دانشکده‌ی علوم ریاضی

مقدمه‌ای بر رمزنگاری	تحویل اصلی: ۲۲ دی ۱۳۹۹

تمرین شماره ۴

مدرّس: دکتر شهرام خزائی	تحویل نهایی: ۲۹ دی 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 120 points.
- For any question contact Aysan Nishaburi via aysannishaburi@gmail.com.

Problem 1

(20 Points) Let $\Pi_1 = (\text{Gen}_1, \text{Enc}_1, \text{Dec}_1)$ be a PKE scheme. Build a private-key encryption scheme $\Pi_2 = (\text{Gen}_2, \text{Enc}_2, \text{Dec}_2)$ such that:

(i) $\text{Gen}_2 := \text{Gen}_1$, that is, the single private key k of Π_2 is the pair (sk, pk) output by Gen_1.

(ii) $\text{Enc}_{2,(pk,sk)}(m) := (\text{Enc}_{1,pk}(m), \text{Enc}_{1,pk}(m))$, that is, encryption of a message m produces a ciphertext (c_0, c_1), where for c_0 and c_1, encryption is performed independently as in Π_1.

(iii) $\text{Dec}_{2,(pk,sk)}(c_0, c_1)$ is defined as follows: Let $m_0 := \text{Dec}_{1,sk}(c_0)$, $m_1 := \text{Dec}_{1,sk}(c_1)$. Then, $\text{Dec}_{2,(pk,sk)}(c_0, c_1)$ is defined as $\perp$ if $m_0 \neq m_1$, and as m_0 otherwise.

Prove or disprove that Π_2 is CCA-secure.

Problem 2

Let $E(k, m)$ be a block cipher where the message space is the same as the key space (e.g. 128-bit AES). Show an efficient algorithm for constructing collisions for f_1 and f_2:

(1) (10 Points) $f_1(x, y) = E(y, x) \oplus y$

(2) (10 Points) $f_2(x, y) = E(x, x \oplus y)$

Recall that the block cipher E and the corresponding decryption algorithm D are both known to you.

Problem 3

(20 Points) Let $\mathbb{G}$ be a cyclic finite group of order $2p$ where p is a prime. Show that the decisional Diffie Hellman problem does not hold in $\mathbb{G}$.

Problem 4

(a) (10 points) **Three-party Diffie-Hellman key exchange:** Suppose Alice, Bob, and Carole can authentically communicate through a public channel. Devise a protocol that enables them to establish a common secret key securely.

(b) (10 points) Generalise your solution with n parties by devising a protocol that works on $n-1$ messaging rounds (in each round, each participant broadcasts a message that s/he computes using the messages received during the previous rounds and every parties receives $n-1$ message from other parties).

(c) (10 points) Using a SKE scheme, devise a protocol with n participants with two rounds.

(d)* (10 points) There exists a protocol for three-party Diffie-Hellman key exchange with one messaging round. It was first described by Antoine Joux in 2000 and it uses a bilinear map. Provide a definition of a bilinear map and show how it can be used for such a protocol. What is the underlying hardness assumption for the security of the protocol?

Problem 5

(20 Points) Let $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ be a public key encryption scheme. An attractive way to perform a bidding is the following: the seller publishes a public key e. Each buyer sends through the net the encryption $\text{Enc}_e(x)$ of its bid x, and then the seller will decrypt all of these and award the product to the highest bidder.
One aspect of security we need from Enc() is that given an encryption $\text{Enc}_e(x)$, it will be hard for someone not knowing x to come up with $\text{Enc}_e(x+1)$ (otherwise bidder B could always take the bid of bidder A and make into a bid that is one dollar higher).
Show that if Π is CCA secure then there is no such algorithm, in the following sense: if M is any polynomial time algorithm, then

$$\Pr_{\substack{(e,d)\leftarrow \text{Gen}(1^n)\\ X\leftarrow_R \{0,10^6\}}}[\text{Dec}_d(M(e, \text{Enc}_e(x))) = x+1] < 10^{-6} + n^{-\omega(1)}$$