SECURITE INFORMATIQUE - Fiche TD N°3
Symétrique par Bloc (DES)/Asymétrique (RSA) et applications (FH,DS, DHKX)

10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

IP							
58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

IP^{-1}							
40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

Exc 01 Une propriété importante qui renforce la sécurité du DES est la non-linéarité des Sboxes. Montrer que $S_3(x_1) \oplus S_3(x_2)$!= $S_3(x_1 \oplus x_2)$, pour : cas1. $x_1 = 000000$, $x_2 = 000001$, cas2. $x_1 = 111111$, $x_2 = 100000$, cas3. $x_1 = 101010$, $x_2 = 010101$ (S_3 donné dans la figure)

Exc 02 Afin de vérifier que IP(·) et $IP^{-1}(\cdot)$ sont deux opérations inversées, on considère un vecteur $x = (x_1,x_2, \ldots ,x_{64})$ de 64 bit. Montrer que $IP^{-1}(IP(x)) = x$ pour les cinq premiers bits de x (i = 1,2,3,4, 5) (IP et IP^{-1} données dans la figure)

Exc 03 Quelle est la sortie de la première itération (round) du DES lorsque les bits du texte clair et la clé sont tous des 0? Même questions pour bits tous 1? (supposant que l'expansion ne change pas les valeurs des bits juste les duplique)

***Exc 04** Soit PC(K) = 1101 0011 1010 1100 0010 1100 0111 0110 1010 1010 0111 1000 1001 1101 = D3AC2C76AA789D, Calculer sous clé K1

***Exc 05** [Examen 2015 UHBC] On dit qu'une fonction f involutive ssi f(f(x))=x. On dit que la clé K de DES est faible si DES avec cette clé K est involutive.
1- Décrire la relation entre les sous clés pour un DES involutive?
2- Il y a 4 clés faibles lesquelles?

Exc 06. Dites combien de clés on a besoin pour un groupe de **n** personnes qui veulent établir une communication sécurisée en utilisant une méthode : 1- **Symétrique**. 2- **Asymétrique**.

Exc 07. Soit deux nombres premiers p=41 et q=17 donnés comme paramètres du RSA.
1- Lequel des deux paramètres e1= 32, e2=49 est un exposant RSA valide? Justifier
2- Calculer la clé privée correspondante (utiliser EE algorithme pour trouver l'inverse)

Exc 08. Pour les messages suivants en utilisant les paramètres RSA correspondants :
1- Crypter : : x=2, e=79, n=101, (* x=3, e=197, n=101)
2- Décrypter : p=3, q=11, d=7, x=5, (* p=3, q=11, e=3, x=9)

***Exc 09**. Dans un système RSA, texte crypté c = 10 dont la clé publique (e,n) = (5,35).
1- Trouver le texte clair? Quelle conclusion faite vous de cette méthode?

Exc 10. Décrypter et crypter les messages suivants en utilisant RSA avec p=29, q=37, M='HELLO'. On va prendre le code ASCII de chaque caractère et on les met bout à bout H 72 E 69 L 76 O 79 (Découper le message en blocs qui comportent moins de chiffres que n)

Exc 11. En donnant un schéma DS avec RSA dont $K_{pb}(n = 9797,e = 131)$ quelle DS est valide?
1. (x = 123, sig(x) = 6292) 2. (x = 4333, sig(x) = 4768) 3. (x = 4333, sig(x) = 1424)

Exc 12. Calculer 2 clés publiques et la clé partagée pour **DHKE** avec p = 467, α = 2,
1. a = 3, b = 5 2. a = 400, b = 134 3. a = 228, b = 57.