Problems for week 5, Cryptography Course - TDA 352/DIT 250

General remarks on problems for the weekly problem session: Exercises will be classified in four different levels:

1. **Easy**: the exercise will require low numerical computations or it can be just a way to look back at the content of the lecture. Exercises of this level should easily be done with just *pen and paper* and are **important to pass** the exam.
2. **Medium**: the exercises will require some time to do (from 5 to 15 minutes each). Maybe a separate paper for some computation is needed! You need to study a bit to answer the questions. These exercises also **may appear** in the exam.
3. **Hard**: the exercises will require you to spend a lot of time doing numerical computations (and we highly recommend using a PC) **or** the questions are real challenge to see if you understood the course in depth. Some of these exercises **may appear** in the exam.
4. **Think**: problems that aim to using your imagination. You are invited to discussion with your colleagues/friends/family and find your best solutions. Generally, the exercises of this level do not take a lot of time in writing the solutions but they will let you think/discuss for (maybe) 30/40 minutes.

In this weekly exercise sheet: you will construct some secret sharing schemes, study hash functions and identification protocols.
Completing the ex. sheet: you will have a good understanding of hash function's theory, know how to build some secret sharing scheme and have some knowledge on identification protocols.

Easy

---

1. Prove that $g = 6$ is a generator of $\mathbb{Z}_{41}^*$.
2. Give the general definition of a Secret Sharing Scheme.
3. State the properties that a Secret Sharing Scheme needs to achieve.
4. Describe the properties of the Fiat-Shamir protocol.
5. Describe the general structure of a Σ-protocol.

Medium

---

6. Let us consider the Mignotte's SSS with $n = 4$ and $t = 1$. Let $m_1 = 3$, $m_2 = 4$, $m_3 = 5$, $m_4 = 7$. Let the secret be $s = 9$.
   (a) Check that the given values m_i make a Mignotte's series.
   (b) Compute the shares for the different parties.
   (c) Consider the shares s_1 and s_4. Reconstruct the original secret s using s_1 and s_4.
   (d) Consider the shares s_1, s_3 and s_4. Reconstruct the original secret s using s_1, s_3 and s_4.
7. *You may need a calculator to facilitate the computations.* Let us consider the Mignotte's SSS with $n = 4$ and $t = 2$. Let $m_1 = 6$, $m_2 = 11$, $m_3 = 13$, $m_4 = 19$. Let the secret be $s = 666$.
   (a) Compute the shares for the different parties.
   (b) Consider the shares s_1, s_3 and s_4. Reconstruct the original secret s.

8. Let us consider the Shamir SSS with $n = 2$ and $t = 1$. The dealer choose to work in $\mathbb{Z}_3$. The secret is $s = 1$ and the polynomial that he randomly generate is $f(x) = 1 + 2x$

   (a) Compute the shares for the two different parties.

   (b) Consider the shares s_1 and s_2. Reconstruct the original secret s.

9. Let us consider the Shamir SSS with $n = 4$ and $t = 2$. The dealer chooses to work in $\mathbb{Z}_7$. The secret is $s = 1$ and the polynomial that he randomly generates is $f(x) = 1 + 3x + 6x^2$

   (a) Compute the shares for the different parties.

   (b) Consider the shares s_1, s_2 and s_3. Reconstruct the original secret s.

10. Suppose that Netflix is using the Fiat-Shamir identification protocol (see slides for lecture 9) to log-in users (in this case the password is a number $x \in \mathbb{Z}_N$). Victor shows you what he claims is a transcript of a protocol run where Peggy has proved her knowledge of the secret x. However, you do not trust Victor; why will the transcript not convince you?

Hard

11. Let us consider a Secure Multi Party Computation (SMPC) protocol for addition between 2 parties. Every party will use a Shamir SSS with $n = 2$ and $t = 1$. The parties decide to work in $\mathbb{Z}_5$. The secrets are $s_1 = 1$ and $s_2 = 2$ and they want to compute the sum of the two values. The polynomials that they randomly generate are $f_1(x) = 1 + 3x$ for P_1 and $f_1(x) = 2 + x$ for P_2.

    (a) Compute all the different shares, i.e., $s_{1,1}, s_{1,2}, s_{2,1}, s_{2,2} \in \mathbb{Z}_5$

    (b) Compute the partial results a_1 and a_2

    (c) Compute the final result y of the multi-party computation, i.e., the sum $s_1 + s_2 = 3 \pmod 5$.

12. Alice and Bob have a shared secret k and have decided to use it in the following protocol, which enables Alice to identify Bob as the party at the other end.

    1. Alice picks a random bit string r and sends it as challenge to Bob.
    2. Bob responds with $r \oplus k$.

    Alice's and Bob's analysis of the protocol is this: The protocol does indeed provide identification, since Alice can check that the sender of message 2 knows k. It is also secure, since only random numbers are ever sent on the communication channel.

    (a) How does Alice check that the sender of message 2 knows k?

    (b) Do you agree with Alice and Bob about the security of their protocol? Motivate your answer!

Think

13. Alice and Bob have invented the following protocol for sending a message securely from A to B. The protocol is based on the ideas of the one-time pad, but without a common, shared secret. Instead, for each message, both A and B invent a random nonce and execute the following protocol to send message M from A to B

    $$\begin{array}{lll} 1. & A \to B & : \quad M_1 = M \oplus N_A \\ 2. & B \to A & : \quad M_2 = M_1 \oplus N_B \\ 3. & A \to B & : \quad M_2 \oplus N_A \end{array}$$

    Here, we extend our protocol notation to give names to an entire message $M_1 = \ldots$. Only the message in the right hand side is sent, but the left hand side can be used to refer to the message content in subsequent messages.

    (a) Show that B can recover M.

    (b) Is the system secure?