# Advanced Cryptography: Lightweight Cryptography

MICHAEL NÜSKEN, DANIEL LOEBENBERGER

## 0. Repetition sheet

**Exercise 0.1** (High powers). *Compute* $3^{98765432101}$ *in* $\mathbb{Z}_{101}$.

**Exercise 0.2.** *Daniel shows you his self-made random-number-generator which produces 16-bit numbers. But the distribution is not uniform! Daniel's favorite number is chosen with probability* $27/1024$ *– and you know that probability, but not the value of the number. How many calls to the random-number-generator do you expect to make, such that the favorite number occurs at least 9 times?*

**Exercise 0.3** (Reductions). *Consider some problems:*

**Problem** (RSA). *Given a number* $N$ *which is a product of two primes* $p$ *and* $q$ *(of approximately same size), a number* $e$ *coprime to* $\varphi(N) = (p-1)(q-1)$*, and a number* $y \in \mathbb{Z}_N^\times$*. Compute* $x$ *such that* $y = x^e$ *in* $\mathbb{Z}_N^\times$*.*

**Problem** (Factoring). *Given a number* $N$ *which is a product of at least two distinct primes compute all prime factors of* $N$*.*

**Problem** (CSAT). *Given a boolean formula* $\varphi(x_1, \ldots, x_n)$*. Find* $u_1, \ldots, u_n \in \{0, 1\}$ *such that* $\varphi(u_1, \ldots, u_n) = 1$*. [We consider* $1$ *as true and* $0$ *as false.]*

(i) *Reduce the RSA problem to factoring, ie. write down a program for the RSA problem using a subroutine for factoring. Make sure that the runtime of your reduction (counting the subroutine as one time step) is polynomial in the input size.*

(ii) *Reduce factoring to CSAT in polynomial time.*

**Exercise 0.4** (Block ciphers in ECB mode). *Consider the block cipher 3DES that uses three* $56$*-bit keys* $K_1, K_2, K_3$ *and encrypts a* $64$*-bit block by applying* $3DES_{K_1,K_2,K_3} = \mathrm{DES}_{K_1} \circ \mathrm{DES}_{K_2}^{-1} \circ \mathrm{DES}_{K_3}$ *on it (this is exactly the definition of Tripple DES with keying option 1 as specified in the NIST standard). Assume now that you plan to encrypt a very long UTF-16 encoded plaintext by grouping the text into blocks of four characters and encrypting each block with* $3DES_{K_1,K_2,K_3}$ *(this is called* electronic codebook mode*). Describe the major advantages and disadvantages of this approach.*