Introduction to Cryptography: HW 4 Solutions

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.
   Answer:
   Choose a random $r \in [0, \ldots |G|]$ and send $a.g^r$ to NSC. Note that $DL_{g,G}(a.g^r) = DL_{g,G}(a) + r \bmod |G|$. Since r is totally random NSC does not learn anything.

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)
   Answer:
   Note that under the trapdoor predicate assumption, we can directly use the Definition 7.7 and Claim 7.8 of the Goldwasser-Bellare book.

   (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)
   Answer:
   $E(b_1 \oplus b_2) = C_1.C_2 \bmod N$. Note that if both b_1 and b_2 is O. then both C_1 and C_2 is QR and $C_1.C_2$ is a QR. If $b_1 = 0$ then C_1 is QR and $b_2 = 1$ is QNR then $C_1.C_2$ is QNR. Similarly for $b_1 = 1$ and $b_2 = 0$. Also note that if $b_1 = b_2 = 1$ then both C_1 and C_2 are QNR. Since we know that $QNR.QNR$ is a QR.

(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.

Answer:
Let $C' = C.r^2 \bmod N$. Note that C' is QR iff C is a QR.

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

   Answer:
   Note that $C'^d = (C.r^e)^d = C^d.r \bmod N$. Therefore $C^d = r^{-1}C'^D \bmod N$. Also note that if r^{-1} does not exist, this implies $gcd(r, N) > 1$ and this means we can factor N.

   (b) Using the Question 3a, 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)

   Answer:
   Above algorithm works because C' is always in S and the loop

Algorithm 1 B uses A to invert RSA

```
C' ← C
if C is not in S then
  repeat
    C' ← C.r^e mod N
  until C' ∈ S
end if
return A(C')
```

will execute expectedly 100 times.

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 $C' = M'^d modN$ 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 $g(C') = H(M)^d \bmod N$
Answer:
Alice sends Bob $M' \leftarrow H(M).r^e \bmod N$ for random $r \in Z_N^*$ Bob returns $M'^d = H(M)^d.r \bmod N$. Alice sets the signature as $M'^d.r^{-1} \bmod N$. Since r is random, Bob does not learn anything about the message.

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
   Answer:
   Note that

$$\begin{aligned} s_1 - s_2 &= k^{-1}(H(m_1) - ar) - k^{-1}(H(m_2) - ar) \bmod (p-1) \\ &= k^{-1}(H(m_1) - H(m_2)) \bmod (p-1) \end{aligned}$$

   Since $gcd(k, p-1) = 1$ and $gcd(s_1 - s_2, p-1) = 1$, this implies that $gcd(H(m_1) - H(m_2), p-1) = 1$. Therefore

$$k = ((s_1 - s_2)(H(m_1) - H(m_2))^{-1})^{-1} \bmod p - 1$$

   (b) Show how to break the signature scheme completely using the given information
   Answer:
   Given k, s_1, m_1, we can retrieve a and sign any message we want.