Problem sheet 10 for Course 02231, 2025

These practice problems have the purpose of helping you understand the material better and learning the skills that are necessary to analyze cryptographic constructions, and sometimes to prepare you for the next class. All answers should be supported by a written justification. To gauge whether a justification is sufficient, ask yourself if your peers would be convinced by it without additional explanations.

Exercise 1. (Computing Discrete Logarithms with smooth group order)

Let p be a prime and $g, h \in \mathbb{Z}_p^*$ where g has order $p-1$. This means that $g^{p-1} = 1 \bmod p$ while $g^x \neq 1 \bmod p$ for every $1 \leq x < p-1$.
Given p, g, h the discrete logarithm problem is to find the unique $a \in \mathbb{Z}_{p-1}$ such that $g^a = h \bmod p$.

For this exercise, let $p = 43$, $g = 12, h = 5$.

1. Try out all possible choices of a (e.g. using a Python script or Excel) to find the discrete logarithm. For an arbitrary p, how many multiplications modulo p would you have to do (in the worst case) to find a this way?
2. We observe that $p - 1 = 2 \cdot 3 \cdot 7$ and want to use this to simplify the computation of the discrete logarithm. Let $x = (p-1)/2, y = (p-1)/3, z = (p-1)/7$ and consider the elements g^x, g^y, g^z. What do you know about the order of these elements modulo p?
3. We can find the value $a \bmod 2$ by computing the discrete logarithm of h^x for the base g^x. Similarly, we can obtain $a \bmod 3$ from g^y, h^y and $a \bmod 7$ from g^z, h^z. Can you use this to find $a \in \mathbb{Z}_{42}$ more efficiently?
4. More generally, assume that $p - 1$ has ℓ prime factors that are all smaller than B. Can you (roughly) say how many multiplications modulo p you have to do, in comparison to the trivial method that tries out all choices of a, to recover the discrete logarithm?
5. Given the results of this exercise, what can you say about the security of the discrete logarithm in groups of smooth order (i.e. where the order of the group only has small prime factors)?

Exercise 2. (When the Decisional Diffie Hellman Problem is easy)

Let p be a prime. In the lecture, we considered the Decision Diffie Hellman (DDH) problem in the case when $g \in \mathbb{Z}_p^*$ was of large prime order q such that $q | p-1$. Now instead, assume that $g \in \mathbb{Z}_p^*$ is a generator of the whole group $\mathbb{Z}_p^*$.

Show that, in this case, the DDH problem is easy: one can distinguish tuples of the form $(g, g^a, g^b, g^{a \cdot b})$ for $a, b \in \mathbb{Z}_{p-1}$ from tuples of the form (g, g^a, g^b, g^c) for $a, b, c \in \mathbb{Z}_{p-1}$ with a very good chance. For this, use the observations from the previous exercise and consider what happens if you raise each element in the tuple to $(p-1)/2$.

Exercise 3. (**From Diffie Hellman to Public-Key Encryption**)

Let p be a prime and $g \in \mathbb{Z}_p^*$ be of large prime order $q|p-1$. In the Diffie Hellman Key Exchange Protocol, Alice and Bob exchange messages $A = g^a \bmod p, B = g^b \bmod p$ where $a, b \in \mathbb{Z}_q$.

1. Assume that Bob publishes the message B as a public key, while he keeps b as his secret key. Alice now encrypts a message $m \in \{0,1\}$ as follows:
   (a) She chooses $a \in \mathbb{Z}_q, r \in \mathbb{Z}_q^*$, and computes $c_1 = g^a \bmod p$.
   (b) If $m = 0$ then she sets $c_2 = B^a \bmod p$, otherwise she sets $c_2 = B^a \cdot g^r \bmod p$.
   (c) She lets c_1, c_2 be the ciphertext for Bob.

   Show how Bob can recover the message.
2. Show that this encryption scheme is IND-CPA secure assuming DDH is hard in the group $\mathbb{Z}_p^*$ with generator g. Namely, show that if there exists an attacker that wins the IND-CPA security game with probability $P > 1/2$, then we can use it to construct an algorithm that breaks DDH with the same probability.

Exercise 4. (**Bad groups for Diffie-Hellman**)

Explain in detail why the following groups are not suitable for use in the Diffie-Hellman key exchange protocol. Below, let p be a prime and let $(S_n, \circ)$ be the group of permutations of n objects ($\circ$ denotes composition of permutations).

1. $(\mathbb{Z}_p, +)$, i.e. the group of remainders modulo p with addition as group operation.
2. $\left(\left\{\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \middle| a \in \mathbb{Z}_p\right\}, \cdot\right)$ where $\cdot$ denotes matrix multiplication modulo p.
3. $(\langle g \rangle, \circ)$ for a full cycle $g \in S_n$[a]

[a] A full cycle is a permutation $g \in S_n$ where $\{1, g(1), g^2(1), \ldots\} = \{1, 2, 3, \ldots, n\}$ (as sets).