Homework 2 Solutions

---

1. This problem provides a numerical example of encryption using a one-round version of DES. Suppose both the key and the output of the initial p-box are:

1010 1101 0101 0110 1100 1001 1101 1010 1001 0001 1011 1011 0001 1001 1011 1010

a. Derive k1, the first round subkey

4	8	12	16	20	24	28	32	36	40	44	48	52	56	60	64
1010	1101	0101	0110	1100	1001	1101	1010	1001	0001	1011	1011	0001	1001	1011	1010

Table: Parity-bit drop table

57	49	41	33	25	17	09	01
58	50	42	34	26	18	10	02
59	51	43	35	27	19	11	03
60	52	44	36	63	55	47	39
31	23	15	07	62	54	46	38
30	22	14	06	61	53	45	37
29	21	13	05	28	20	12	04

After parity drop and permutation:

L	R
1011 1101 0000 1110 1010 0001 1111	1010 1010 0000 0011 1110 1101 1010

Both parts are shifted to the left by 1 bit:

4	8	12	16	20	24	28	32	36	40	44	48	52	56
0111	1010	0001	1101	0100	0011	1111	0101	0100	0000	0111	1101	1011	0101

After going through the compression P-box:

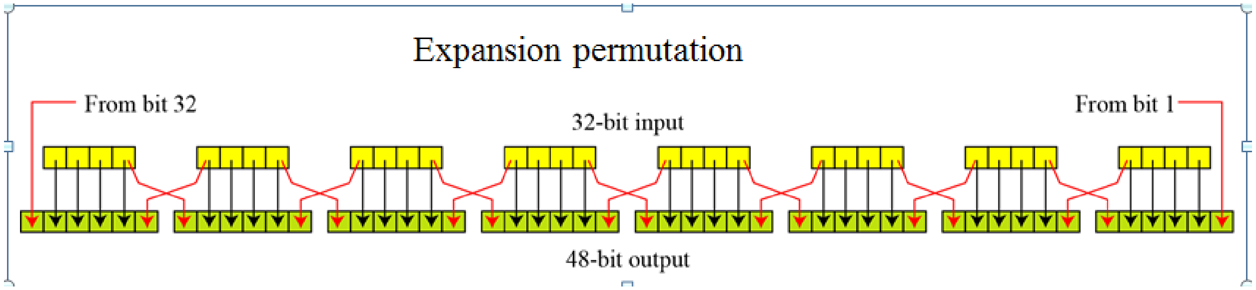
14	17	11	24	01	05	03	28
15	06	21	10	23	19	12	04
26	08	16	07	27	20	13	02
41	52	31	37	47	55	30	40
51	45	33	48	44	49	39	56
34	53	46	42	50	36	29	32

K1 = 1001 0111 0000 1011 1011 1011 0100 0010 1101 1101 1011 0001 (9 7 0 B B B 4 2 D D D 1)

b. Derive L0, R0

L0 = 1010 1101 0101 0110 1100 1001 1101 1010
R0 = 1001 0001 1011 1011 0001 1001 1011 1010

c. Expand R0 to get E[R0] using the Expansion P-box



E(R0) = 010010 100011 110111 110110 100011 110011 110111 11 0101
= 0100 1010 0011 1101 1111 0110 1000 1111 0011 1101 1111 0101
= 4 A 3 D F 6 8 F 3 D F 5

d. Calculate A = E[R0] XOR K1

E[R0] $\oplus$ K1

= 0100 1010 0011 1101 1111 0110 1000 1111 0011 1101 1111 0101
$\oplus$ 1001 0111 0000 1011 1011 1011 0100 0010 1101 1101 1011 0001

= 1101 1101 0011 0110 0100 1101 1100 1101 1110 0000 0100 0100

= D D 3 6 4 D C D E 0 4 4

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

1101 1101 0011 0110 0100 1101 1100 1101 1110 0000 0100 0100

Formatted to groups of 6 bits:

110111	010011	011001	001101	110011	011110	000001	000100
S1	S2	S3	S4	S5	S6	S7	S8

4 8 12

S_1	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
S_2	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
S_3	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
S_4	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14
S_5	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3
S_6	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
S_7	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12
S_8	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

110111 → S1 → ~~7~~ 14 = ~~0111~~ 1110

010011 → S2 → 0 = 0000

011001 → S3 → 12 = 1100

001101 → S4 → 0 = 0000

110011 → S5 → F = 1111

011110 → S6 → 11 = 1011

000001 → S7 → 13 = 1101

000100 → S8 → 8 = 1000

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

B = 1110 0000 1100 0000 1111 1011 1101 1000 (70C0 FBD8)

g. Apply the permutation to get P(B)

The straight P-box:

16	07	20	21	29	12	28	17
01	15	23	26	05	18	31	10
02	08	24	14	32	27	03	09
19	13	30	06	22	11	04	25

4 8 12 16 20 24 28 32

B = 1110 0000 1100 0000 0110 1011 1101 1000

P(B) = 0011 1011 1011 0101 1010 0011 1000 0001

h. Calculate R1 = P(B) XOR L0

$P(B) \oplus L0$

= 0011 1011 1011 0101 1010 0011 1000 0001

$\oplus$ 1010 1101 0101 0110 1100 1001 1101 1010

= 1001 0110 1110 0011 0110 1010 0101 1011

= 9 6 E 3 6 A 5 C

i. Write down the output of the first round.

