Problem Set 9

We will work on the following exercises together during the work sessions on Tuesday, 10 October 2017.

You are strongly encouraged to work together on the exercises, including the homework. You do not have to hand in solutions to these problem sets.

Problem 1: Modular roots

Show that the 7th root of 47 modulo 143 is $[47^{103} \mod 143]$. Note that $143 = 11 \cdot 13$.

Problem 2: Computing seemingly huge numbers by hand

Compute the final two (decimal) digits of 3^{1000} (by hand).

Hint: The answer is $[3^{1000} \mod 100]$. If $\gcd(a, b) = 1$, then $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$.

Problem 3: Easy discrete-logarithm problem.

Explain why the discrete-logarithm problem in the additive group $(\mathbb{Z}_N, +)$ generated by $\langle 1 \rangle$ is easy to solve.

Problem 4: Modular arithmetic.

Let p, N be integers with $p|N$. Prove that for any integer X,

$$[[X \mod N] \mod p] = [X \mod p]. \tag{1}$$

Show that, in contrast, $[[X \mod p] \mod N]$ need not equal $[X \mod N]$.

Problem 5: Computational Diffie-Hellman

Define the Computational Diffie-Hellman assumption. Show your answer to one of the teachers.

Problem 6: RSA

Let $N = pq$ be a RSA-modulus and let $(N, e, d) \leftarrow$ GenRSA. Show that the ability of efficiently factoring N allows to compute d efficiently.

Given

$$N = 214031067212049329336229845740265819265210841155431369578247592 7669427 \tag{2}$$

try to compute $\phi(N)$. If that takes too long compute $\phi(p \cdot q)$, where

$$p = 5824008035249052677649712288 5950201 \tag{3}$$
$$q = 3674978913433052912147339186 4214027. \tag{4}$$

Knowing that compute d for given N and $e = 11$. Is it

$$19457369746549939030566349612751437251474899315756889071017828886 41091? \tag{5}$$

★ **Problem 7: DDH is hard $\Rightarrow$ CDH is hard $\Rightarrow$ DLog is hard**

Prove that hardness of the CDH problem implies hardness of the discrete-logarithm problem, and that hardness of the Decisional Diffie-Hellman problem implies hardness of the CDH problem.