Network Security

Homework 2

CHANG LIU

chang.liu@jhu.edu

Feb. 29, 2012

1.

1	5	9	13	17	21	25	29
0000	**0001**	**0010**	**0011**	**0100**	**0101**	**0110**	**0111**
33	37	41	45	49	53	57	61
1000	**1001**	**1010**	**1011**	**1100**	**1101**	**1110**	**1111**

(a) Derive the first round key K1.

PC-1

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

1111000
0110011
0010101
0100000

1010101
0110011
0011110
0000000

Thus,

L = 1111 0000 1100 1100 1010 1010 0000

R = 1010 1010 1100 1100 1111 0000 0000

Rotations

Round number	Number of left rotations
1	1
2	1
3	2
4	2
5	2
6	2
7	2
8	2
9	1
10	2
11	2
12	2
13	2
14	2
15	2
16	1

⇨ C_1(L) = 1110 0001 1001 1001 0101 0100 0001

⇨ D_1(R) = 0101 0101 1001 1001 1110 0000 0001

1 5 9 13 17 21 25

C_1(L) = 1110 0001 1001 1001 0101 0100 0001

29 33 37 41 45 49 53

D_1(R) = 0101 0101 1001 1001 1110 0000 0001

➔

PC-2

14	17	11	24	1	5	3	28
15	6	21	10	23	19	12	4
26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40
51	45	33	48	44	49	39	56
34	53	46	42	50	36	29	32

0000 1011
0000 0010
0110 0111

1001 1011
0100 1001
1010 0101

Thus,

K1 = 0000 1011 0000 0010 0110 0111
1001 1011 0100 1001 1010 0101

(b) Derive L0 and R0.

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

1100 1100
0000 0000
1100 1100
1111 1111

1111 0000
1010 1010
1111 0000
1010 1010

⇨ L0 = 1100 1100 0000 0000 1100 1100 1111 1111

⇨ R0 = 1111 0000 1010 1010 1111 0000 1010 1010

(c) **Expand R0 to get E[R0], where E[.] is the expansion function of Table 3.2 of your textbook.**

E

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

1 5 9 13 17 21 25 29

R0 = 1111 0000 1010 1010 1111 0000 1010 1010

⇨

$E[R_0]$ = 011110 100001 010101 010101
011110 100001 010101 010101

(d) **Calculate A = E[R0] ⊕ K1.**

$A = E[R_0] \oplus K_1 =$

0111 1010 0001 0101 0101 0101
0111 1010 0001 0101 0101 0101

⊕

0000 1011 0000 0010 0110 0111
1001 1011 0100 1001 1010 0101

=

0111 0001 0001 0111 0011 0010
1110 0001 0101 1100 1111 0000

Thus

A = 011100 010001 011100 110010
111000 010101 110011 110000

(e) **Group the 48 bit results of (d) into sets of 6 bits and evaluate the corresponding S-box substitutions.**

A = 011100 010001 011100 110010
111000 010101 110011 110000

S_1																
	x0000x	x0001x	x0010x	x0011x	x0100x	x0101x	x0110x	x0111x	x1000x	x1001x	x1010x	x1011x	x1100x	x1101x	x1110x	x1111x
0yyyy0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0yyyy1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
1yyyy0	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
1yyyy1	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

$S_1(011100) = 0000$

S_2

	x0000x	x0001x	x0010x	x0011x	x0100x	x0101x	x0110x	x0111x	x1000x	x1001x	x1010x	x1011x	x1100x	x1101x	x1110x	x1111x
0yyyy0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
0yyyy1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
1yyyy0	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
1yyyy1	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

$S_2(010001) = 1100$

S_3

	x0000x	x0001x	x0010x	x0011x	x0100x	x0101x	x0110x	x0111x	x1000x	x1001x	x1010x	x1011x	x1100x	x1101x	x1110x	x1111x
0yyyy0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
0yyyy1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
1yyyy0	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
1yyyy1	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

$S_3(011100) = 0010$

S_4

	x0000x	x0001x	x0010x	x0011x	x0100x	x0101x	x0110x	x0111x	x1000x	x1001x	x1010x	x1011x	x1100x	x1101x	x1110x	x1111x
0yyyy0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
0yyyy1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
1yyyy0	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
1yyyy1	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

$S_4(110010) = 0001$

S_5

	x0000x	x0001x	x0010x	x0011x	x0100x	x0101x	x0110x	x0111x	x1000x	x1001x	x1010x	x1011x	x1100x	x1101x	x1110x	x1111x
0yyyy0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
0yyyy1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
1yyyy0	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
1yyyy1	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

