Problem 4.

Alice and Bob use the ElGamal signature scheme to sign messages. In order to reduce the amount of computation, Alice signs $h(m)$ (instead of signing a message $m$ directly) with $h$ as hash function given by

$$h(m) = m(m + 3) \mod n,$$

with $n = uv$ and $u, v$ are prime numbers.

(a) List the four requirements that the function $h$ should fulfill to be used as cryptographic hash function.

(b) Is $h$ collision free in general?

Alice wants to sign $h(m)$ with $m = 83$ using the ElGamal signature scheme. She chooses the prime number $p = 101$ and the parameter $a = 7$.

(c) Calculate the hash value $h(m)$ given $u = 3$ and $v = 19$.

(d) Which condition must be fulfilled by $a$, to be used in the ElGamal signature scheme? Show that $a = 7$ fulfills this condition.

(e) Alice chooses the private key $x_A = 11$ and the random secret $k = 17$. Compute the signature $(r, s)$ of $h(m)$.

(f) Bob receives a signature $(r, s) = (120, 67)$ (this is not the signature from (e)). Is this signature valid?

Problem 5.

In the following, a certification and identification protocol is considered. It is an extension of the Fiat-Feige-Shamir protocol. It establishes authentication between $A$ and $B$ with the aid of a trusted authority server $T$. The utilized parameters are denoted as a public $n = pq$ of two secret, large primes $p, q$ with $p \neq q$, $A$’s private key $u \in \mathbb{Z}_n^*$, $A$’s public key $v \in \mathbb{Z}_n^*$, a random number $r \in \mathbb{Z}_n \setminus \{p, q\}$, a random number $c$ and a large publicly known exponent $e \in \mathbb{Z}_{\phi(n)}$. Furthermore, a signature algorithm $S_T$ used by $T$, a verification algorithm $V_T$, a signature $s$ and a public certificate $\text{cert}_T(A)$ issued by $T$ to $A$ are used.
Certification and Identification Protocol

(1) \(A\) computes \(v = (u^{-1})^e \pmod{n}\).
\(A \rightarrow T : v\)

(2) \(T\) computes \(s = S_T(A, v)\) and \(cert_T(A) = (A, v, s)\).
\(T \rightarrow A : cert_T(A)\)

(3) \(A\) chooses a random \(r \in \mathbb{Z}_n \setminus \{p, q\}\) and computes \(x = re \pmod{n}\).
\(A \rightarrow B : x, cert_T(A)\)

(4) \(B\) checks \(V_T(s)\) and matches \((A, v)\) from \(cert_T(A)\).
If both are valid, \(B\) chooses a random \(c \in \{1, \ldots, e\}\).
\(B \rightarrow A : c\)

(5) \(A\) computes \(y = r^c \pmod{n}\).
\(A \rightarrow B : y\)

(6) \(B\) verifies \(x \equiv y^e v^c \pmod{n}\).

Answer the following questions with respect to this protocol.

(a) What is the purpose of the certificate \(cert_T(A)\) in this protocol?
(b) Name the two number-theoretic problems this protocol relies on.
(c) Prove that the verification works.

(d) The security of this protocol also relies on cryptographically secure random numbers. Calculate the random sequence \(b_1, \ldots, b_t\) with the Blum-Blum-Shub Generator using \(x_0 = 29\), \(n = 13 \cdot 23\) and \(t = 5\). The given numbers are decimal. Is \(x_0 = 29\) a valid initial value? Reason your statement.

Problem 6.
Consider the equation
\[Y^2 = X^3 + X + 3.\]

(a) Show that this equation describes an elliptic curve \(E\) over the field \(\mathbb{F}_7\).
(b) Calculate all points on \(E(\mathbb{F}_7)\). What is the order of \(E(\mathbb{F}_7)\)?
(c) For each point on \(E(\mathbb{F}_7)\), calculate its inverse.
(d) For each point on \(E(\mathbb{F}_7)\), calculate its order.
(e) Is the group \(E(\mathbb{F}_7)\) cyclic?
(f) Find all solutions of the equation \(4P = O\) in \(E(\mathbb{F}_7)\).