Exercise 13.

Bob receives the following cryptogram from Alice:

\[(10101011100001101000101110010111100110111000, 1306)\]

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 14.

Consider the following function:

\[
h : \{0, 1\}^* \to \{0, 1\}^*, \quad k \mapsto ([10000((k)_{10}(1 + \sqrt{5})/2 - [(k)_{10}(1 + \sqrt{5})/2])]_2).
\]

Here, \([x]\) is the floor function of \(x\) (round down to the next integer smaller than \(x\)). For computing \(h(k)\), the bitstring \(k\) is identified with the positive integer it represents. The result is then converted to binary representation.

(example: \(k = 10011, (k)_{10} = 19\), \(h(k) = (7426)_2 = 1110100000010)\)

(a) Determine the maximal length of the output of \(h\).

(b) Give a collision for \(h\).

Exercise 15.

Consider the following functions. Check if they fulfil the necessary properties of hash functions.

(a) Let \(p\) a 1024 bit prime, \(a\) a primitive root modulo \(p\). Define \(h : \mathbb{Z} \to \mathbb{Z}_p^*, \ x \mapsto a^x \mod p\).

(b) Let \(g : \{0, 1\}^* \to \{0, 1\}^n\) a cryptographic hash function, \(n \in \mathbb{N}\). Define \(h : \{0, 1\}^* \to \{0, 1\}^{n+1}\) as follows: If \(x \in \{0, 1\}^n\), then \(h(x) = (1, x)\). In other cases, \(h(x) = (0, g(x))\).