89-656: Introduction to Cryptography
Exercise 5
Gilad Asharov
January 13, 2020
Due Date: January 19

Question 1. Fix $N$, and assume there exists an adversary $A$ running in time $t$ for which
$$\Pr[A([x^e \mod N]) = x] = 0.01,$$
where the probability is taken over random choice of $x \leftarrow \mathbb{Z}_N^*$. Show that it is possible to construct an adversary $A'$ for which
$$\Pr[A'([x^e \mod N]) = x] = 0.99.$$
The running time $t'$ of $A'$ should satisfy $t' = \text{poly}(|N|, t)$.

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

1. If $b = 0$ then choose a random $y \leftarrow \mathbb{Z}_q$ and compute $c_1 = g^y$ and $c_2 = h^y$. The ciphertext is $\langle c_1, c_2 \rangle$.
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 to $\langle c_1, c_2 \rangle$.

Show that it is possible to decrypt efficiently given the knowledge of $x$. Prove that this encryption scheme is CPA-secure if the decisional Diffie-Hellman problem is hard relative to $G$.

Question 3. For each of the following variants of the definition of security for signatures, state whether textbook RSA is secure and prove your answer:

1. In this first variant, the experiment is as follows: the adversary is given the public key $pk$ and a random message $m$. The adversary is then allowed the query the signing oracle once on a single message that does not equal $m$. Following this, the adversary outputs a signature $\sigma$ and succeeds if $\text{Vrfy}_{pk}(m, \sigma) = 1$. As usual, security is said to hold if the adversary can succeed in this experiment with at most negligible probability.

2. The second variant is as above, except that the adversary is not allowed to query the signing oracle at all.

Question 3. In addition to the regular requirements of security in encryption, the problem of anonymity is sometimes considered. Informally, an anonymous public-key encryption is one for which no efficient adversary can know under which public-key a ciphertext was generated (i.e., an encryption under Alice’s public key should look like an encryption under Bob’s public key).
1. Write a formal definition of security to capture this additional property.

2. Prove that ElGamal encryption meets your definition of security, when all parties' public keys use the same group parameters \((G, g, q)\).

3. Does RSA encryption also meet this definition? (Assume a secure version of RSA encryption, i.e., not plain RSA, and that a ciphertext is just a random element in \(\mathbb{Z}_N^*\)). Prove your answer.

**Question 4.** Say that three users have RSA public keys \(\langle N_1, 3 \rangle\), \(\langle N_2, 3 \rangle\) and \(\langle N_3, 3 \rangle\) (i.e., they all use \(e = 3\)). Consider the following method for sending the same message \(m\) to each of these parties: Choose a random \(r \leftarrow \mathbb{Z}_{N_i}^*\) and send to everyone the same ciphertext

\[
\langle [r^3 \mod N_1], [r^3 \mod N_2], [r^3 \mod N_3], H(r) \oplus m \rangle
\]

1. Show that this is insecure, and an adversary can recover \(m\) even when \(H\) is modeled as a random oracle.

2. Show a simple way to fix this scheme and obtain a CPA-secure scheme with a ciphertext of length \(3|m| + O(n)\).

3. Show a better approach that gives a ciphertext of length \(|m| + O(n)\).