Homework 2

October 3 2018

Key-Exchange Protocol

1 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 $w \oplus t$.

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)

CPA-security of a Public-Key Encryption Scheme

2 Consider the following public-key encryption scheme for messages of a single bit. The public key is $(\mathbb{G}, q, g, h)$ and the private key is x, generated exactly as in the ElGamal encryption scheme. In order to encrypt a **bit** $b \in \{0, 1\}$, the sender does the following:

1. If $b = 0$ then sample a random $y \leftarrow \mathbb{Z}_q$ and compute $c_1 = g^y$ and $c_2 = h^y$. The ciphertext is (c_1, c_2).
2. If $b = 1$ then choose independent random $y, z \leftarrow \mathbb{Z}_q$, compute $c_1 = g^y$ and $c_2 = g^z$, and set the ciphertext as (c_1, c_2).

Show that we can efficiently decrypt the ciphertext given the private key x. Analyze the security of this scheme: If it is secure, give a formal proof of its security (i.e., proving this scheme is CPA-secure if the decisional Diffie-Hellman assumption is hard); if it is insecure, provide a concrete attack.

RSA

3 Suppose we have an adversary that wishes to decrypt a particular message $c = m^e \mod n$, intended for Alice. Assume that the adversary can query Alice with arbitrary ciphertexts (except c) and receive the corresponding plaintexts. Describe how Alice can decrypt the ciphertext c to get the corresponding m.

4 Bob decides to use RSA with $p = 11, q = 23$ and $e = 7$. Bob publishes $n = pq = 253$ and e as his public key.

1. Can you find Bob's private key d? (Hint : Use extended Euclidean algorithm)
2. Alice wants to send the message 44 to Bob. What is the encrypted message that Alice sends.
3. Suppose Bob receives from Alice the ciphertext 103. What was the original message that Alice sent.

ElGamal Encryption

5 Suppose Bob receives two ElGamal ciphertexts from Alice - $(B_1, C_1), (B_2, C_2)$. These are ciphertexts to two unknown messages M_1 and M_2. Bob knows Alice's public key A and the cyclic group generator g. What information can Bob infer about M_1 and M_2 if :

1. $B_1 = B_2$
2. $B_1 = g \cdot B_2$
3. $B_1 = (B_2)^2$