1001 0001 1011 1011 0001 1001 1011 1010 1001 0110 1110 0011 0110 1010 0101 1011

9 1 D D 1 9 D A 9 6 E 3 6 A 5 C

---

2. For the group $G = \langle Z_{26^*}, x \rangle$

a. Find the order of the group

Z_{26^*} = {1, 3, 5, 7, 9, 11,15,17,19, 21, 23, 25}

There are 12 elements in the group, so the order of the group is 12

b. Find the order of each element in the group

1^0= 1
ord(1) = 1

3^0= 1
3^1= 3
3^2= 9
3^3= 9*3 mod 26 = 1
Ord(3) = 3

5^0= 1
5^1= 5
5^2= 25
5^3= 25*5 mod 26 = 21
5^4= 21*5 mod 26 = 1
Ord(5) = 4

7^0= 1
7^1= 7
7^2= 7*7 mod 26 = 23
7^3= 23*7 mod 26 = 5
7^4= 5*7 mod 26 = 9
7^5= 9*7 mod 26 = 11

$7^6 = 11*7 \bmod 26 = 25$
$7^7 = 25*7 \bmod 26 = 19$
$7^8 = 19*7 \bmod 26 = 3$
$7^9 = 3*7 \bmod 26 = 21$
$7^{10} = 21*7 \bmod 26 = 17$
$7^{11} = 17*7 \bmod 26 = 15$
$7^{12} = 15*7 \bmod 26 = 1$
Ord(7) = 12

$9^0 = 1$
$9^1 = 9$
$9^2 = 9*9 \bmod 26 = 3$
$9^3 = 3*9 \bmod 26 = 1$
Ord(9) = 3

$11^0 = 1$
$11^1 = 11$
$11^2 = 11 * 11 \bmod 26 = 17$
$11^3 = 17*11 \bmod 26 =5$
$11^4 = 5*11 \bmod 26 = 3$
$11^5 = 3*11 \bmod 26 = 7$
$11^6 = 7*11 \bmod 26 = 25$
$11^7 = 25*11 \bmod 26 = 15$
$11^8 = 15*11 \bmod 26 = 9$
$11^9 = 9*11 \bmod 26 = 21$
$11^{10} = 21*11 \bmod 26 = 23$
$11^{11} = 23*11 \bmod 26 = 19$
$11^{12} = 19*11 \bmod 26 = 1$

Ord(11) =12

$15^0 = 1$
$15^1 = 15$
$15^2 = 15 * 15 \bmod 26 = 17$
$15^3 = 17 * 15 \bmod 26 = 21$
$15^4 = 21 * 15 \bmod 26 = 3$
$15^5 = 3 * 15 \bmod 26 = 19$
$15^6 = 19 * 15 \bmod 26 = 25$
$15^7 = 25 * 15 \bmod 26 = 11$
$15^8 = 11 * 15 \bmod 26 = 9$
$15^9 = 9 * 15 \bmod 26 = 5$
$15^{10} = 5 * 15 \bmod 26 = 23$
$15^{11} = 23 * 15 \bmod 26 = 7$
$15^{12} = 7 * 15 \bmod 26 = 1$
Ord(15) = 12

$17^0 = 1$
$17^1 = 17$
$17^2 = 17 * 17 \bmod 26 = 3$
$17^3 = 3*17 \bmod 26 = 25$
$17^4 = 25*17 \bmod 26 = 9$
$17^5 = 9*17 \bmod 26 = 23$
$17^6 = 23*17 \bmod 26 = 1$
Ord(17) = 6

$19^0 = 1$
$19^1 = 19$
$19^2 = 19 * 19 \bmod 26 = 23$

$19^3 = 23*19 \bmod 26 = 21$
$19^4 = 21*19 \bmod 26 = 9$
$19^5 = 9*19 \bmod 26 = 15$
$19^6 = 15*19 \bmod 26 = 25$
$19^7 = 25*19 \bmod 26 = 7$
$19^8 = 7*19 \bmod 26 = 3$
$19^9 = 3*19 \bmod 26 = 5$
$19^{10} = 5*19 \bmod 26 = 17$
$19^{11} = 17*19 \bmod 26 = 11$
$19^{12} = 11*19 \bmod 26 = 1$
Ord(19) = 12

$21^0 = 1$
$21^1 = 21$
$21^2 = 21 * 21 \bmod 26 = 25$
$21^3 = 25*21 \bmod 26 = 5$
$21^4 = 5*21 \bmod 26 = 1$
Ord(21) = 4

$23^0 = 1$
$23^1 = 23$
$23^2 = 23 * 23 \bmod 26 = 9$
$23^3 = 9*23 \bmod 26 = 25$
$23^4 = 25*23 \bmod 26 = 3$
$23^5 = 3*23 \bmod 26 = 17$
$23^6 = 17*23 \bmod 26 = 1$
Ord(19) = 6

$25^0 = 1$
$25^1 = 25$

$25^2 = 25 * 25 \bmod 26 = 1$
Ord(25) = 2

c. Is the group is a cyclic group? Prove your answer and find the generator(s) if the answer is yes.

