Exercise 17. Bob gets the message

(10101100011010001000011010010111001101110000110111100110111000001101110011011100011010001011011001101110000011011001, 1306)

from Alice. This message was encrypted with the Blum-Goldwasser Cryptosystem with the public key $n = 1333$. The number 1306 represents $x_{10}$. Decrypt this message.

Note: The security requirement to only use a maximum of $\log_2(\log_2(n))$ bits of the BBS generator is violated in this example. Instead, 5 bits of output are used.

Note: The letters of the alphabet $A, \ldots, Z$ are represented in the following way by 5 bits: $A = 00000$, $B = 00001$, $\ldots$, $Z = 11001$.

Exercise 18. The security of the Blum-Blum-Shub-generator is based on the difficulty to compute square roots modulo $n$, where $n = pq$ for two distinct primes $p$ and $q$ with $p, q \equiv 3 \pmod{4}$.

Design a generator for pseudorandom bits which is based on the hardness of the RSA-problem.

Exercise 19. Complete the proof of example 10.2 from the lecture notes: Show that from

$$k(x_1 - x'_1) \equiv x'_0 - x_0 \pmod{p - 1}$$

the discrete logarithm $k = \log_a b$ can be efficiently computed.