# Analog of El Gamal

*Public Key:* $\mathbf{F}_q$, $E$, $B \in E$, $a_B B$

*Secret Key:* $a_B$

*Protocol:*
Alice has a message $P_m$ and choose a number $k$ by random. She sends

$$(kB, P_m + k(a_B B))$$

to Bob.

Bob calculates $a_B kB$ and subtracts this from $P_m + k(a_B B)$

# Analog of Diffie-Helman Key Exchange

*Public Key:* $\mathbf{F}_q$, $E$, $B \in E$

*Protocol:*
Alice chooses natural number $a$ by random and sends $aB \in E$ to Bob

Bob chooses natural number $b$ by random and sends $bB \in E$ to Alice

Alice computes $a(bB) \in E$ (the key)

Bob computes $b(aB) \in E$ (the key)

# Exercises

**Exercise 1:**
Consider Example 6.7 in [Stinson]. Show $4\alpha = (10, 2)$ in two different ways.

**Exercise 2:**
In this exercise we consider the analog of the Diffie-Helman key exchange.
Let $E$ be as in Example 6.7 of [Stinson], and let $B = (2, 7)$. Choose random numbers $a$ for Alice and $b$ for Bob. Exchange the key $abB$

**Exercise 3:**
In this exercise we consider the analog of ElGamal.
Let $E$ be as in Example 6.7 of [Stinson], and let $B = (2, 7)$. Choose, $P_m$, $k$ and $a_B$ and exchange information.