CS 435: Introduction to Cryptography **Spring 2020**

Homework 7

Professor Somesh Jha **Due:** May 6

1. **Exercise 10.3**

   Describe a man-in-the-middle attack on the Diffie-Hellman protocol where the adversary shares a key k_A with Alice and a (different) key k_B with Bob, and Alice and Bob cannot detect that anything is wrong.

2. Consider the following public-key encryption scheme. The public key is $(\mathbb{G}, q, g, h)$ and the private key is x, generated exactly as in the El Gamal encryption scheme. In order to encrypt a bit b, the sender does the following:

   (a) If $b = 0$ then chose uniformly $y \in \mathbb{Z}_q$ and compute $c_1 := g^y$ and $c_2 := h^y$. The cipher text is $\langle c_1, c_2 \rangle$.

   (b) If $b = 1$ then choose independent uniform $y, z \in \mathbb{Z}_q$, compute $c_1 := g^y$ and $c_2 := g^z$ and set the ciphertext equal to $\langle c_1, c_2 \rangle$.

   Show that it is possible to decrypt efficiently given knowledge of x.

3. How can CRT be used to speed up RSA decryption?

4. **Exercise 10.4**

   Consider the following key-exchange protocol:

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

   (b) Bob chooses uniform $t \in \{0,1\}^n$, 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 $w \oplus t$.

   Show that Alice and Bob output the same key. Analyze the security of the scheme (i.e., either prove its security or show a concrete attack).