Problem 1

1. Possible element orders are factors of 42 which are less than or equal to half of 42. The orders would be: 1, 2, 3, 6, 7, 14, 21 and 42 if the element does not form a cyclic group. Below is a table of the number of elements for each order:
2.

Order	Number of elements
1	1
2	1
3	2
6	2
7	6
14	6
21	12
42	12

3. Order of all elements:

Order	Elements
1	1
2	42
3	6, 36
6	7, 37
7	4, 11, 16, 21, 35, 41
14	2, 8, 22, 27, 32, 39
21	9, 10, 13, 14, 15, 17, 23, 24, 25, 31, 38, 40
42	3, 5, 12, 18, 19, 20, 26, 28, 29, 30, 33, 34

4. 3, 5, 12, 18, 19, 20, 26, 28, 29, 30, 33, 34 are possible generators

Problem 2

a. X = 6
b. No solution
c. No solution
d. X = 11

Problem 3

P = 709
α = 2
Alice private key (A) = 17
Bob private key (B) = 41

Part a - Alice's Public Key

Private key (y_A) = $α^A$ mod P
= 2^{17} mod 709
= 616

Part b - Bob's Private Key

Private key (y_B) = $α^B$ mod P
= 2^{41} mod 709
= 323

Part c - Common Key

$z_A = z_B$

$z_A = {y_B}^A$ mod P
= 323^{17} mod 709
= 350
Check by finding z_B, which should be the same number:
$z_B = {y_A}^B$ mod P
= 616^{41} mod 709
= 350

Part d - Explain How Keys Are Established

Alice and Bob establish the key by multiplying the same exponents so that the results are equal. A is Alice's private key, B is Bob's private key, g is the generator, p is the prime.

Alice's public key: $K_A = g^A \bmod p$
Bob's public key: $K_B = g^B \bmod p$

When the two compute the common key:
Alice: $Z_A = K_B{}^A \bmod p = (g^B)^A \bmod p = g^{AB} \bmod p$
Bob: $Z_B = K_A{}^B \bmod p = (g^A)^B \bmod p = g^{AB} \bmod p$

Thus, $Z_A = Z_B$

Problem 4 - ElGamal Encryption

$F = \mathbb{Z}^*_{971}$
g = 314

Part a

Private key x = 23
Random parameter k = 21
Message m = 49

$\beta = g^x \bmod p$
$= 314^{23} \bmod 971$
= 865

Public key: (p, g, β) = {971, 314, 865}

Private key: (x) = {23}

Encryption:
$Y_1 = g^k \bmod p$
$= 314^{21} \bmod 971$
= 575

$Y_2 = m*\beta^k \bmod p$
$= 49*865^{21} \bmod 971$
= 751

Encryption: (Y_1, Y_2) = (575, 751)

Decryption

$m = Y_2 (Y_1^x)^{-1} \bmod p$
$= 751(575^{23})^{-1} \bmod 971$

Using Fermat's little theorem:
$575^{-23} = 575^{947}$
Since $x^{-p} \bmod q = x^{q-p-1}$
Same as taking multiplicative inverse of 575^{23}

947 in binary = 1110110011
Now use square and multiply to get:

$575^{947} \bmod 971 = 525$

$751(525) \bmod 971 = 49$

Message = 49

Part b

Private key x = 23
Random parameter k = 51
Message m = 49

$\beta = g^x \bmod p$
$= 314^{23} \bmod 971$
$= 865$

Public key: $(p, g, \beta) = \{971, 314, 865\}$

Private key: $(x) = \{23\}$

Encryption:

$Y_1 = g^k \bmod p$
$= 314^{51} \bmod 971$
$= 7$

$Y_2 = m*\beta^k \bmod p$
$= 49*865^{51} \bmod 971$
$= 285$

Encryption: $(Y_1, Y_2) = (7, 285)$

Decryption:

$m = Y_2 (Y_1^x)^{-1} \bmod p$
$= 285(7^{23})^{-1} \bmod 971$

Using Fermat's little theorem:
$7^{-23} = 7^{947}$
Since $x^{-p} \bmod q = x^{q-p-1}$
Same as taking multiplicative inverse of 7^{23}

947 in binary = 1110110011
Now use square and multiply to get:

$7^{947} \bmod 971 = 208$

$285(208) \bmod 971 = 49$

Message = 49