EE 720: An Introduction to Number Theory and Cryptography (Spring 2018)
Instructor: Saravanan Vijayakumaran
Indian Institute of Technology Bombay

Quiz 3 : 20 points April 20, 2018

1. (5 points) Let $p = rq + 1$ where p, q are primes. Then prove that

$$G = \left\{ h^r \bmod p \mid h \in \mathbb{Z}_p^* \right\}$$

is a subgroup of $\mathbb{Z}_p^*$ of order q.

2. (5 points) Consider the following key-exchange protocol:

   1. Alice chooses uniform $k, r \in \{0,1\}^n$, and sends $s = k \oplus r$ to Bob.
   2. Bob chooses uniform $t \in \{0,1\}^n$, and sends $u = s \oplus t$ to Alice.
   3. Alice computes $w = u \oplus r$ and sends w to Bob.
   4. Alice outputs k and Bob outputs $w \oplus t$ (which are the same).

   Show that an eavesdropper who **only** sees the messages being exchanged between Alice and Bob can recover the shared key k. You have to describe the procedure used by the eavesdropper.

3. (5 points) Suppose a message m is sent to three different receivers using plain RSA encryption. Three different moduli N_1, N_2, N_3 are generated (one per receiver) using **GenRSA** where the encryption exponent is fixed to $e = 3$ in all three cases. Assume that $m \in \mathbb{Z}_{N_1}^* \cap \mathbb{Z}_{N_2}^* \cap \mathbb{Z}_{N_3}^*$. Suppose an eavesdropper observes the ciphertexts c_1, c_2, c_3 sent to the three receivers. Describe an attack which can be used by the eavesdropper to recover m from c_1, c_2, c_3.

4. (5 points) Suppose Alice uses the plain RSA signature scheme to sign a message $m \in \mathbb{Z}_N^*$ where N is an RSA modulus. Suppose m represents the price Alice agrees to pay Bob for some goods. Given the resulting message-signature pair (m, σ), show how an adversary with access to a signing oracle can generate a valid signature for a different price $m' = km \bmod N$ for some integer $k > 1$.