Introduction to Cryptography: Homework 9

November 24, 2021

Requirements about the delivery of this assignment:

- Submit a pdf-document via Brightspace;
- Make sure that you write both name and student number on all documents (not only in the file name).

Deadline: Monday, December 6, 17:00 sharp!

Grading: You can score a total of 100 points for the hand-in assignments. To get full points, please **explain all answers clearly and verify computations, e.g., concerning inverses**.

1. **Encoding messages in modular subgroups.** Consider the group $((\mathbb{Z}/9467\mathbb{Z})^*, \times)$, where 9467 is prime, and the generator $g = 3$, which generates a cyclic group $\langle 3 \rangle$ of prime order 4733. For this group, we consider a naive way to encode 13-bit message blocks. We first "convert" the bit string to an integer such that we obtain $m' \in (\mathbb{Z}/9467\mathbb{Z})^*$. A naive way to map the integer in the subgroup is by checking whether it is in $\langle 3 \rangle$ already, and otherwise increment it by 1, until it is. You can check whether an element $h \in (\mathbb{Z}/9467\mathbb{Z})^*$ is in $\langle 3 \rangle$ by checking whether $h^{4733} \equiv 1 \pmod{9467}$ holds. [Note that checking whether some element is in $\langle g \rangle$ in this way is only guaranteed to always work, because $(\mathbb{Z}/p\mathbb{Z})^*$ is such that $p = 2q+1$, where both p and q are prime. You may use a computer algebra system for this exercise, but show what queries you do.]

   (a) Is $m = 2211$ in $\langle 3 \rangle$?

   (b) Is $m = 111$ in $\langle 3 \rangle$?

   (c) Give the representation of $m = 133$ in $\langle 3 \rangle$.

   (d) Give the representation of $m = 136$ in $\langle 3 \rangle$.

   (e) Does each 13-bit message have a unique encoding in $\langle 3 \rangle$? Explain your answer.

2. **Generating domain parameters.** In the lecture, we have shown that $(\mathbb{Z}/p\mathbb{Z})^*$, where p is a large prime, is always cyclic, so it contains some generator g such that $\langle g \rangle = (\mathbb{Z}/p\mathbb{Z})^*$. Suppose p is such that there exists a large prime $q < p$ such that $q \mid p - 1$.

   (a) What is the order of $g^{\frac{p-1}{q}}$? [Hint: Make sure that you show why your choice is the smallest positive integer k for which $(g^{\frac{p-1}{q}})^k \equiv 1 \pmod{p}$ holds.]

   (b) Show how you can find a cyclic subgroup of $(\mathbb{Z}/p\mathbb{Z})^*$ with order q.

3. **ElGamal encyption with repeating secret ephemeral key** In this exercise, Alice and Bob decide to use ElGamal encryption to communicate with each other. We consider the cyclic group $G = (\mathbb{Z}/467\mathbb{Z})^*$, and the subgroup generated by $g = 3$ with order 233. Note that 467 and 233 are prime numbers. We assume that Bob's public key is $B = 38$.

   (a) Assume that Alice's secret ephemeral key is $a = 7$ and she wants to encrypt the message $M = 62$. Show that $(C, A) = (122, 319)$.

   Alice wants to reuse her secret ephemeral key a to encrypt another message M' which results into (C', A'). We, playing the role of an eavesdropper, intercept both (C, A) and (C', A').

   (b) Explain how we can conclude that Alice used the same secret ephemeral key a to ecrypt M'. [Hint: What does A' look like?]

   (c) Assume that we know the message M. Show how we can determine M' without knowing a.

   (d) Determine M' assuming that $(C', A') = (432, 319)$.

Hand-in assignment:

1. **(30 points) Merkle-Diffie-Hellman key agreement.** Alice and Bob want to share a key and they decide to use the Merkle-Diffie-Hellman key agreement. They have decided on the subgroup of $(\mathbb{Z}/5791\mathbb{Z})^*$, generated by $g = 137$ of order 193. (Observe that 5791 and 193 are prime numbers.) [You may use a computer algebra system for this exercise (a)-(c), but show what queries you do.]

   (a) Determine Alice's public key, given Alice's private key is $a = 567$. 5 pt

   (b) Using Bob's public key $B = 1262$, compute their shared secret. 5 pt

   (c) An eavesdropper Eve wants to find their shared secret. She has access to the generator $g = 137$ and both public keys. Eve decides to try to find Bob's private key and manages to find it with relative ease using brute force. Compute Bob's private key using brute force. [Hint: Work upwards from 1.] 15 pt

   (d) Explain that the private key that you found for Bob in (c) is unique. [Hint: What kind of group are we working in?] 5 pt

2. **(30 points) ElGamal encryption.** In this exercise, Alice and Bob decide to use ElGamal encryption to securely communicate with each other. We consider the cyclic group $G = (\mathbb{Z}/719\mathbb{Z})^*$, and the subgroup generated by $g = 3$ of order 359. Note that 719 and 359 are prime numbers. We consider messages m to be encoded so that their associated integral residue class $M \in \langle g \rangle$.

