Example (Cont.)

Let's modify ElGamal encryption by using the elliptic curve $E(Z_{11})$. Suppose that $\alpha = (2,7)$ and Bob's private key is 7, so

$$\beta = 7\alpha = (7,2)$$

Thus the encryption operation is

$$e_K(x,k) = \big(k(2,7), x + k(7,2)\big),$$

where $x \in E$ and $0 \le k \le 12$, and the decryption operation is

$$d_K(y_1, y_2) = y_2 - 7y_1.$$

Example (Cont.)

Suppose that Alice wishes to encrypt the plaintext x = (10,9) (which is a point on E).
If she chooses the random value k = 3, then

$$y_1 = 3(2,7) = (8,3) \text{ and}$$
$$y_2 = (10,9) + 3(7,2) = (10,9) + (3,5) = (10,2)$$

Hence $y = \big((8,3),(10,2)\big)$. Now, if Bob receives the ciphertext y, he decrypts it as follows: $x = (10,2) - 7(8,3) = (10,2) - (3,5)$

$$= (10,2) + (3,6) = (10,9)$$