CS 4920/5920 Applied Cryptography Spring 2018

Assignment 3 – Solution

Problem 1 –

4. First, pass the 64 bit input through PC – 1 to produce a 56 bit result. Then perform a left circular shift separately on the two 28 bit halves. Finally, pass the 56 bit result through PC – 2 to produce the 48 bit K_1.:

in binary notation: 0000 1011 0000 0010 0110 0111

1001 1011 0100 1001 1010 0101

In hexadecimal notation: **0 B 0 2 6 7 9 B 4 9 A 5**

b) L_0, R_0 are derived by passing the 64 – plaintext through IP:

L_0 = 1100 1100 0000 0000 1100 1100 1111 1111 R_0 = 1111 0000

1010 1010 1111 0000 1010 1010

c) The E table expands R_0 to 48 bits:

$E(R_0)$ = 01110 100001 010101 010101 011110 100001 010101 010101

d) A = 011100 010001 011100 110010 111000 010101 110011 110000

e) s_1^{00} (1110) = s_1^{0}(14) = 0 (base 10) = 0000 (base 2) s_2^{01} (1000) = s_2^{1}(8) = 12 (base 10) = 1100 (base 2)

s_3^{00} (1110) = s_3^{0}(14) = 2 (base 10) = 0010 (base 2) s_4^{10} (1001) = s_4^{2}(9) = 1 (base 10) = 0001 (base 2)

s_5^{10} (1100) = s_5^{2}(12) = 6 (base 10) = 0110 (base 2)

s_6^{01} (1010) = s_6^{1}(10) = 13 (base 10) = 1101 (base 2)

s_7^{11} (1001) = s_7^{3}(9) = 5 (base 10) = 0101 (base 2) s_8^{10} (1000) =

s_8^{2}(8) = 0 (base 10) = 0000 (base 2)

f) B = 0000 1100 0010 0001 0110 1101 0101 0000

g) Using table 4.2d, P(B) = 1001 0010 0001 1100 0010 0000 1001 1100

h) R_1 = 0101 1110 0001 1100 1110 1100 0110 0011

i) $L_1 = R_0$. The ciphertext is the concatenation of L_1 and R_1.

Problem 2 –

a.) 4321 = 1234(3) + 619

1234 = 619(1) + 615

619 = 615 (1) + 4

615 = 4(153) + 3

4 = 3(1) + 1 3 = 1(3) + 0

gcd(4321, 1234) = 1

Thus, multiplicative inverse does exist

1 = 4 – 3(1)

1 = 4 – (615 – 4*153)

1 = 4*154 – 615

1 = (619 - 615)*154 – 615

1 = 619(154) – 615(155)

1 = 619(154) – (1234 – 619*1)155

1 = 619(154) – 1234(155) + 619(155)

1 = 619(309) – 1234(155)

1 = (4321 – 1234*3)(309 - 1234*155)

1 = 4321(309) – 1234(927) – 1234(155)

1 = 4321(309) – 1234(1082)

1 = 4321(309) + 1234(-1082)

1 mod 4321 = 1234(-1082)

= 4321 – 1082

= **3239**

b.) gcd(40902, 550) = 34 ≠ 1, so there is no multiplicative inverse.

c.) 550

Problem 3 –

(a)

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

x	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

w	-w	w-1
0	0	-
1	4	1
2	3	3
3	2	2
4	1	4

(b)

Power Representation	Polynomial Representation	Binary Representation	Decimal (Hex) Representation
0	0	0000	0
g^0 (= g^{15})	1	0001	1
g1	g	0010	2
g^2	g2	0100	4
g^3	g3	1000	8
g^4	g + 1	0011	3
g^5	$g^2 + g$	0110	6
g^6	g3 + g2	1100	12
g^7	$g^3 + g + 1$	1011	11
g^8	$g^2 + 1$	0101	5
g^9	$g^3 + g$	1010	10
g10	$g^2 + g + 1$	0111	7
g11	$g^3 + g^2 + g$	1110	14
g12	$g^3 + g^2 + g + 1$	1111	15
g13	$g^3 + g^2 + 1$	1101	13
g14	$g^3 + 1$	1001	9

Problem 4 –

a) $\begin{bmatrix} x^3+1 & x \\ x & x^3+1 \end{bmatrix} \begin{bmatrix} 1 & x^2 \\ x^2 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

To get the above result, observe that $(x^5 + x^2 + x)$ mod $(x^4 + x + 1) = 0$

b) It is easy to see that x^4 mod $(x^4 + 1) = 1$. This is so because we can write:

$x^4 = [1 \text{ x } (x^4 + 1)] + 1$

Recall that the addition operation is XOR. Then, x^8 mod $(x^4 + 1) =$

$[x^4 \text{ mod } (x^4 + 1)]$ x $[x^4 \text{ mod } (x^4 + 1)]$

= 1 x 1

= 1

So, for any positive integer a, $x^{4a} \bmod (x^4 + 1) = 1$. Now consider any integer i of the form $i = 4a + (i \bmod 4)$. Then, $x^i \bmod (x^4 + 1) = [(x^{4a}) \times (x^{i \bmod 4})] \bmod (x^4 + 1)$

$= [x^{4a} \bmod (x^4 + 1)] \times [x^{i \bmod 4} \bmod (x^4 + 1)]$

$= x^{i \bmod 4}$

The same result can be demonstrated using long division.

Problem 5 –

5. a.

00	04	08	0C
01	05	09	0D
02	06	0A	0E
03	07	0B	0F

b.

01	05	09	0D
00	04	08	0C
03	07	0B	0F
02	06	0A	0E

c.

7C	6B	01	D7
63	F2	30	FE
7B	C5	2B	76
77	6F	67	AB

d.

7C	6B	01	D7
F2	30	FE	63
2B	76	7B	C5
AB	77	6F	67

e.

75	87	0F	B2
55	E6	04	22
3E	2E	B8	8C
10	15	58	0A