   (a) In Exercise 2, you have seen it is quite difficult to find a unique encoding for messages in the group $\langle g \rangle$. Suppose that $\text{enc}\colon G \to \langle g \rangle$ encodes messages given in G to an element in $\langle g \rangle$. On average, how many elements in G will be encoded as the same element in $\langle g \rangle$? 5 pt

   (b) With Bob's public key $B = 526$ and random ephemeral private key $a = 17$, encrypt the message $M = 96$, which Alice wants to send to Bob. 7 pt

   (c) Suppose that Bob receives the following ciphertext $(C, A) = (113, 375)$, and Bob's private key is $b = 13$. What was the original message? [Choose from the table below.] 8 pt

message m	encoding of message M
"Joan Daemen"	98
"Bart Mennink"	100
"Bobby Subroto"	104
"Jan Schoone"	108

   (d) Suppose you as Eve intercept another ciphertext, next to the $(C, A) = (113, 375)$ that Bob received from Alice (in exercise (c)). Let this other ciphertext be $(C', A') = (81, 375)$. What did Alice do wrong in using the ElGamal encryption scheme? Furthermore, show that Eve can obtain the second plaintext without knowing Bobs private key, given that she has access to the first plaintext. [Give the corresponding plaintext message.] 10 pt

3. (**40 points**) **ElGamal is secure if DDH is hard.** In this exercise, you will provide yourself with more insight as to why ElGamal encryption is secure if the DDH hardness assumption holds. As you have seen in the lecture, ElGamal is IND-CPA secure if an attacker cannot guess (with non-negligible advantage over random guessing) which of some given messages M_0 or M_1 was encrypted. Recall that the group that we work in is $\langle g \rangle \subset (\mathbb{Z}/p\mathbb{Z})^*$, where $\text{ord}(g) = q$. (Both p and q are prime numbers.) You will first show that, if you can solve the DDH problem, you can also break ElGamal.

   (a) Let the ciphertext (C, A) be given. We know that (C, A) is the form $(M \times g^{ab}, g^a)$, but we don't know the values of a and b. Explain why we can interpret $C = M \times g^{ab}$ as g^c for some $c \in \mathbb{Z}/q\mathbb{Z}$. 6 pt

   (b) Suppose that $M_0 = 1$ and M_1 is another element in $\langle g \rangle$. Show that if we can determine whether $c = ab$, then we can also determine which value is encrypted. [Hint: What does (C, A) look like if M_0 was encrypted?] 10 pt

(c) How many times do we have to solve the DDH problem to determine whether M_0 or M_1 was encrypted (and therefore successfully break ElGamal)? 5 pt

You will now show that, if you can break ElGamal encyrption, that you can also solve the DDH problem. Suppose you're given the triple $(A' = g^{a'}, B' = g^{b'}, C')$, for which you have to determine whether $C' = g^{a'b'}$ holds or not. You have access to an adversary $\mathcal{A}$ that can break ElGamal encryption with respect to IND-CPA security, i.e., it can determine with non-negligible advantage $\text{Adv}_{\mathcal{A}}$ whether some M_0 or M_1 was encrypted. You will use this adversary $\mathcal{A}$ to solve the DDH problem.

(d) Let M_0 and M_1 be two messages that were given to you by the adversary $\mathcal{A}$. Randomly choose $b \xleftarrow{\$} \{0,1\}$. Show that, if $C' = g^{a'b'}$, then $(M_b \times C', A')$ is a valid ElGamal encryption of M_b with public key B'. 7 pt

(e) Suppose that, if the ciphertext in (d) that you give to the adversary is valid, then the probability that the adversary $\mathcal{A}$ guesses correctly which message was encrypted is $\frac{1}{2} + \text{Adv}_{\mathcal{A}}$. If it is not valid, the adversary $\mathcal{A}$ guesses correctly with probability $\frac{1}{2}$. You decide that, if the adversary $\mathcal{A}$ guesses correctly, that you, adversary $\mathcal{B}$, determine that $C' = g^{a'b'}$ holds. Compute $\Pr[\mathcal{B} = 1 \mid C' = g^{a'b'}]$ and $\Pr[\mathcal{B} = 1 \mid C' \neq g^{a'b'}]$. 7 pt

(f) Compute your advantage $\text{Adv}_{\mathcal{B}}$. 5 pt