Introduction to Cryptography: HW 4

1. Assume that a company called NSC ("No such Company") starts a web service such that given a cyclic group G and a generator g of group G, it calculates $DL_{g,G}(a)$ for any $a \in G$. Assume that you do not want the NSC to learn $DL_{g,G}(a)$. Devise a scheme such that you can use the NSC discrete logarithm service without letting NSC know which a you want to learn the discrete logarithm for.

2. Let p; q be distinct primes with $p = q = 3 \bmod 4$. Consider the following encryption scheme based on the quadratic residuosity assumption: the public key is $N = pq$ and to encrypt a 0 the sender sends a random quadratic residue, while to encrypt a 1 she sends a random non-quadratic residue with Jacobi symbol +1

   (a) Assuming that given N and an element a in Z_N^* with Jacobi symbol +1, predicting whether a is a quadratic residue or not is a trapdoor predicate. Prove that the above scheme is semantically secure public key encryption. (**Hint:** You can use any theorem from the book. Your proof should not be longer than 3 lines)

   (b) Assume that bit b_1 is encrypted as C_1 and bit b_2 is encrypted as C_2, show how to calculate $E(b_1 \oplus b_2)$ just using C_1 and C_2. (Note that you do not know b_1 or b_2)

   (c) Assume that you are given an encryption C of bit b. Show how to generate an another C' using C without knowing b such that C' is also an encryption of b.

3. Assume that you have given an algorithm A that can invert the RSA function with given N and public key e if the ciphertext C where $C = m^e \bmod N$ is an element of some set S. Assume that $|S|$ is small compared to Z_N^* (i.e., $\frac{|S|}{|Z_N^*|} = 0.01$). In other words, if $C \in S$, A will find the correct m such that $A(C) = C^d = m \bmod N$ else A will not be successful.

   (a) First show that if we can invert RSA function on C' for $C' = C.r^e \bmod N$ then we can invert C

   (b) Using the Question **??**, devise a randomized algorithm that uses the algorithm A as a subroutine to invert RSA on any ciphertext

C. (A is successful only if $C' \in S$, how to map given C to some $C' \in S$? Repeating may also help)

4. Consider the FDH-RSA signature scheme. Assume that Alice wants Bob to sign a message such that Bob does not have any idea about the message he signed. Devise a scheme such that given any message M, Alice generates some M', Bob returns $C' = M'^d mod N$ to Alice, and finally Alice applies some function g where $g(C') = H(M)^d \bmod N$. Precisely define how to generate M' such that Bob learns **nothing** about M or $H(M)$ from M'. Also define the function g and show that $g(C') = H(M)^d \bmod N$

5. Suppose Bob is using the ElGamal signature scheme. Bob signs m_1 and m_2 and gets signatures (r, s_1) and (r, s_2) (i.e., the same r occurs in both of them). Also assume that $gcd(s_1 - s_2, p - 1) = 1$.

   (a) Show how to efficiently compute k (as defined in class) given the above information

   (b) Show how to break the signature scheme completely using the given information