دانشکده‌ی علوم ریاضی

مقدمه‌ای بر رمزنگاری	تحویل اصلی: ۱ خرداد ۱۴۰۰
مدرّس: دکتر شهرام خزائی	تحویل نهایی: ۸ خرداد ۱۴۰۰

تمرین شماره ۶

- 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 sets include 75 points.
- For any question contact Sara Sarfaraz via `sarassm60@gmail.com`.

Problem 1

(10 points) Consider the following key-exchange protocol:
(a) Alice chooses a random key k and a random string r both of length n, and sends $s = k \oplus r$ to Bob.
(b) Bob chooses a random string t of length n and sends $u = s \oplus t$ to Alice.
(c) Alice computes $w = u \oplus r$ and sends w to Bob.
(d) Alice outputs k and Bob computes $w \oplus t$.
Show that Alice and Bob output the same key. Analyze the security of the scheme (i.e., either prove its security or show a concrete break).

Problem 2

(20 Points) Prove that hardness of the CDH problem relative to $\mathcal{G}$ implies hardness of the discrete-logarithm problem relative to $\mathcal{G}$, and that hardness of the DDH problem relative to $\mathcal{G}$ implies hardness of the CDH problem relative to $\mathcal{G}$.

Problem 3

(25 points) Consider the following variant of El Gamal encryption. Let $p = 2q + 1$, let G be the group of squares modulo p(so G is a subgroup of $\mathbb{Z}_p^*$ of order q), and let g be a generator of G. The private key is (G, q, g, x) and the public key is (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 $c_1 = g^r$ mod 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 4

(20 points) 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 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 $c_2 = g^z$, and set 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 G.