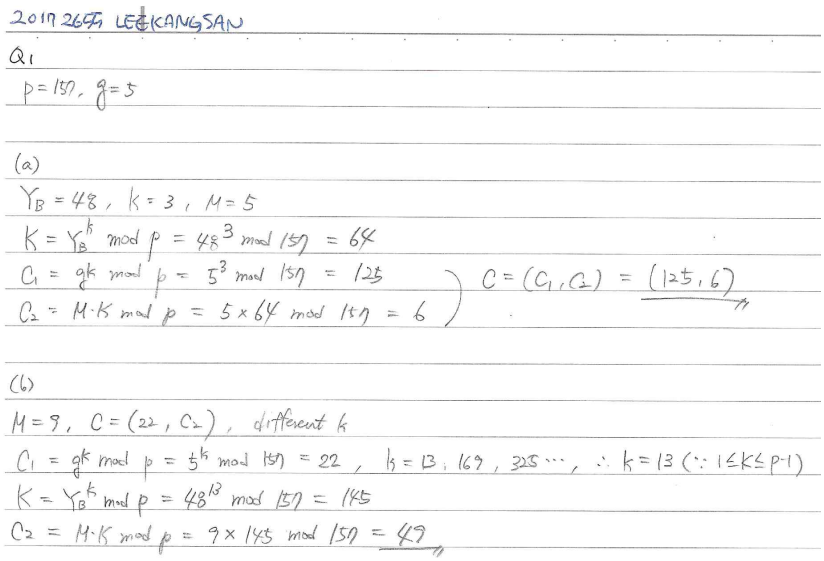
Assignment #4 – ElGamal, Elliptic Curve, Security Protocols (Total: 10 points)
name / student id : Kangsan Lee / 20172655

Q1. (2 points) Suppose Alice and Bob use an ElGamal scheme with a common prime q=157 and a primitive root α = 5.

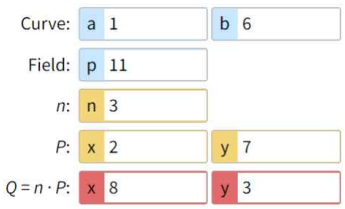
(a) If Bob has a public key Y_B=48 and Alice chose the random integer k=3, what is the ciphertext of M=5? (2 points)
answer) C=(125, 6)

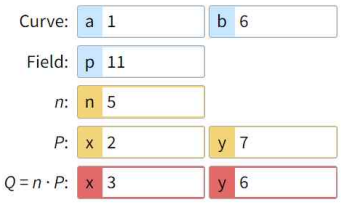
(b) If Alice now chooses a different value of k so that the encoding of M=9 is C=(22,C_2), what is the integer C_2?
answer) C_2=49

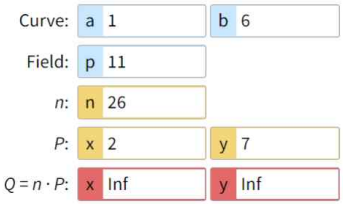


Q2. (4 points) Perform an elliptic curve encryption/decryption using the given parameters. Show all steps and tools used. The cryptosystem has parameters E_p(a,b)=E_11(1,6) where p is the common prime and G=(2,7). B's private key is n_B=7.

(a) Compute the multiples of G from 2G through 26G. (2 points)
a=1, b=6, p=11, G=(2,7), n=2to26
answer)
n=1=14) (2,7) / n=2=15) (5,2) / n=3=16) (8,3) / n=4=17) (10,2) / n=5=18) (3,6) / n=6=19) (7,9) / n=7=20) (7,2) / n=8=21) (3,5) / n=9=22) (10,9) / n=10=23) (8,8) / n=11=24) (5,9) / n=12=25) (2,4) / n=13=26) (infinity,infinity)

