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 1. x1 = 000000, x2 = 000001 2. x1 = 111111, x2 = 100000 3. x1 = 101010, x2 = 010101
S1(x1)=00000 S1(x2) =000000 S1(x1) + S1(x2)= 0000000 (1)
X1 + x2 = 000000 S1(x1 + x2)=0000000 (2) on (1)!= (2) non lineare

Exc 02 IP(X)=IP($x_1x_2...x_{64}$)=$x_{58}x_{50}x_{42}...x_7$ = Y= $y_1y_2...y_{64}$ on a $y_1=x_{58}$ $y_2=x_{50}$ $y_{40}=x_1...y_{25}=x_{64}$
IP-1(Y) =IP-1($y_1y_2...y_{64}$)=$y_{40}y_8y_{48}...y_{25}$= $x_1x_2...x_{64}$=X

Exc 03 cas des 0 :
K=0^{56} , K1 = PC1(ROT1(PC(0^{56}))) = 0^{48} parceque toute les operations ne changent pas les bits.
B=0^{64} => DES(B)=IP-1(R16(..(R1(IP(B)))..))
On IP*(0^{64}) = 0^{64} la permutation ne modifie pas les bits juste change leurs places
R1(0^{64})= R(0^{32} , 0^{32}) = (0^{32} , 0^{32} + f(0^{32}, 0^{48})) =(0^{32} , 0^{32} + P(S(E(0^{32})+ 0^{48}))))
=(0^{32} , 0^{32} + P(S(0^{48}))) = (0^{32} , 0^{32} + P(S(0^{48}))) =(0^{32} , P($(14)^8$))= (0^{32} , $(1110)^8$)= $0^{32}(1110)^8$

Exc 06. 1- **Symétrique**. n(n-1)/2, 2- **Asymétrique**.: 2n

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

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

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 (solution trouvée dans presentation cours)

Exc 11. En donnant un schéma DS avec RSA dont K_{pb}(n = 9797,e = 131) quelle DS est valide?
Un calcul 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,
Un calcul 1. a = 3, b = 5 2. a = 400, b = 134 3. a = 228, b = 57.