The Elgamal Public Key Cryptosystem

Say that Bob wants to send a message to Alice.

Step 1: Public Parameter Creation.

Choose and publish a large prime p and a primitive root g of p.

Step 2: Key Creation.

Alice chooses a secret integer a with $1 \leq a \leq p-2$ and computes

$$A \equiv g^a (\mathrm{mod}\, p).$$

Alice then publishes the public key A.

Step 3: Convert Message to Base 10

Bob takes his message and converts it to an integer m in base 10. Note that Bob's message must be small enough so that $2 \leq m \leq p-1$.

Step 4: Encrypt Message

Bob chooses any integer k, and computes two values

$$c_1 \equiv g^k (\mathrm{mod}\, p)$$

$$c_2 \equiv m A^k (\mathrm{mod}\, p).$$

Bob then sends (c_1, c_2) to Alice.

Step 5: Decrypt Message

Alice uses her private key a to compute

$$(c_1^a)^{-1} \cdot c_2 (\mathrm{mod}\, p).$$

Observe that this quantity is equal to m.

Step 6: Convert Message to Base 27

Alice takes the value m and converts it back to Base 27 to reveal the secret message.

Example 1. Let's say Bob and Alice choose the prime $p = 941$ and the primitive root $g = 627$. Show how Bob can send the secret message "hi" to Alice using Elgamal without Eve intercepting their message.