## CS456 Cryptography: Elliptic Curve ElGamal (Solutions)

Bob is using an ELGAMAL probabilistic public-key cryptosystem on an elliptic curve $y^2 = x^3 + 4x + 34$ modulo $q = 43$. As his "generator", Bob used $G = (12, 41)$ and as the secret multiplier he used $N = 4$. This determines his public point $P = 4 * G = (31, 8)$. Bob then published his public keys $(q, A = 4, B = 34, G, P)$.

One day, Bob received from Alice the pair of points $C = (12, 2)$ and $H = (32, 32)$, where $C$ is the cipher and $H$ is the half-mask.

1. What is the value of the discriminant $\Delta$ of the curve?
2. Show how Bob recovers the full mask $F$ from the half-mask $H$. What is the value of $F$?
3. Show how Bob recovers the plaintext $M$ from $C$ and $F$. What is the value of $M$?
4. What is the value of $C + G$?
5. Is it true that $C = 2 * M$? If so, where does this place $M$ in the sequence generated by $G$?

Show all your work including any modular inverse computations (using the Pulverizer table), any point doublings, additions and multiplications on the elliptic curve.

**Answer:**

1. $\Delta = 4 \times A^3 + 27 \times B^2 = 35 \not\equiv 0 \pmod{43}$.
2. Bob needs to compute $F = 4 * H$, since $N = 4$ is his secret multiplier. Thus, Bob applies point doubling twice to $H = (32, 32)$.

   Let $H_1 = 2 * H$. Successively computing the slope $m$, the $x$-value and the $y$-value:

$$\begin{aligned} m &= \frac{3x_1^2 + A}{2y_1} = (3 \times 32^2 + 4)(2 \times 32)^{-1} = 23 \times 21^{-1} = 23 \times 41 = 40 \pmod{43} \\ x_3 &= m^2 - 2x_1 \equiv 40^2 - 2 \times 32 \equiv 31 \pmod{43} \\ y_3 &= y_1 + m(x_3 - x_1) = 32 + 40(31 - 32) \equiv 35 \pmod{43}. \end{aligned}$$

   Here is the Pulverizer table for $21^{-1} \equiv 41 \pmod{43}$:

| $\phi$ | $e$ | $Q$ | $R$ | $X_1$ | $Y_1$ | $X_2$ | $Y_2$ |
|---|---|---|---|---|---|---|---|
| 43 | 21 | 2 | 1 | 1 | 0 | 0 | 1 |
| 21 | 1 | 21 | 0 | 0 | 1 | 1 | -2 |

   So $\boxed{H_1 = (31, 8)}$ (since we need to reflect the $y$-value).

   Let $H_2 = 2 * H_1$. Successively computing the slope $m$, the $x$-value and the $y$-value:

$$\begin{aligned} m &= \frac{3x_1^2 + A}{2y_1} = (3 \times 31^2 + 4)(2 \times 8)^{-1} = 6 \times 16^{-1} = 6 \times 35 = 38 \pmod{43} \\ x_3 &= m^2 - 2x_1 \equiv 38^2 - 2 \times 31 \equiv 6 \pmod{43} \\ y_3 &= y_1 + m(x_3 - x_1) = 8 + 38(6 - 31) \equiv 4 \pmod{43}. \end{aligned}$$

   Here is the Pulverizer table for $16^{-1} \equiv 35 \pmod{43}$:

| $\phi$ | $e$ | $Q$ | $R$ | $X_1$ | $Y_1$ | $X_2$ | $Y_2$ |
|---|---|---|---|---|---|---|---|
| 43 | 16 | 2 | 11 | 1 | 0 | 0 | 1 |
| 16 | 11 | 1 | 5 | 0 | 1 | 1 | -2 |
| 11 | 5 | 2 | 1 | 1 | -2 | -1 | 3 |
| 5 | 1 | 5 | 0 | -1 | 3 | 3 | -8 |

So $\boxed{F = H_2 = (6, 39)}$ (since we need to reflect the $y$-value).

3. Bob computes $M = C + (-F)$ but $-F = (6, 4)$. Let $C = (x_1, y_1) = (12, 2)$ and $-F = (x_2, y_2) = (6, 4)$. Successively computing the slope $m$, the $x$-value and the $y$-value:

$$\begin{aligned}
m &= \frac{y_2 - y_1}{x_2 - x_1} = (4-2)(6-12)^{-1} = 2 \times 37^{-1} = 2 \times 7 = 14 \pmod{43} \\
x_3 &= m^2 - (x_1 + x_2) \equiv 14^2 - (12+6) \times 6 \pmod{43} \\
y_3 &= y_1 + m(x_3 - x_1) = 2 + 14(6-12) \equiv 4 \pmod{43}.
\end{aligned}$$

Here is the Pulverizer table for $37^{-1} \equiv 7 \pmod{43}$:

| $\phi$ | $e$ | $Q$ | $R$ | $X_1$ | $Y_1$ | $X_2$ | $Y_2$ |
|---|---|---|---|---|---|---|---|
| 43 | 37 | 1 | 6 | 1 | 0 | 0 | 1 |
| 37 | 6 | 6 | 1 | 0 | 1 | 1 | -1 |
| 6 | 1 | 6 | 0 | 1 | -1 | -6 | 7 |

So $\boxed{M = (6, 39)}$ (since we need to reflect the $y$-value).

4. Since $C = (12, 2)$ and $G = (12, 41)$, we have $C + G = \mathcal{O}$ (Point At Infinity).

5. Yes, $C = 2M$. Thus, $M$ should be in the middle of the sequence generated by $G$ (since $C + G = \mathcal{O}$).