Cryptography: Homework 9

(Deadline: 11:59am, 2019/11/27)

1. (30 points) Consider the following key-exchange protocol:

   (a) Alice chooses $k, r \in \{0,1\}^n$ uniformly, and sends $s = k \oplus r$ to Bob.

   (b) Bob chooses $t \in \{0,1\}^n$ uniformly, and sends $u = s \oplus t$ to Alice.

   (c) Alice computes $w = u \oplus r$ and sends w to Bob.

   (d) Alice outputs k and Bob outputs $w \oplus t$.

   Is the protocol correct? Is the protocol secure? Prove your answers.

2. (20 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 $c = (102879, 19677)$.