UEE4611 Assignment #8 Solution

1. Alice and Bob use the Die-Hellman key exchange technique with a common prime $q = 23$ and a primitive root $\alpha = 5$.

(a) If Bob has a public key $Y_B = 10$, what is Bob's private key X_B? (5%)

(b) If Alice has a public key $Y_A = 8$, what is the shared key K with Bob? (5%)

(c) Show that 5 is a primitive root of 23. (5%)

(a)

$$Y_B = \alpha^{X_B} \mod q \Rightarrow 5^{X_B} \mod 23 = 10 \Rightarrow X_B = 3.$$

(b)

$$K = (Y_A)^{X_B} \mod 23 = 8^3 \mod 23 \Rightarrow K = 6.$$

(c)

$$\begin{aligned} 5^0 &= 1 \mod 23 \\ 5^1 &= 5 \mod 23 \\ &\vdots \\ 5^{22} &= 1 \mod 23 \end{aligned}$$

By Euler's Theorem, $5^{22} \equiv 1(\mod 23)$, so we only need to make sure that $5^2 \mod 23$ and $5^{11} \mod 23 \neq 1$, and it is true that both of them is not equal to 1, so we can get that 5 is a primitive root of 23.

2. Suppose Alice and Bob use an Elgamal scheme with a common prime $q = 157$ and a primitive root $\alpha = 5$.

(a) If Bob has public key $Y_B = 10$ and Alice chose the random integer $k = 3$, what is the ciphertext of $M = 9$? (5%)

(b) If Alice now chooses a different value of k so that the encoding of $M = 9$ is $C = (25, C_2)$, what is the integer C_2? (5%)

(a)

$$
\begin{aligned}
K' &= (Y_B)^k \mod q = 10^3 \mod 157 = 58 \\
C_2 &= 58 \times 9 \mod 157 = 51 \\
C_1 &= \alpha^k \mod q = 5^3 \mod 157 = 125 \\
&\Rightarrow \text{Ciphertext } C = (C_1, C_2) = (125, 51)
\end{aligned}
$$

(b)

$$
\begin{aligned}
C_1 &= 5^k \mod 157 = 25 \\
&\Rightarrow k = 2 \\
K' &= (Y_B)^k \mod q = 10^2 \mod 157 = 100 \\
C_2 &= 100 \times 9 \mod 157 = 115
\end{aligned}
$$

3. Given 5 as a primitive root of 23, solve the following congruence:

$$7x^{10} + 1 \equiv 0(\mod 23).$$

(10%)

$$
\begin{aligned}
&7x^{10} + 1 \equiv 0(\mod 23) \\
&\Rightarrow 7x^{10} \equiv 22(\mod 23)
\end{aligned}
$$

$$
\begin{aligned}
x^{10} \equiv& 22 \times 7^{-1} \equiv 13 \equiv 5^{14}(\mod 23) \\
\equiv& 5^{14}(5^{22})^3 \equiv 5^{80}(\mod 23)
\end{aligned}
$$

$$
\begin{aligned}
x \equiv& 5^8(\mod 23) \\
x \equiv& 16(\mod 23) \\
\Rightarrow x =& 16
\end{aligned}
$$

4. This problem performs elliptic curve encryption/decryption using the scheme outlined in Section 10.4. The cryptosystem parameters are $E_{11}(1,7)$ and $G = (3,2)$. B's private key is $n_B = 7$.

- **(a) Find B's public key P_B. (5%)**
- **(b) A wishes to encrypt the message $P_m = (10,7)$ and chooses the random value $k = 5$. Determine the ciphertext C_m. (5%)**
- **(c) Show the calculation by which B recovers P_m from C_m. (5%)**

(a)

$$P_B = n_B \times G = 7G = 7(3,2)$$

2G:

$$\begin{aligned}
m &= \frac{3 \times 9 + 1}{2 \times 2} = 7(\mod 11) \\
x_3 &= 49 - 3 - 3 = 43 \equiv 10(\mod 11) \\
y_3 &= 7(3 - 10) - 2 = -51 \equiv 4(\mod 11) \\
&\Rightarrow \text{2G} = (10, 4).
\end{aligned}$$

3G:

$$\begin{aligned}
m &= \frac{4 - 2}{10 - 3} = \frac{2}{7} \equiv 5(\mod 11) \\
x_3 &= 25 - 3 - 10 \equiv 12(\mod 11) \\
y_3 &= 5(3 - 1) - 2 \equiv 8(\mod 11) \\
&\Rightarrow \text{3G} = (1, 8).
\end{aligned}$$

4G:

$$\begin{aligned}
m &= \frac{3 \times 10^2 + 1}{2 \times 4} = \frac{301}{8} \equiv 6(\mod 11) \\
x_3 &= 36 - 10 - 10 = 16 \equiv 5(\mod 11) \\
y_3 &= 6(10 - 5) - 4 = 26 \equiv 4(\mod 11) \\
&\Rightarrow \text{4G} = (5, 4).
\end{aligned}$$

$$\begin{aligned}
\text{7G} &= \text{3G} + \text{4G} = (1, 8) + (5, 4). \\
m &= \frac{4}{-4} \equiv -1(\mod 11).
\end{aligned}$$

$$\begin{aligned}
x_3 &= 100 - 1 - 5 = 94 \equiv 6(\mod 11) \\
y_3 &= 10 \times 6 - 8 = 52 \equiv 8(\mod 11) \\
&\Rightarrow \text{7G} = (6, 8)
\end{aligned}$$

