Exercise 16. Prove Proposition 9.13. of the lecture notes:
Let \( p > 3 \) be prime and \( g \) a primitive element modulo \( p \).
Then \( a \) is a quadratic residue \( \pmod{p} \) \( \iff \ a \equiv g^i \pmod{p} \) for some even integer \( i \).

Exercise 17. Establish a message decryption with the Goldwasser-Micali cryptosystem. Start by finding the cryptosystem’s parameters.

(a) Find a pseudo-square modulo \( n = p \cdot q = 31 \cdot 79 \) by using the algorithm from the lecture notes. Start with \( a = 10 \) and increase \( a \) by 1 until you find a quadratic non-residue modulo \( p \). For \( b \), start with \( b = 17 \) and proceed analoguously.

(b) Decrypt the ciphertext \( c = (1418, 2150, 2153) \).

Exercise 18.
Bob receives the following cryptogram from Alice:

\[(10101011100001101000101110010111, 1306)\]

The corresponding message has been encrypted using the Blum-Goldwasser cryptosystem with public key \( n = 1333 \). The number 1306 corresponds to the value \( x_{10} \) (cf. lecture notes). Decipher the cryptogram.

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.

Hint: The letters of the latin alphabet \( A, \ldots, Z \) are represented using the following 5 bit representation: \( A = 00000, B = 00001, \ldots, Z = 11001 \).

Exercise 19. The security of the Blum-Blum-Shub-generator is based on the intricacy 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.