دانشکده‌ی علوم ریاضی

مقدمه‌ای بر رمزنگاری		تحویل اصلی: ۵ بهمن ۱۳۹۹
	تمرین شماره ۵	
مدرّس: دکتر شهرام خزائی		*تحویل نهایی: ۱۲ بهمن ۱۳۹۹*

- Upload your answers on courseware with the name: StudentNumber.pdf
- Upload a PDF file. Image and zip formats are not accepted.
- Similar answers will not be graded.
- NO answers will be accepted via e-mail.
- You can't upload files bigger than 2 Mb, so you'd better type.
- Deadline time is always at 23:55 and will not be extended.
- You should submit your answers before soft deadline.
- You will lose 5 percent for each day delay if you submit within a week after soft deadline.
- You can not submit any time after hard deadline.
- This problem set includes 100 points.
- For any question contact Amirreza Akbari via `amrz.akbari@gmail.com`.

Problem 1

Consider the following public-key encryption scheme:
The public key is $(\mathbb{G}, q, g, h) \longleftarrow \mathcal{G}$ 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 $y \in \mathbb{Z}_q$ 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 $y, z \in \mathbb{Z}_q$, compute $c_1 := g^y$ and $c_2 := g^z$, and st the ciphertext equal to $\langle c_1, c_2 \rangle$.

Show that it is possible to decrypt efficiently given knowledge of x. Prove that this encryption scheme is CPA-secure if decisional Diffie-Hellman problem is hard relatove to $\mathcal{G}$. (20 Points)

Problem 2

Alice have an online movie store with movies $m_1, ..., m_n \in \mathcal{M}$. Bob wants to watch movie number $1 \leqslant i \leqslant n$ and to do this pays Alice for the movie (the price is the same for all movies); However, Bob doesn't want to reveal to Alice what is his desired movie. Similarly, Alice wants to make sure Bob gets exactly one movie. This online movie store need a protocol that show m_i to Bob and reveal nothing to Alice. So they decided to use the following protocol that use a group $\mathbb{G}$ of a prime number q with generator g:

1. First of all, Alice sends a random $v \overset{R}{\leftarrow} \mathbb{G}$ to Bob,

2. Bob chooses $\alpha \overset{R}{\leftarrow} \mathbb{Z}_q$ and sends $u \longleftarrow g^\alpha v^{-i} \in \mathbb{G}$ to Alice,

3. and at the end, for $k = 1,\ 2, ...,\ n$ Alice encrypts movie m_k using ElGamal public-key $u_k \leftarrow uv^k$ to obtain an ElGamal ciphertext c_k. She sends all n ElGamal ciphertexts $c_1,\ c_2,\ ...,\ c_n$ to Bob.

- Explain how Bob can recover his desired movie from the data it receives from Alice. (5 Points)

- Explain why nothing reveals to Alice. (10 Points)

- Explain why Bob learns nothing other than m_i if CDH is hard in $\mathbb{G}$. (15 Points)

Problem 3

An administrator comes up with the following key managment scheme; He generates an RSA modulus N and an element s in $\mathbb{Z}_N^*$. He then gives he i'th user secret key $s_i = s^{r_i}$ in $\mathbb{Z}_N$ where r_i is the i-th prime number.
Now, the administrator encrypts a file that is accssible to users i, j and t with the key $k = s^{r_i r_j r_t}$ in $\mathbb{Z}_N$. It is easy to see that each of the three users can compute k. For example, user i computes k as $k = (si)^{r_j r_t}$. The administrator hopes that other than users i, j and t, no other user can compute k and access the file. We want to show that this system is insecure by showing that any two colluding users can combine their secret keys to recover the master secret s and then access all files on the system. Suppose users 1 and 2 collude. Show how they can compute s from their secret keys s_1 and s_2. (25 Points)

Problem 4

Recall that an RSA public key consists of an RSA modulus N and an exponent e. One might be tempted to use the same RSA modulus in different public keys. For example, Alice might use $N, 3$ as her public key while Bob may use $N, 5$ as his public key. Alice's secret key is $d_a = 3^{-1} \mod \phi(N)$ and Bob's secret key is $d_b = 5^{-1} \mod \phi(N)$. In this question we will show that it is insecure for Alice and Bob to use the same modulus N. In particular, we show that either user can use their secret key to factor N. Alice can use the factorization to compute $\phi(N)$ and then compute Bob's secret key.

- As a first step, show that Alice can use her public key $\langle N, 3\rangle$ and private key d_a to construct an integer multiple of $\phi(N)$.

- Now that Alice has a multiple of $\phi(N)$ let's see how she can factor $N = pq$. Let x be the given muliple of $\phi(N)$. Then for any g in $\mathbb{Z}_{\mathbb{N}}^*$ we have $g^x = 1$ in $\mathbb{Z}_N$. Alice chooses a random g in $\mathbb{Z}_N^*$ and computes the sequence

  $$g^x, g^{\frac{x}{2}}, g^{\frac{x}{4}}, g^{\frac{x}{8}}, \ldots$$

  in $\mathbb{Z}_N$ and stops as soon as she reaches the first element $y = g^{\frac{x}{2^i}}$ such that $y \neq 1$ (if she gets stuck because the exponent becomes odd, she picks a new random g and tries again). It can be shown that with probability $\frac{1}{2}$ this y satisfies

  $$((y = 1 \mod p) \wedge (y = -1 \mod q)) \vee ((y = -1 \mod p) \wedge (y = 1 \mod q))$$

  How can Alice use this y to factor N? (25 Points)