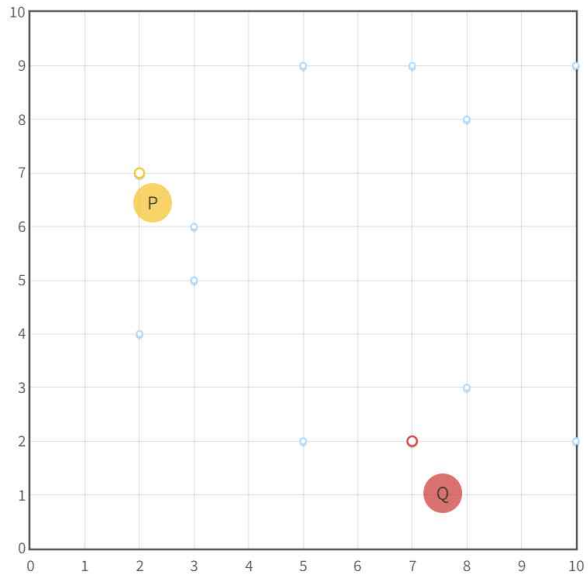


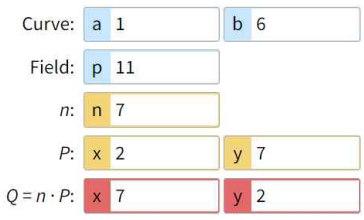




(b) Find B's public key P_B. (1 point)
answer) P_B=(7,2)

P_B=n_B*G=7*(2,7)



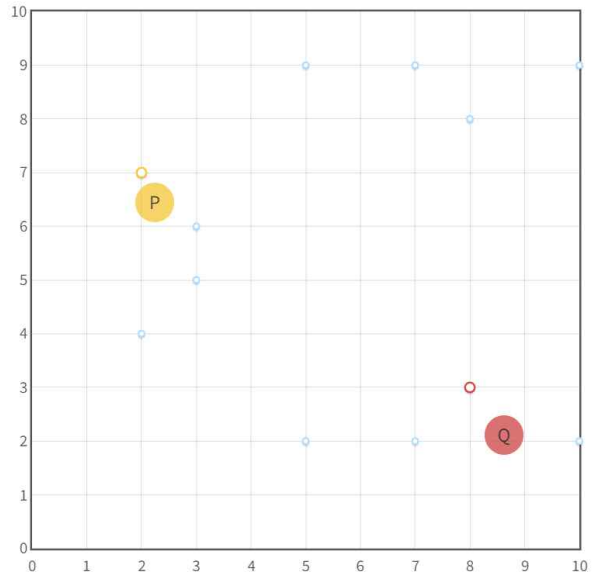


Scalar multiplication over the elliptic curve $y^2 = x^3 + 1x + 6$ in $\mathbb{F}_{11}$.
The curve has 13 points (including the point at infinity).
The subgroup generated by P has 13 points.

(c) Encrypt the message P_m=10 using the random value k=3 to generate the ciphertext C_m. (1 point)

answer) C_m=8

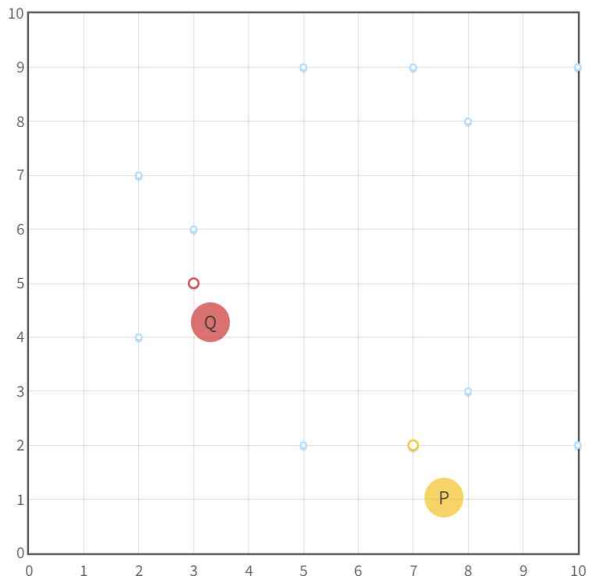
Temp Public Key R=k*G=3*(2,7)=(8,3)



Curve: a 1 b 6
Field: p 11
n: n 3
P: x 2 y 7
$Q = n \cdot P$: x 8 y 3

Scalar multiplication over the elliptic curve $y^2 = x^3 + 1x + 6$ in $\mathbb{F}_{11}$.
The curve has 13 points (including the point at infinity).
The subgroup generated by *P* has 13 points.

