EECE 632 – Cryptography and Computer Security

Homework #3 – Solution

CHAPTER 4

Exercise #1

Determine gcd(24140, 16762)

GCD (24140, 16762) = GCD (16762, 24140 mod 16762) =
GCD (16762, 7378) = GCD (7378, 16762 mod 7378) =
GCD (7378, 2006) = GCD (2006, 7378 mod 2006) =
GCD (2006, 1360) = GCD (1360, 2006 mod 1360) =
GCD (1360, 646) = GCD (646, 1360 mod 646) =
GCD (646, 68) = GCD (68, 646 mod 68) =
GCD (68, 34) = GCD (34, 68 mod 34) =
GCD (34, 0) = **34**

Exercise #2

Use the extended Euclidean algorithm to find the multiplicative inverse of:
a) 1234 mod 4321 b) 24140 mod 40902

a. Inverse of 1234 in GF(4321) is -1082 + 4321 = **3239**

Q	A1	A2	A3	B1	B2	B3
–	1	0	4321	0	1	1234
3	0	1	1234	1	-3	619
1	1	-3	619	-1	4	615
1	-1	4	615	2	-7	4
153	2	-7	4	-307	1075	3
1	-307	1075	3	309	**-1082**	**1**

b. Inverse of 24140 in GF(40902) **does not exist** since they are not relatively prime.

Q	A1	A2	A3	B1	B2	B3
–	1	0	40902	0	1	24140
1	0	1	24140	1	-1	16762
1	1	-1	16762	-1	2	7378
2	-1	2	7378	3	-5	2006
3	3	-5	2006	-10	17	1360
1	-10	17	1360	13	-22	646
2	13	-22	646	-36	61	68
9	-36	61	68	337	-571	34
2	337	-571	34	-710	1203	**0**

Exercise #3

For polynomial arithmetic with coefficients in Z_{10}, perform the following calculations:
a) $(7x + 2) - (x^2 + 5)$
b) $(6x^2 + x + 3) * (5x^2 + 2)$

a. $9x^2 + 7x + 7$
b. $5x^3 + 7x^2 + 2x + 6$

Exercise #4

Determine the multiplicative inverse of $x^3 + x + 1$ in $GF(2^4)$.
The irreducible polynomial $m(x) = x^4 + x + 1$

The multiplicative inverse is $\boldsymbol{x^2 + 1}$

Q	A1	A2	A3	B1	B2	B3
–	1	0	$x^4 + x + 1$	0	1	$x^3 + x + 1$
x	0	1	$x^3 + x + 1$	1	x	$x^2 + 1$
x	1	x	$x^2 + 1$	x	$\boldsymbol{x^2 + 1}$	**1**

Exercise #5

Show that an integer N is congruent modulo 9 to the sum of its decimal digits.
For example, $475 \equiv 4 + 7 + 5 = 16 \equiv 1 + 6 = 7 \bmod 9$.

$10 \bmod 9 = 1 \Rightarrow 10^n \bmod 9 = 1$
Any number can be written in decimal form as $D = D_n D_{n-1} \ldots D_1 D_0$
Then we know that:

$$\sum_{i=0}^{n} D_i 10^i \equiv \sum_{i=0}^{n} D_i \ (mod\ 9)$$

The above expression says that D is congruent to the sum of its decimal digits modulo 9.

CHAPTER 5

Exercise #6

a. $\{44\} \longrightarrow \{0100\ 0100\} \longrightarrow x^6 + x^2$
$GF(2^8) \longrightarrow m(x) = x^8 + x^4 + x^3 + x + 1$

Initialization	$A1(x) = 1;$	$A2(x) = 0;$	$A3(x) = x^8 + x^4 + x^3 + x + 1$
	$B1(x) = 0;$	$B2(x) = 1;$	$B3(x) = x^6 + x^2$
Iteration 1	$Q(x) = x^2$		
	$A1(x) = 0;$	$A2(x) = 1;$	$A3(x) = x^6 + x^2$
	$B1(x) = 1;$	$B2(x) = x^2;$	$B3(x) = x^3 + x + 1$
Iteration 2	$Q(x) = x^3 + x + 1$		
	$A1(x) = 1;$	$A2(x) = x^2;$	$A3(x) = x^3 + x + 1$
	$B1(x) = x^3 + x + 1;$	$B2(x) = \mathbf{x^5 + x^3 + x^2 + 1};$	$B3(x) = 1$

$x^5 + x^3 + x^2 + 1 \longrightarrow \{0010\ 1101\} \longrightarrow \{2D\}$
Inverse of $\{44\}$ in $GF(2^8)$ is $\{2D\}$

b. After getting the multiplicative inverse of $\{44\} \rightarrow \{0100\ 0100\}$, we apply the below transformation:

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{bmatrix} \oplus \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} \longrightarrow \{0001\ 1011\} \longrightarrow \{1B\}$$

The entry of $\{44\}$ in the AES S-box is $\{1B\}$.

Exercise #7

W(0) = AA AA AA AA
W(1) = BB BB BB BB
W(2) = CC CC CC CC
W(3) = DD DD DD DD
W(4) = 6A 6B 6B 6B
W(5) = D1 D0 D0 D0
W(6) = 1D 1C 1C 1C
W(7) = C0 C1 C1 C1

Exercise #8

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

Exercise #9

C6 AB 01 E4