CS 485 - Information Security - Assignment 3

Question 1:
w[36] = 3A 74 E5 8D (in hex)
Bin : = 0011 1010 0111 0100 1110 0101 1000 1101
w[39] = 8F 17 60 C2 (in hex)
Left Shift: = 17 60 C2 8F
LookUp Table= F0 D0 25 73
RoundConst[40] = 36 00 00 00
XOR = C6 D0 25 73
Bin: = 1100 0110 1101 0000 0010 0101 0111 0011
Calculate w[40] = w[36] + g(w[39])
Bin = 1111 1100 1010 0100 1100 0000 1111 1110
Hex: FC A4 C0 FE

Question 2:
a) a = 7, m = 26 (affine cipher)
26 = 7*3 + 5 → 5 = r0 - 3(r1)
7 = 5*1 + 2 → 2 = r1 - (r0 - 3r1) = 4r1 - r0
5 = 2*2 + 1 → 1 = (r0-3r1) - 2(4r1-r0) = r0 - 3r1 - 8r1 + 2r0 = 3r0 - 11r1
26 - 11 = 15
Inverse = 15
Test: 7*15 = 105 mod 26 = 1 TRUE

b) a=19,m=999
999 = 19*52 + 11 → 11 = r0 - 52r1
19 = 11 * 1 + 8 → 8 = r1 - (r0 -52r1) = 53r1 - r0
11 = 8 * 1 + 3 → 3 = (r0 - 52r1) - (53r1 - r0) = 2r0 - 105r1
8 = 3*2 + 2 → 2 = 53r1 - r0 - 2(2r0 - 105r1) = -5r0 + 263r1
3 = 2*1 + 1 → 1 = 2r0 - 105r1 +10r0 - 526r1 = -12r0 + 631r1
Inverse = 631
Test: 19 * 631 = 11989 mod 999 = 1 TRUE

Question 3:
Verify that Euler's Theorem holds in Zm , m=6, 9, for all elements a for which gcd(a,m) = 1.
Also verify that the theorem does not hold for elements a for which gcd(a,m) ≠ 1

The theorem: a^φ(m) ≡ 1 (mod m)
φ(6) = 2 {1, 5} ⇒ 1^2 mod 6 = 1, 5^2 mod 6 = 1 ⇒ TRUE
φ(9) = 6 {1, 2, 4, 5, 7, 8} 1^6 mod 9 = 1, 64 mod 9 = 1, 4096 mod 9 = 1, 7^6 mod 9 = 1, 8^6 mod 9 = 1 ⇒ TRUE

4^2 = 16 mod 6 = 4 != 1 FALSE
3^6 = 729 mod 9 = 0 != 1 FALSE

Question 4:
One of the most attractive applications of public-key algorithms is the establishment of a secure session key for a private-key algorithm such as AES over an insecure channel. Assume Bob has a pair of public/private keys for the RSA cryptosystem. Develop a simple protocol using RSA which allows the two parties Alice and Bob to agree on a shared secret key. Who determines the key in this protocol, Alice, Bob, or both?

Answer:
Under the RSA structure, Alice and Bob will not need to agree on a shared secret key because Bob can simply encrypt a message (or a new shared key) using Alice's public key and vice versa. Both (depending on who initiates the proposal for a shared key) can determine the key in this protocol. If they want a better method to generate a shared secret key, they should use a DH key exchange protocol instead.

Question 5:
Z*5

a	ord(a)
1	1^ 1= 1 mod 5 = 1
2	2^4 = 16 mod 5 = 1
3	3^4 = 81 mod 5 = 1
4	4^2 = 16 mod 5 = 1

Z*7

a	ord(a)
1	1^ 1= 1 mod 7 = 1
2	2^3 = 8 mod 7 = 1
3	3^6 = 729 mod 7 = 1
4	4^6 = 4096 mod 7 = 1
5	5^6 = 15625 mod 7 = 1
6	6^2 = 36 mod 7 = 1

Z*13

a	ord(a)

1	1^ 1 = 1 mod 13 = 1
2	2^12 = 4096 mod 13 = 1
3	3^3 = 27 mod 13 = 1
4	4^6 = 4096 mod 13 = 1
5	5^4 = 625 mod 13 = 1
6	6^12 = 2176782336 mod 13 = 1
7	7^12 = 13841287201 mod 13 = 1
8	8^4 = 4096 mod 13 = 1
9	9^3 = 729 mod 13 = 1
10	10^6 = 1000000 mod 13 = 1
11	11^12 = ... mod 13 = 1
12	12^2 = 144 mod 13 = 1

Question 6:
We consider the group Z*53. What are the possible element orders? How many elements exist for each order?
a) How many elements does each of the multiplicative groups, Z*5, Z*7 , Z*13 have?

- They have 4, 6, and 12 elements respectively.

b) Do all orders from above divide the number of elements in the corresponding multiplicative group (Z*5, Z*7 , Z*13)? **YES**
c) Verify for the groups that the number of primitive elements is given by φ (|Z*p|).
φ (|Z*p|) = p - 1; since Euler's phi function gives us the number of coprime elements in Z, they also correspond to the number of primitive elements in Z.

