Cryptography: Homework 10

(Deadline: 10am, 2022/12/2)

1. (25 points) Let $G = \langle 3 \rangle$ be a subgroup of $\mathbb{Z}^*_{263819}$. The order of G is $q = 131909$. Let $pk = (q, G, 3, 36832)$ be the public key of ElGamal encryption. Decrypt the ciphertext $c = (102879, 19677)$.

2. (25 points) Let $N = 160693804425899027554196210541317559207570458201679629191838 3, e = 7$, and $d = 1147812888756421625387115789579028779196605802295573489640943$. In an RSA encryption with public key $pk = (N, e)$ and private key $sk = (N, d)$, decrypt the ciphertext $c = 11$. (**Hint**: Implement the square-and-multiply algorithm.)