دانشکده‌ی علوم ریاضی

رمزنگاری — تحویل اصلی ۱۷ بهمن

تمرین : سری ۴

مدرّس : دکتر شهرام خزائی — *تحویل نهایی ۲۴ بهمن*

- 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 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.
- **One problem is optional.**
- For any question contact Ali Adibifar via @Aliadibifar.

Problem 1

Consider the following variant of El Gamal encryption. Let $p = 2q + 1$, let $\mathbb{G}$ be the group of squares modulo p(so $\mathbb{G}$ is a subgroup of $\mathbb{Z}_p^*$ of order q), and let g be a generator of $\mathbb{G}$. The private key is $(\mathbb{G}, q, g, x)$ and the public key is $(\mathbb{G}, q, g, h)$, where $h = g^x$ and $x \in \mathbb{Z}_q$ is chosen uniformly. To encrypt a message $m \in \mathbb{Z}_q$, choose a uniform $r \in \mathbb{Z}_q$, compute $c_1 = g^r \bmod p$ and $c_2 = h^r + m \bmod p$, and let the ciphertext be (c_1, c_2). Is this scheme CPA-secure? Prove your answer.

Problem 2

Show that El Gamal encryption is not CPA-secure if the DDH assumption does not hold in the underlying group.

Problem 3

Suppose that we have a public-key encryption scheme, $\xi = (G, E, D)$ with message space $\mathcal{M}$. From this, we would like to build an encryption scheme with message $\mathcal{M}^2$. To this end, consider the following encryption scheme $\xi^2 = (G^2, E^2, D^2)$, where

- $G^2(1^n) := (pk_0, sk_0) \leftarrow G(1^n), (pk_1, sk_1) \leftarrow G(1^n),$

  then output $pk := (pk_0, pk_1)$ and $sk := (sk_0, sk_1)$

- $E^2(pk, (m_0, m_1)) := (E(pk_0, m_0)), (E(pk_1, m_1))$
- $D^2(sk, (c_0, c_1)) := (E(sk_0, c_0)), (E(sk_1, c_1))$

Show that ξ^2 is CPA secure, assuming ξ itself is CPA secure.

Problem 4

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

- If $b = 0$ then choose a uniform $y \in \mathbb{Z}_q$ and compute $c_1 = g^y$ and $c_2 = h^y$. The ciphertext is (c_1, c_2).
- If $b = 1$ then choose independent uniform $y, z \in \mathbb{Z}_q$, compute $c_1 = g^y$ and $c_2 = g^z$. The ciphertext equal to (c_1, c_2).

a) Show that with high probability we can decrypt the ciphertext efficiently given knowledge of x . Specifically, show how to decrypt a bit that is encrypted correctly.
b) Prove that this encryption scheme is CPA-secure if the decision Diffie-Hellman problem is hard relative to $\mathbb{G}$.

Problem 5

Suppose Alice and Bob live in a country with 50 provinces. Alice is in province $a \in \{1, \ldots, 50\}$ and Bob is in province $b \in \{1, \ldots, 50\}$. Alice wants to know if they are in the same province or not, and Bob wants to be sure that if they are not in the same province, Alice will not gain any additional information about Bob's province. Also, Bob should not gain any information about Alice's province. For this purpose, they execute the following protocol:

- They choose a group $\mathbb{G}$ of prime order p and a generator $g \in \mathbb{G}$.
- Alice chooses $x, y \in \mathbb{Z}_p$ randomly and independently, and sends the values $(A_0, A_1, A_2) = (g^x, g^y, g^{xy+a})$ to Bob.
- Bob chooses $r, s \in \mathbb{Z}_p$ randomly and independently, and sends the values $(B_1, B_2) = (A_1^r g^s, (\frac{A_2}{g^b})^r A_0^s)$ to Bob.

a) How can Alice find out if they are in the same province or not? If they are not, can she gain any further information about Bob's province?
b) Explain why Bob does not gain any information about Alice's province.

Problem 6

Let $\mathbb{G}$ be a cyclic group of prime order p with a generator $g \in \mathbb{G}$. Let n be a poly-bounded parameter. We define a hash function H defined over $(\mathbb{Z}_p^n, \mathbb{G})$. The hash function is parameterized by the group $\mathbb{G}$ and n randomly chosen group elements $g_1, \ldots, g_n \in \mathbb{G}$. For $(a_1, \ldots, a_n) \in \mathbb{Z}_p^n$, we define

$$H(a_1, \ldots, a_n) := g_1^{a_1}, \ldots, g_n^{a_n}$$

Prove that H is collision resistant under the DL assumption for $\mathbb{G}$.