Shared Point S=k*P_B=3*(7,2)=(3,5)



Curve: a 1 b 6
Field: p 11
n: n 3
P: x 7 y 2
$Q = n \cdot P$: x 3 y 5

Scalar multiplication over the elliptic curve $y^2 = x^3 + 1x + 6$ in $\mathbb{F}_{11}$.
The curve has 13 points (including the point at infinity).
The subgroup generated by *P* has 13 points.

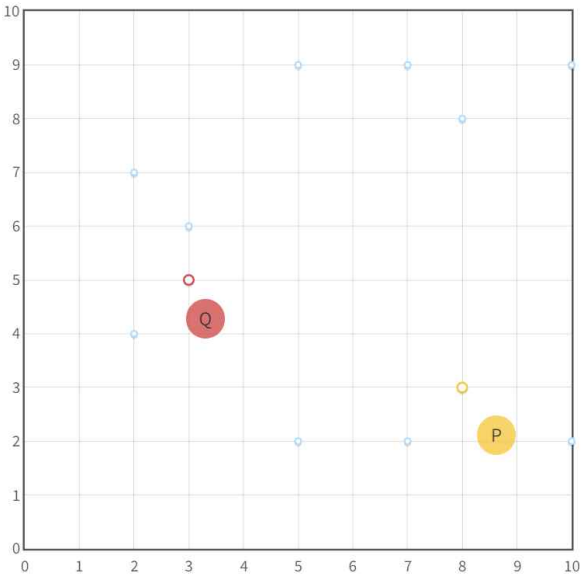
C_m = (SxP_m)mod p = (3,5)x10 mod11 = (30, 50) mod11 = (8, 6)
so C_m is 8.

(d) Show the calculation to recover P_m from C_m. (1 point)

answer)

S=n_B*R=7*(8,3)=(3,5)

P_m = (C_m x S^(-1)) mod p = (8x3^(-1)) mod 11 = (8x4) mod 11 = 10



Curve: a 1 b 6

Field: p 11

n: n 7

P: x 8 y 3

$Q = n \cdot P$: x 3 y 5

Scalar multiplication over the elliptic curve $y^2 = x^3 + 1x + 6$ in $\mathbb{F}_{11}$.

The curve has 13 points (including the point at infinity).

The subgroup generated by *P* has 13 points.

Q3. (2 points) The following is a new elliptic curve signature scheme. We have a global elliptic curve, prime p, and generator G. Alice picks a private signing key X_A and forms the public verifying key Y_A=X_AG. To sign the message M, Alice picks a value k and sends Bob M, k, and the signature S=M-kX_AG. Bob verifies that M=S+kY_A.

(a) Show that this new scheme works. That is, show that the verification process produces equality if the signature is valid.

answer) Since Bob received message M, value k, signature S = M - kX_AG from Alice so that Bob can verify M=S+kY_A that means S is valid.

M = S+kY_A <- Y_A = X_AG public key
= S+kX_AG <- S = M - kX_AG received from Alice
= M-kX_AG+kX_AG
= M

(b) Show that the new scheme is unacceptable by describing a simple technique that can forge a user's signature on an arbitrary message.

answer) The attacker could capture the M, k, S that Alice sends to Bob, then attacker could forge a fake signature.

Q4. (1 point) In quantum computing, what is a qubit? How is it different from bits?

answer) A bit only have two possible states 0 and 1, and state of a bit can only be either 0 or 1 at a time. On the other hand, A qubit can represent 0, 1, or a mixed state, called superposition which represents both 0 and 1 at the same time.

Q5. (1 point) What is a Heisenberg Uncertainty Principle? How is it used in the Quantum Key Distribution (QKD)?

answer) The Heisenberg Uncertainty Principle expresses that it is difficult to know the exact position and force of a quantum at the same time.

The QKD relies on the Heisenberg Uncertainty Principle and the bits of secret key are encoded in the polarization of the photons. Heisenberg Uncertainty Principle can be used to guarantee that an attacker cannot measure and transmit key without disturbing the photon's state.