Question 7:
An easy man in the middle attack that Oscar can attempt is to simply intercept the messages between Alice and Bob and substitute them with his own public keys. This will allow Oscar to initiate his own DH key exchange with both Alice and Bob individually.

Question 8:

x	y	x^3 + 3x + 2 mod 7	y^2 mod 7
0	0	2	0

1	1	6	1
2	2	2	4
3	3	3	2
4	4	1	2
5	5	2	4
6	6	5	1

A) 0,3 ; 0,4 ; 2,3 ; 2,4 ; 5,3 ; 5,4 ; 4,1 ; 4,6

B) The order of the group is len(all the points) + neutral element = 9

P	s
1 P = 0, 3	

2 P = P+P
X = 16 -0 -0 mod 7 = 2
Y = 4(0-2)-3 mod 7 = 3
	3(0)^2 + 3/6 = 3 * 6^-1 mod 7 = 3*6 = 18 mod 7 = 4

3 P = 2P +P X= 0 - 2 -0 = -2 mod 7 = 7-2 = 5 Y=0-3 mod 7 = 7 - 3 = 4	3-3 / 2-0 = 0*2^-1 = 0

4 P = 3P +P
X = 9 - 0 - 5 mod 7 = 4
y = 3(5-4) - 4 mod 7 = -1 mod 7 = 6
	4-3 / 5-0 = 1 * 5^-1 mod 7 = 3

5 P = 4P +P
X = 36 - 0 - 4 mod 7 = 4
Y = 6(0-4) - 3 mod 7 = -6 mod 7 = 1
	6-3 / 4-0 = 3 * 4^-1 mod 7 = 6

6 P = 5P + P
X = 9 - 0 - 4 mod 7 = 5
Y = 3(0-5) - 3 mod 7 = -4 = 3
	1-3 / 4-0 = -2 * 4^-1 mod 7 = -4 = 3

7 P = 6P + P
X = 0 - 0 - 5 mod 7 = -5 = 2
Y = 0(0-2) - 3 mod 7 = -3 = 4
	3-3 / 5-0 = 0

8 P = 7P + P
X = 16 - 0 - 2 mod 7 = 0
Y = 4(0-0) - 3 mod 7 = -3 = 4
	4-3 / 2-0 = 1 * 2^-1 mod 7 = 4

9 P = 8P + P	4-3 / 0-0 NEUTRAL ELEMENT

C) This alpha has an order of 9 and because it has the maximum order, it is also a primitive element.

Question 9:
a = 4, b = 20, p = 29

P	S (2P**) = 3(x)^2 +4 mod 29 * (2*y)^-1 mod 29
1 P = 8, 10	

2P = 2P
X = 16 - 8-8 mod 29 = 0
Y = 4(8-0)-10 mod 29 = 22
	3(64) + 4 mod 29 * 20^-1 mod 29
	22 * 16 mod 29 = 4

4P = 2(2P)
X = 64 - 0 - 0 mod 29 = 6
Y = 8(0-6)-22 mod 29 = 17
	4 mod 29 * (2*22)^-1 mod 29 or 15^-1 mod 29
	4 * 2 mod 29 = 8

8P = 2(4P)
X = 25 - 6- 6 mod 29 = 13
Y = 5(6-13)-17 mod 29 = 6
	3(36)+4 mod 29 * 2(17)^-1 mod 29
	25 * 6 mod 29 = 5

9P = 8P + P
X = 25 - 13 - 8 mod 29 = 4
Y = 5(8-4)-10 mod 29 = 10
K = 9, (4, 10)
	6-10 / 13-8 mod 29 = -4 * 5^-1 mod 29
	-4 * 6 = -24 mod 29 = 5

18P = 2(9P)
X = 400 - 4 - 4 mod 29 = 15
Y = 20(4-15)-10 mod 29 = 2
	3(16)+4 mod 29 * 20^-1 mod 29
	52 * 16 mod 29 = 20

20P = 18P +2P
X = 324 - 0 - 15 mod 29 = 19
Y = 18(0-19)-22 mod 29 = 13
K = 20, (19, 13)
	2-22 / 15-0 mod 29
	-20 * 2 mod 29 = 18

Question 10:
We basically have to calculate 6B since we TAB = aB and a = 6.
You receive Bob's public key B = (5,9). The elliptic curve being used is defined by y2 ≡ x3+x+6 mod 11.
a = 1, b = 6, p = 11

B	s
1 B = (5, 9)	
2B = 2(B) X = 9 - 5 -5 mod 11 = 10	3(25)+1 mod 11 * 18^-1 mod 11 10 * 8 = 80 mod 11 = 3

Y = 3(5-10)-9 mod 11 = 9	

4B = 2(2B)
X = 81 - 10 -10 mod 11 = 6
Y = 9(10-6)- 9 mod 11 = 5
	3(100)+1 mod 11 * 20^-1 mod 11
	4 * 5 mod 11 = 9

6B = 2B + 4B
X = 1 - 6 - 10 mod 11 = 7
Y = 1(6 - 7)- 5 mod 11 = 5
	9-5 / 10-6 mod 11 = 4 * 4^-1 mod 11
	4 * 3 mod 11 = 1

TAB = (7, 5)

Question 11:
Refer to the python file.