Solution of Problem 1

Parameters: \( n = pq \) with \( p, q \equiv 3 \mod 4 \), and \( p, q \) secret primes.

Each user chooses an arbitrary sequence of seeds \( s_1, ..., s_K \in \{1, ..., n - 1\} \), with \( \gcd(s_i, n) = 1 \) and publishes: \( v_i = (s_i^2)^{-1} \mod n \).

A public hash function is applied:
\[
H : \{0, 1\}^* \to \{(b_1, ..., b_K) \mid b_i \in \{0, 1\}\}
\]

Signature generation:

(i) A chooses an arbitrary value \( r \in \{1, ..., n - 1\} \) and calculates \( x \equiv r^2 \mod n \). (witness)

(ii) A calculates:
\[
h(m, x) = (b_1, ..., b_K) \quad \text{(challenge)}
\]
and afterwards \( y \equiv r \prod_{j=1}^{K} s_{b_j}^j \mod n \) (response)

(iii) The signature of \( m \) is \( (x, y) \):
\[
A \to B : m, x, y
\]

Verification:

(i) B calculates \( h(m, x) = (b_1, ..., b_K) \). (challenge)

(ii) B calculates \( z \equiv y^2 \prod_{j=1}^{K} v_{b_j}^j \mod n \). (response)

(iii) B accepts the signature if \( z = x \) holds.

Proof that this signature and verification scheme is correct:
\[
z = y^2 \prod_{j=1}^{K} v_{b_j}^j \equiv y^2 \prod_{j=1}^{K} s_{b_j}^{2b_j} \prod_{j=1}^{K} v_{b_j}^j \equiv x \mod n. \quad \blacksquare
\]
Solution of Problem 2

a) The secret service (MI5) chooses an arbitrary seed \( s \in \mathbb{Z}_n \) per iteration.

The MI5 calculates the quadratic residue \( y \equiv s^2 \mod n \):

\[
\text{MI5} \rightarrow \text{JB}: y
\]

JB calculates the four square roots of \( y \) modulo \( n \) using the factors \( p, q \) of \( n \).

JB chooses a square root \( x \):

\[
\text{JB} \rightarrow \text{MI5}: x
\]

The MI5 verifies that \( x^2 \equiv y \mod n \).

Since JB has no information about \( s \), he chooses the \( x \) with probability \( \frac{1}{2} \), such that \( x \neq \pm s \mod n \).

If the MI5 receives such an \( x \), \( n \) can be factorized:

\[
y \equiv s^2 \equiv x^2 \mod n
\]

\[
\Rightarrow s^2 - x^2 \equiv 0 \mod n
\]

\[
\Rightarrow (s - x)(s + x) \equiv 0 \mod n.
\]

The probability that JB always fails by sending \( x \equiv \pm s \mod n \) in all 20 submissions is:

\[
\frac{1}{2^{20}} = \frac{1}{1048576} \approx 10^{-6}.
\]

b) Zero-knowledge property: No information about the secret may be revealed during the response.

However, in this protocol it is even possible, that the full secret \( s \) is revealed. Hence, this is not secure a zero-knowledge protocol!

c) A passive eavesdropper \( E \) can only obtain the values \( x \) and \( y \). \( E \) only knows the square roots \( \pm x \) of \( y \) modulo \( n \), which is useless in the next iteration. This knowledge is not sufficient to factorize \( n \).

Solution of Problem 3

By definition: \( E : Y^2 = X^3 + aX + b \) with \( a, b \in K \) and \( \Delta = -16(4a^3 + 27b^2) \neq 0 \) describes an elliptic curve.

a) Here: \( E : Y^2 = X^3 + X + 1 \), i.e., \( a = b = 1 \), \( K = \mathbb{F}_7 \). Then,

\[
\Delta = -16(4a^3 + 27b^2) = -16(4 + 27) \equiv 5 \cdot 3 \equiv 1 \neq 0 \mod 7.
\]

It follows that \( E \) is an elliptic curve in \( \mathbb{F}_7 \).

b) We use the following table to determine the points.

It follows from the third column that,

\[
Y^2 \in \{0, 1, 2, 4\} = A.
\]
and from the last column that
\[ 1 + X + X^3 \in \{1, 3, 4, 5, 6\} = B . \]

Furthermore,
\[ C = A \cap B = \{1, 4\} . \]

With \( Y^2 = 1 \Leftrightarrow Y \in \{1, 6\} \) and \( 1 + X + X^3 = 1 \Leftrightarrow X = 0 \)
\[ \Rightarrow (0, 1), (0, 6) \in E(\mathbb{F}_7) . \]

With \( Y^2 = 4 \Leftrightarrow Y \in \{2, 5\} \) and \( 1 + X + X^3 = 4 \Leftrightarrow X = 2 \)
\[ \Rightarrow (2, 2), (2, 5) \in E(\mathbb{F}_7) . \]

We can determine the set of all points on \( E , \)
\[ E(\mathbb{F}_7) = \{O, (0,1), (0,6), (2,2), (2,5)\} . \]

For the trace \( t \) it holds
\[ \#E(\mathbb{F}_q) = q + 1 - t . \]

Here, \( q = 7 \), and \( \#E(\mathbb{F}_7) = 5 \), so
\[ 5 = 7 + 1 - t \Leftrightarrow t = 3 . \]

\textit{Note (Hasse):} \( t < 2\sqrt{q} = 2\sqrt{7} \approx 5.3 \)

\textbf{c) With the group law addition,} \( E(\mathbb{F}_7) \) \textit{is a finite abelian group. It holds ord}(P) | \#E(\mathbb{F}_7) \)
(Lagrange’s theorem). It follows for \( P \neq O : 1 < \text{ord}(P) = 5 \), i.e., every \( P \neq O \) is a generator. The addition for \( P = (x, y) , P_1 = (x_1, y_1) , P_2 = (x_2, y_2) \) is defined by

(i) \( P + O = P \)
(ii) \( P + (x, -y) = O \Rightarrow -P = (x, -y) \)
(iii) If \( P_1 \neq \pm P_2 \Rightarrow P_3 = (x_3, y_3) = P_1 + P_2 \) with \( z = \frac{y_2 - y_1}{x_2 - x_1} , x_3 = z^2 - x_1 - x_2 , y_3 = z(x_1 - x_3) - y_1 . \)
(iv) If \( P_1 \neq -P_1 \Rightarrow 2P_1 = P_1 + P_1 = (x_3, y_3) \) with \( c = \frac{3x_1^2 + a}{2y_1} , x_3 = c^2 - 2x_1 , y_3 = c(x_1 - x_3) - y_1 . \)
Start with $P = (0, 1)$.

$2P = 2 \cdot (0, 1) \overset{(iv)}{=} (2, 5)$

using $c = \frac{1}{2} = 2^{-1}$ Table 4 $\Rightarrow x_3 = 4^2 \equiv 2 \Rightarrow y_3 = 4(-2) - 1 \equiv 5 \mod 7$

$3P = (2, 5) + (0, 1) \overset{(iii)}{=} (2, 2)$

using $z = \frac{-4}{-2} = 4 \cdot 2^{-1} = 2 \Rightarrow x_3 = 4 - 0 - 2 = 2$

$\Rightarrow y_3 = 2(2 - 2) - 5 \equiv 2 \mod 7$

$4P = (2, 2) + (0, 1) = (0, 6)$

$5P = (0, 6) + (0, 1) \overset{(ii)}{=} O$

$6P = O + (0, 1) \overset{(i)}{=} (0, 1)$