Yes. The generators are: 7,11,15,19

---

3. Using the irreducible polynomial $f(x) = x^5+x^4+x^3+ x^2+1$ to

a) generate the elements of the field $GF(2^5)$

0	**0**	**0**	**0**	**00000**
g^0	g^0	g^0	g^0	**00001**
g^1	g^1	g^1	g^1	**00010**
g^2	g^2	g^2	g^2	**00100**
g^3	g^3	g^3	g^3	**01000**
g^4	g^4	g^4	g^4	**10000**
g^5	g^5	g^5	$g^4 + g^3 + g^2 + 1$	**11101**
g^6	$g\ (g^5)$	$g\ (g^4 + g^3 + g^2 + 1)$	$g^2 + g+1$	**00111**
g^7	$g\ (g^6)$	$g\ (g^2 + g+1)$	$g^3 + g^2 + g$	**01110**
g^8	$g\ (g^7)$	$g\ (g^3 + g^2 + g)$	$g^4 + g^3 + g^2$	**11100**
g^9	$g\ (g^8)$	$g\ (g^4 + g^3 + g^2\ )$	$g^2 + 1$	**00101**
g^{10}	$g\ (g^9)$	$g\ (g^2 +1)$	$g^3 + g$	**01010**
g^{11}	$g\ (g^{10})$	$g\ (g^3 + g)$	$g^4 + g^2$	**10100**
g^{12}	$g\ (g^{11})$	$g\ (g^4 + g^2)$	$g^4 + g^2 + 1$	**10101**

g^{13}	$g(g^{12})$	$g(g^4+g^2+1)$	g^4+g^2+g+1	10111
g^{14}	$g(g^{13})$	$g(g^4+g^2+g+1)$	g^4+g+1	10011
g^{15}	$g(g^{14})$	$g(g^4+g+1)$	g^4+g^3+g+1	11011
g^{16}	$g(g^{15})$	$g(g^4+g^3+g+1)$	g^3+g+1	01011
g^{17}	$g(g^{16})$	$g(g^3+g+1)$	g^4+g^2+g	10110
g^{18}	$g(g^{17})$	$g(g^4+g^2+g)$	g^4+1	10001
g^{19}	$g(g^{18})$	$g(g^4+1)$	$g^4+g^3+g^2+g+1$	11111
g^{20}	$g(g^{19})$	$g(g^4+g^3+g^2+g+1)$	$g+1$	00011
g^{21}	$g(g^{20})$	$g(g+1)$	g^2+g	00110
g^{22}	$g(g^{21})$	$g(g^2+g)$	g^3+g^2	01100
g^{23}	$g(g^{22})$	$g(g^3+g^2)$	g^4+g^3	11000
g^{24}	$g(g^{23})$	$g(g^4+g^3)$	g^3+g^2+1	01101
g^{25}	$g(g^{24})$	$g(g^3+g^2+1)$	g^4+g^3+g	11010
g^{26}	$g(g^{25})$	$g(g^4+g^3+g)$	g^3+1	01001
g^{27}	$g(g^{26})$	$g(g^3+1)$	g^4+g	10010
g^{28}	$g(g^{27})$	$g(g^4+g)$	g^4+g^3+1	11001

g^{29}	$g\ (g^{28})$	$g\ (g^4 + g^3 + 1\ )$	$g^3 + g^2 + g + 1$	01111
g^{30}	$g\ (g^{29})$	$g\ (g^3 + g^2 + g + 1\ )$	$g^4 + g^3 + g^2 + g$	11110

b) **based on the results of a)**, calculate the followings in $GF(2^5)$

b.1) $(x^4 - x + 1)^{-1}$

$x^4 - x + 1 = x^4 + x + 1 = \mathbf{10011} = \mathbf{g^{14}}$

$(x^4 - x + 1)^{-1} = g^{\mathbf{-14\ mod\ 31}} = \mathbf{g^{17} = 10110 = x^4 + x^2 + x}$

b.2) $(x^3 - x + 1) * (x^4 + x^2 - x + 1)$

$x^3 - x + 1 = \mathbf{01011} = \mathbf{g^{16}}$

$x^4 + x^2 - x + 1 = \mathbf{10111} = \mathbf{g^{13}}$

$\mathbf{g^{16}\ x\ g^{13} = g^{29}}$

so, $(x^3 - x + 1) * (x^4 + x^2 - x + 1) = x^3 + x^2 + x + 1$

b.3) $(x^4 - x^3 + 1) / (x^2 + x + 1)$

$x^4 - x^3 + 1 = \mathbf{11001} = \mathbf{g^{28}}$

$x^2 + x + 1 = \mathbf{00111} = \mathbf{g^6}$

$(x^4 - x^3 + 1) / (x^2 + x + 1) = \mathbf{g^{28} / g^6 = g^{22} = 01100} = x^3 + x^2$