


دانشکده‌ی علوم ریاضی

رمز نگاری تحویل اصلی ۲۸ دی ۱۴۰۲

تمرین : سری ۵

مدرّس : دکتر شهرام خزائی *تحویل نهایی ۵ 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 can't upload files bigger than 1 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.
- For any question contact Hossein Hafezi via `contact@hosseinhafezi.com`.

Problem 1

Verify that the Pailler (Section 15.2) and Goldwasser-Micali (Section 15.4) cryptosystems are homomorphic.

Problem 2

A simple commitment scheme is a tuple of two algorithm (`Setup`, `Com`) as defined in section 6.6.5 of the textbook. Prove the following definition of a commitment scheme $\mathcal{C} = (\texttt{Setup}, \texttt{Com})$ satisfies the following properties.

- **Setup**: Given a security parameter λ, run $(\mathbb{G}, g, p) \leftarrow \text{GrGen}(\lambda)$. Assume GrGen always produces a prime p. Choose a random $a \in \mathbb{Z}_p$, compute $h = g^a \in \mathbb{G}$. The commitment key is $k = (g, h)$.
- **Com((g, h), m; r)**: Assume the message space is $\mathbb{Z}_p$. For a message m and a random $r \in \mathbb{Z}_p$, output $c \leftarrow g^m h^r$.

1. Show that the scheme is perfectly hiding under DDH assumption. (Hint: show that for any $m' \in \mathbb{Z}_p$ there exists a unique $r' \in \mathbb{Z}_p$ such that $c = g^{m'} h^{r'}$)
2. Show that the scheme is computationally binding, assuming the discrete log problem is hard for G. (Hint: use the fact that $c = g^m h^r = g^{m'} h^{r'}$, where having m, m', r, r' can be used to break discrete logarithm of h with base g)
3. Show that the commitment is additively homomorphic: given a commitment to $m \in \mathbb{Z}_p$ and a commitment to $m' \in \mathbb{Z}_p$, one can construct a commitment to $z = am + bm'$, for any a, $b \in \mathbb{Z}_p$ of his choice.

Problem 3

Suppose you see the encryption of messages m, $m + 1$ and $m + 2$ under textbook RSA with exponent 3. Show that you can recover m in polynomial time. Can there be such an attack on an public-key encryption scheme with indistinguishable encryptions?

Problem 4

Let $\Pi_1 = (\texttt{Gen}_1, \texttt{Enc}_1, \texttt{Dec}_1)$ and $\Pi_2 = (\texttt{Gen}_2, \texttt{Enc}_2, \texttt{Dec}_2)$ be two public-key encryption schemes for which it is known that at least one has indistinguishable encryptions. The problem is that you don't know which one is secure and which is not.

1. Show how to construct an encryption scheme Π that is guaranteed to have indistinguishable encryptions as long as at least one of Π_1 or Π_2 has indistinguishable encryptions. Try to provide a full proof of your answer. (Hint: Generate two plaintext messages from the original plaintext so that knowledge of either one of the parts reveals nothing about the plaintext, but knowledge of both does yield the original plaintext.)

2. Generalise this result to n public-key encryption schemes where at least one of them is secure and we do not know which one(s).