPS) 197: Advanced Encryption Standard (AES)
http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf