


دانشکده‌ی علوم ریاضی

مقدمه‌ای بر رمزنگاری تحویل اصلی: ۲۸ خرداد ۱۴۰۰

تمرین شماره ۸

مدرّس: دکتر شهرام خزائی *تحویل نهایی: ۴ تیر ۱۴۰۰*

- 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 50 points.
- For any questions contact Elahe Kooshafar via `cyberian.eli@gmail.com`.

Problem 1

(15 points) Suppose there are n people who hold numbers $x_1, x_2, ..., x_n$, respectively. They wish to calculate the sum of their numbers, although they do not trust each other. Construct a protocol to calculate the sum of their numbers without anyone gaining any information (about anyone else's number) beyond what the calculated sum dictates (Assume all of the parties will follow the protocol honestly).

Problem 2

(15 points) A commitment scheme enables Alice to commit to a value x and sends it to Bob. The scheme is hiding if the commitment does not reveal to Bob any information about the committed value x. At a later time, Alice may open the commitment by sending some information to Bob to convince him that the committed value is x. The commitment is binding if Alice cannot cheat to convince Bob that the committed value is some $x' \neq x$. Here is an example of a commitment scheme:

- Public values: A group G of prime order q and two generators $g, h \in G$.
- Commitment: To commit to a value $x \in Z_q$, Alice does the following: (1) she chooses a random $r \in Z_q$, (2) she computes $b = g^x h^r \in G$, and (3) she sends b to Bob as her commitment to x.
- Open: To open the commitment, Alice sends (x, r) to Bob. Bob verifies that $b = g^x h^r$.

Show that this scheme is hiding and binding.

Hint: To prove the hiding property, show that b reveals no information about x. In other words, show that given b, the committed value can be any element x in Z_q. You can do so by proving that for any $x \in Z_q$ there exists a unique $r \in Z_q$ so that $b = g^x h^r$. To prove the binding property, show that if Alice can open the commitment as (x', r'), where $x' \neq x$, then Alice can compute the discrete log of h base g. In other words, show that if Alice can find an (x', r') such that $b = g^{x'} h^{r'}$ and $x' \neq x$ then she can find the discrete log of h base g. Recall that Alice also knows the (x, r) used to create b.

Problem 3

(20 points) 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 G of prime order p and a generator $g \in G$.
- Alice chooses $x, y \in Z_p$ randomly and independently, and sends the values $\langle A_0, A_1, A_2 \rangle = \langle g^x, g^y, g^{xy+a} \rangle$ to Bob.
- Bob chooses $r, s \in Z_p$ randomly and independently, and sends the values $\langle B_1, B_2 \rangle = \langle A_1^r g^s, (\frac{A_2}{g^b})^r A_0^s \rangle$ 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.