$S_5(111000) = 0110$

S_6

	x0000x	x0001x	x0010x	x0011x	x0100x	x0101x	x0110x	x0111x	x1000x	x1001x	x1010x	x1011x	x1100x	x1101x	x1110x	x1111x
0yyyy0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
0yyyy1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
1yyyy0	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
1yyyy1	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

$S_6(010101) = 1101$

S_7

	x0000x	x0001x	x0010x	x0011x	x0100x	x0101x	x0110x	x0111x	x1000x	x1001x	x1010x	x1011x	x1100x	x1101x	x1110x	x1111x
0yyyy0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
0yyyy1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
1yyyy0	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
1yyyy1	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

$S_7(110011) = 0101$

S_8																
	x0000x	x0001x	x0010x	x0011x	x0100x	x0101x	x0110x	x0111x	x1000x	x1001x	x1010x	x1011x	x1100x	x1101x	x1110x	x1111x
0yyyy0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
0yyyy1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
1yyyy0	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
1yyyy1	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

S_8(110000) = 0000

(f) Concatenate the results of (e) to get a 32 bit result, B.

B = 0000 1100 0010 0001 0110 1101 0101 0000

(g) Apply the permutation to get P(B).

P

16	7	20	21	29	12	28	17
1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9
19	13	30	6	22	11	4	25

1 5 9 13 17 21 25 29

B = 0000 1100 0010 0001 0110 1101 0101 0000

- ⇨ 10010010
- ⇨ 00011100
- ⇨ 00100000
- ⇨ 10011100

P(B) = 1001 0010 0001 1100 0010 0000 1001 1100

(h) Calculate R1 = P(B) ⊕ L0.

$R_1 = P(B) \oplus L_0$

⇨

1001 0010 0001 1100 0010 0000 1001 1100

⊕

1100 1100 0000 0000 1100 1100 1111 1111

R_1 = 0101 1110 0001 1100 1110 1100 0110 0011

(i) Write down the ciphertext.

Cypertext = $L_1 + R_1 = R_0 + R_1$ =

1111 0000 1010 1010 1111 0000 1010 1010

0101 1110 0001 1100 1110 1100 0110 0011

2. **(a) Using RSA, choose p=3, and q=11, and encode the word "dog" by encrypting each letter separately. Apply the decryption algorithm to the encrypted version to recover the original plaintext message.**

N = pq = 33
(p-1)(q-1) = 2x10 = 20
e = 3

$$(\mathrm{d} \times \mathrm{e}) \bmod ((\mathrm{p}-1)(\mathrm{q}-1)) \equiv 1$$

d: $\Rightarrow (\mathrm{d} \times 3) \bmod 20 \equiv 1$

$\Rightarrow \mathrm{d} = 7$

Encrypting:

d: $c = m^e (\bmod N) = 4^3 \bmod 33 = 31 = e$

o: $c = m^e (\bmod N) = 15^3 \bmod 33 = 9 = i$

g: $c = m^e (\bmod N) = 7^3 \bmod 33 = 13 = m$

The cypertext is "eim"

Decryption:

m1: $m = c^d (\bmod N) = 31^7 \bmod 33 = 4 = c$

m2: $m = c^d (\bmod N) = 9^7 \bmod 33 = 15 = o$

m3: $m = c^d (\bmod N) = 13^7 \bmod 33 = 7 = g$

Thus, we get the plaintext "dog".

(b) Repeat part (a) but now encrypt "dog" as one message.
dog = 4,15,7 = 00100 01111 00111 = 10747 = 22(mod 33) = v

Encryption:

v: $c = m^e (\bmod N) = 10747^3 \bmod 33 = 22 = v$

Decryption:

v: $m = c^d (\bmod N) = 22^7 \bmod 33 = 22 = v$

3. Consider RSA with p=5 and q=11.

(a) what are n and z.

n = pq = 55

z = (p-1)(q-1) = 4x10 = 40

(b) Let e be 3, why is this an acceptable choice for e.

e = 3 is acceptable because we need to choose an integer e such that 1 < e < z and e, z are coprime.

When e = 3, it fulfill all the above requirements, thus e = 3 is acceptable.

(c) Find d such that de=1(mod z) and d<160.

$$(\mathrm{d}\times\mathrm{e})\bmod((\mathrm{p}-1)(\mathrm{q}-1))\equiv 1$$

d: $\Rightarrow (\mathrm{d}\times 3)\bmod 40\equiv 1$

$\Rightarrow \mathrm{d}=27$

(d) Encrypt the message m=8 using the key (n,e). Let c denote the corresponding ciphertext. Show all the work.

Encrypting:

8: $c = m^e (\bmod N) = 8^3 \bmod 55 = 17$

Thus the ciphertext is 17.