Problems for week 4, 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 define and use Diffie Hellman key exchange protocol, RSA, ElGamal encryption scheme
Completing the ex. sheet: you will be able to use and describe the most famous public key exchange protocols.

Easy

---

1. **Define** Unconditional, Computational and Provable security.
2. **Define** RSA encryption scheme.
3. **Define** ElGamal encryption scheme.
4. **Describe** the IND-CPA security game.
5. **Describe** the IND-CCA security game.

Medium

---

6. In an adaptive chosen ciphertext attack (IND-CCA), the Adversary wants to decrypt a message c and is allowed to ask for, and get, the decryption of *any* message *except* c. Show that both ElGamal and RSA are not secure against such an attack.
7. Use the extended Euclidean algorithm to show that 313 and 276 are relatively prime and find a solution x and y such that $313 \cdot x + 276 \cdot y = 1$.
8. Let $p = 13, q = 17$ be two primes and $N = p \cdot q$ be the RSA modulo. Consider as a public exponent, $e = 11$.
   - Compute the private exponent d
   - Encrypt the message $m = 2$
   - Decrypt the message $c = 126$
9. **Prove** that Textbook RSA is not CPA-secure.

10. **Describe** the Diffie Hellman (DH) key exchange protocol. Describe the Man-in-the-Middle attack against the DH key exchange protocol.
Consider $G = \mathbb{Z}_p^*$ with $p = 11$ and the generator $g = 2$. Simulate the DH protocol where you play Alice's role and want to communicate with Bob.
Bob will send you $B = g^b = 8$.

    - What is the common secret between you and Bob?
    - After a couple of months, you meet Bob that tells you that *"he never exchanged keys with you"*. You realize that in the key exchange between you and Charlie, there was a Man-in-the-Middle. How could you prevent this Man-in-the-Middle attack?

Hard

11. Textbook RSA is a deterministic encryption scheme, i.e., has the problem that a message encrypted several times for the same user always encrypts to the same ciphertext, which opens for attacks in situations where only a few messages are possible. In this exercise we study this property for the ElGamal encryption scheme. We first recall ElGamal encryption.

    The setting is $\mathbb{Z}_p^*$ for a large prime p where $p-1$ has a prime divisor q, i.e. $q|(p-1)$. Let g be a generator of the subgroup of order q of $\mathbb{Z}_p^*$. A community of users share parameters p, q and g. Typically, p is a 1024-bit number, while q has only 160 bits.

    Each user has a private key $x < q$ and a public key $X = g^x \bmod p$. To encrypt a message m for this user, the sender chooses a random number $y < q$ and encrypts the message as $(c_1, c_2) = (g^y, m \cdot X^y)$.

    Because of the random choice of y for each message, different encryptions of the same message will be different. However, there is another quantity involving only m and q that can be computed from the ciphertext. This gives the basis for attacks on this textbook version of ElGamal.

    (a) Show how to compute m^q given the encryption of m.
    (b) Given two messages m_1 and m_2 in $\mathbb{Z}_p^*$ with $m_1^q = m_2^q$, can one conclude that $m_1 = m_2$?

12. We consider an identification protocol based on the discrete log problem. The setting is some cyclic group G of prime order q with generator g. Peggy chooses a private key $x < q$ and has as public key $X = g^x$. The purpose of the following protocol is to convince Victor that Peggy knows x:

    1. Peggy chooses $r < q$ at random and computes $R = g^r$ and $S = g^{x-r}$. She sends R and S to Victor.
    2. Victor chooses a random bit b and sends to Peggy.
    3. If $b = 0$, Peggy sends $z = r$ to Victor; if $b = 1$ she sends $z = x - r$.

    (a) What computations will Victor now do to check Peggy's values?
    (b) Show that a *false* Peggy (i.e. someone who does not know x) can participate in this protocol and have probability 0.5 to pass Victor's check.
    (c) How would you extend the protocol so that Victor can be *reasonably* convinced that if Peggy passes, she really knows the secret x?

Think

13. **Why** in RSA encryption we consider $\mathbb{Z}_N^*$ with the multiplication $\cdot$ and not $\mathbb{Z}_N$ with the addition $+$?

14. Let N be the public RSA modulo and suppose that $\mathbb{Z}_N^*$ is cyclic. **How many** generator does $\mathbb{Z}_N^*$ have?
How are they connected to the Discrete Logarithm? We supposed that $\mathbb{Z}_N^*$ is cyclic, does this happen in reality? (*Hint:* think about *when* $\mathbb{Z}_N^*$ is cyclic with respect to N)

15. **Is it possible** to modify the Diffie Hellman key exchange protocol to work for a three party key exchange? [1]

[1] Here you can see that it is possible!