(b)

$$
\begin{aligned}
5\text{G} &= 3\text{G} + 2\text{G} = (1,8) + (10,4) \\
m &= \frac{8-4}{1-10} = \frac{4}{-9} \equiv 2 \pmod{11} \\
x_3 &= 4 - 10 - 1 = -4 \equiv 4 \pmod{11} \\
y_3 &= 2(10-4) - 4 = 2 \times 6 - 4 \equiv 8 \pmod{11} \\
&\Rightarrow 5\text{G} = (4,8).
\end{aligned}
$$

$$
\begin{aligned}
2(6,8) &= (6,8) + (6,8) \\
m &= \frac{3 \times 36 + 1}{2 \times 8} = \frac{109}{16} = \frac{10}{5} \equiv 2 \pmod{11} \\
x_3 &= 4 - 6 - 6 = -8 \equiv 3 \pmod{11} \\
y_3 &= 2(6-3) - 8 = 6 - 8 = -2 \equiv 9 \pmod{11} \\
&\Rightarrow 2(6,8) = (3,9).
\end{aligned}
$$

$$
\begin{aligned}
3(6,8) &= 2(6,8) + (6,8) = (3,9) + (6,8) \\
m &= \frac{9-8}{3-6} = \frac{1}{-3} = \frac{1}{8} \equiv 7 \pmod{11} \\
x_3 &= 49 - 6 - 3 = 40 \equiv 7 \pmod{11} \\
y_3 &= 7(6-7) - 8 = -15 \equiv 7 \pmod{11} \\
&\Rightarrow 3(6,8) = (7,7).
\end{aligned}
$$

$$
\begin{aligned}
5(6,8) &= 3(6,8) + 2(6,8) = (7,7) + (3,9) \\
m &= \frac{7-9}{7-3} = \frac{-2}{4} = \frac{9}{4} = 9 \times 3 \equiv 5 \pmod{11} \\
x_3 &= 25 - 3 - 7 = 15 \equiv 4 \pmod{11} \\
y_3 &= 5(3-4) - 9 = -14 \equiv 8 \pmod{11} \\
&\Rightarrow 5(6,8) = (4,8).
\end{aligned}
$$

$$
\begin{aligned}
(10,7) + 5(6,8) &= (10,7) + (4,8) \\
m &= \frac{8-7}{4-10} = \frac{1}{-6} = \frac{1}{5} \equiv 9 \pmod{11} \\
x_3 &= 81 - 10 - 4 = 67 \equiv 1 \pmod{11} \\
y_3 &= 9(10-1) - 7 = 81 - 7 = 74 \equiv 8 \pmod{11} \\
&\Rightarrow (10,7) + 5(6,8) = (1,8) \\
&\Rightarrow C_m = \{(4,8),(1,8)\}.
\end{aligned}
$$

(c)

$$
\begin{aligned}
P_m &= P_m + kP_B - n_B(kG) \\
P_m &= (1,8) - 7(5(3,2)) = (1,8) - 7(4,8)
\end{aligned}
$$

$$
\begin{aligned}
2(4,8) &= (4,8) + (4,8) \\
m &= \frac{3 \times 16 + 1}{2 \times 8} = \frac{49}{16} = \equiv 1 \pmod{11} \\
x_3 &= 1 - 4 - 4 = -7 \equiv 4 \pmod{11} \\
y_3 &= 1(4-4) - 8 = -8 \equiv 3 \pmod{11} \\
&\Rightarrow 2(4,8) = (4,3).
\end{aligned}
$$

$$
\begin{aligned}
3(4,8) &= 2(4,8) + (4,8) = (4,3) + (4,8) \\
&\text{Because } m \text{ goes to infinity.} \\
&\text{We have point}(0,0).
\end{aligned}
$$

$$
\begin{aligned}
4(4,8) &= 2(4,8) + 2(4,8) = (4,3) + (4,3) \\
m &= \frac{3 \times 16 + 1}{2 \times 3} = \frac{49}{6} = \frac{5}{6} = 5 \times 2 \equiv 10 \pmod{11} \\
x_3 &= 100 - 4 - 4 = 92 \equiv 4 \pmod{11} \\
y_3 &= 10(4-4) - 3 = -3 \equiv 8 \pmod{11} \\
&\Rightarrow 4(4,8) = (4,8).
\end{aligned}
$$

$$
\begin{aligned}
7(4,8) &= 3(4,8) + 4(4,8) = (0,0) + (4,8) = (4,8) \\
P_m &= (1,8) - (4,8) = (1,8) - (4,-8) = (1,8) + (4,3) \\
m &= \frac{3-8}{4-1} = \frac{-5}{3} = \frac{6}{3} \equiv 2 \pmod{11} \\
x_3 &= 4 - 1 - 4 = -1 \equiv 10 \pmod{11} \\
y_3 &= 2(1-10) - 8 = 2 \times (-9) - 8 = -26 \equiv 7 \pmod{11} \\
&\Rightarrow P_m = (1,8) + (4,3) = (10,7).
\end{aligned}
$$