Problem Set 5

Due: Tuesday 12/13/2016, by 11pm (submit on courseworks). **No late days** allowed for this homework.

Note: this homework is shorter, and counts as half a homework. I added a couple of problems not for submission as extra practice.

1. Alice and Bob want to run the DH key exchange protocol. Alice generates the prime $p = 11$ (which satisfies $11 = 2 \cdot 5 + 1$), and the generator $g = 2$ (check that this is indeed a generator). Recall that for the protocol, they will work in the subgroup generated by $g^2$ (which is $QR_{11}$).

   (a) (5 points) Figure out (quickly) how many elements are in this subgroup, then calculate and write down all the elements in the subgroup.

   (b) (5 points) Describe an execution of the protocol where Alice chooses $x = 3$ and Bob chooses $y = 2$. Describe both Alice’s computations, and Bob’s computations in the protocol (as well as their outputs).

Do all your calculations by hand (and show them).

2. (a) (10 points) Consider the El-Gamal PKE scheme, and a given a ciphertext $(R, c)$ encrypting some unknown message $m$ (that is, $(R, c) := (g^y, h^y \cdot m)$). Prove that given the public key and the ciphertext $(R, c)$, it is possible in poly time to generate a ciphertext $(R', c')$ encrypting $am$ for any desired $a$, and such that $R' \neq R$ and $c' \neq c$.

   (b) (5 points) Conclude that El-Gamal is not CCA secure (prove how this follows from the above).

3. Consider the following RSA-based PKE scheme:

   - Gen$(1^n)$ runs GenRSA$(1^n)$ to obtain $(N, e, d)$, and sets $PK = (N, e), SK = (N, d)$.
   - Enc$_{N,e}(m)$ chooses $r \in \mathbb{Z}_N^*$ uniformly at random, and outputs $(r^e \mod N, r \oplus m)$.

   (a) (5 points) What is the appropriate decryption algorithm for correctness to be maintained?

   (b) (10 points) Is the scheme CPA secure? If your answer is yes, prove it under the RSA assumption. If your answer is no, construct an attack according to the security definition.

The rest of the problems are all **NOT for submission**, just for practice.

4. (answer the following without consulting with any textbook or other sources):

   Based on our discussions in class, provide a formal definition of security (against a passive adversary) for key exchange. Prove that DH KE satisfies this definition of security if we work in a group where the DDH assumption holds.
5. For any positive integer \( n \), recall that \( \mathbb{Z}_n^* \) is a group with respect to multiplication modulo \( n \) (and with identity element 1). We defined \( QR_n = \{ a \in \mathbb{Z}_n^* \mid \exists x \ a = x^2 \ (\text{mod} \ n) \} \). That is, \( QR_n \) is the set of all elements that have square roots modulo \( n \) (such elements are called quadratic residues).

(a) Prove that for all \( n \), \( QR_n \) is a subgroup of \( \mathbb{Z}_n^* \) (namely, it’s also a group with respect to the same operation).
   Specifically, you need to prove closure of \( QR_n \), identity is in \( QR_n \), and multiplicative inverses of each element in \( QR_n \) are also in \( QR_n \).

(b) Let \( p > 2 \) be a prime (recall that in this case \( \mathbb{Z}_p^* \) is cyclic), and let \( g \) be a generator of \( \mathbb{Z}_p^* \). Prove that \( QR_p \) is the group generated by \( g^2 \ (\text{mod} \ p) \) (namely, prove that \( a \in QR_p \) if and only if \( a \) is some power of \( g^2 \) modulo \( p \)).