Modern Cryptography
Bachelor Computer Science, University of Amsterdam, 2017/18
teacher: Christian Schaffner, TA: Jan Czajkowski, Christian Majenz

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 $[3^{1000} \mod 100]$.