Année : 2023/2024

Université Abdalhafid Boussouf Mila
Institut de Mathématiques et Informatique
3ème Année informatique
Module: Sécurité informatique

Série TD N° 05

Exercice 01 :

Soit le texte clair (représenté en Héxadécimal) :

$$i = 3243f6a8885a308d313198a2e0370734$$

Et la clé (représentée en Héxadécimal) :

$$k = 2b7e151628aed2a6abf7158809cf4f3c$$

- Selon l'algorithme AES-128 :
  1. Donnez les tables d'états du message (texte clair) « i » et de la clé « k ».
  2. Donnez la table d'état courant obtenue après l'application de chacune de ces étapes :
     a) L'addition initiale $i \oplus k$ définie par l'opération AddRoundKey.
     b) L'opération « SubByte » appliquée sur le résultat de l'addition $i \oplus k$.
     c) L'opération « ShiftRow » appliquée sur le résultat de l'opération « SubByte ».
  3. Donnez le résultat de l'application de l'opération MixColumn sur la colonne suivante :

$$\begin{bmatrix} d4 \\ bf \\ 5d \\ 30 \end{bmatrix}$$

Exercice 02 :

1. L'utilisateur A choisit les facteurs premiers p = 3 et q = 11.
   - Déterminez une clé privée et une clé publique du cryptosystème RSA utilisant p et q.
2. Les utilisateurs A et B décident d'un protocole RSA dans lequel les lettres d'un message sont codées par leur position dans l'alphabet (en base 10), et le message est découpé en blocs de 2 chiffres (en base 10). B veut envoyer le message « CALCUL ».
   - Donnez le message chiffré que B envoie à A.
   - Donnez le message déchiffré par A, du message reçu de B, et vérifiez qu'il correspond bien à celui envoyé par B.
3. Si on découpe le message en blocs de 3 chiffres (en base 10).
   - Donnez le message chiffré que B envoie à A.
   - Donnez le message déchiffré par A, du message reçu de B, et vérifiez qu'il correspond bien à celui envoyé par B.

Exercice 03 :

Soit l'utilisateur A qui possède la clé privée (3, 55) et la clé publique (27, 55) RSA.
Soit l'utilisateur B qui possède la clé privée (7, 187) et la clé publique (23, 187) RSA.

1. Pour assurer la confidentialité de ses messages, l'utilisateur A chiffre le message m = 2 avec la clé RSA de B. Donnez le message chiffré.
2. Pour assurer l'authenticité de ses messages, l'utilisateur A signe le message m en utilisant la signature RSA et chiffre le résultat avec la clé RSA de B. Donnez le message signé et chiffré c.
3. L'utilisateur B reçoit le message c. Vérifiez la signature.

S-Box

		y															
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
x	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