Homework #7

Case 1	Case 2	Case 3
11	37	59
6	11	15
	p and a are published	
4	13	17
5	9	20
9	11	35
10	36	7
	A and B exchange keys	
1	36	46
1	36	46

Case 1

A = α^a mod p→ 6^4 mod 11 = 9

B = α^b mod p→ 6^5 mod 11 = 10

Exchange public keys

A = 10^4 mod 11 = 1

B = 9^5 mod 11 = 1

Case 2

A = 11^13 mod 37 = 11

B = 11^9 mod 37 = 36

Exchange public keys

A = 36 ^13 mod 37

36^13 = -1^13 mod 37 → -1 ^13 = - mod 37

-1 +37 = 36 → 36^13 mod 37 = 36

B = 11^9 mod 37 = 36

Case 3

A = 15^17 mod 59 =35

B = 15^20 mod 59 = 7

Exchange keys

A = 7^17 mod 59 = 46

B = 35^20 mod 59 = 46

For the given three cases where Alice is trying to send encrypted data to Bob, and Bob is trying to decrypt it, using Elgamal encryption scheme, fill the values in the table.

Case 1	Case 2	Case 3
11	31	59
7	3	2
6	9	3
4	29	8
	p, a and B are sent to Alice	
4	5	7
3	26	10
3	6	56
7	7	9
10	11	56
	Alice sends kE and y to Bob	
3	30	56
	Verify Alice and Bod computed same key	
3	30	56
8	20	9

Case 1

P = 11, a = 7, d = 6, i = 4, x = 7

B = a^d mod p

7^6 mod 11 = 4

kE = α^i mod p → 7^4 mod 11 = 3

kM = B^i mod p → 4^4 mod 11 = 3

Alice encrypts

Y = x*kM mod p → 7 *3 mod 11 = 10

Bob computed

kM = kE ^ d mod p → 3^6 mod 11 = 3

Verify that Bob indeed computed the same KM

Km mod p → 3 mod 11 = 3

Y* kM mod p→ 10 * 3 mod 11 = 8

Case 2

P = 31, α = 3, d = 9, i = 5, x = 7

3^9 mod 31 =29

3^5 mod 31 = 26

29^5 mod 31 = 6

7*6 mod 31 = 11

Alice sends kE y to bob

26^9 mod 31 = 30

Verify that Bob indeed computed the same KM

30 mod 31 = 30

11 * 30 mod 31 = 20

Case 3

P = 59, α = 2, d = 3, I = 7, x = 9

B = 2^3 mod 59 = 8

2^7 mod 9 = 10

kM = B^i mod p → 8 ^7 mod 59 = 56

9 * 56 mod 59 = 56

10^3 mod 59 = 56→ 56 mod 59 = 56

56 * 56 mod 59 = 9