Problem 1 Let $n = 2465$.

a) Use a fast modular exponentiation algorithm to compute $3^{(n-1)/2} \bmod n$, showing that the result is 1.

b) Compute the Jacobi symbol $\left(\frac{3}{n}\right)$. Use the result together with the result from the previous problem to explain why n is not prime.

c) Compute $3^{(n-1)/4} \bmod n$ and use the result to find a proper factor of n.

Problem 2 Let $E : Y^2 = X^3 + X + 20$ be an elliptic curve defined over $\mathbb{F}_{79}$. Let $P = (62, 15)$ and $Q = (33, 19)$ be points on the curve.

a) Given that $\log_P Q \leq 5$, find $\log_P Q$.

Hint: $30^{-1} = 29$, $23^{-1} = 55$, $50^{-1} = 49$.

b) You have been told that P has prime order less than 11. Explain why P has order 7.

You have also been told that there is a point R on the curve of order 11. How many $\mathbb{F}_{79}$-rational points are there on the curve?

c) There are points S, T on the curve such that $11S = P$, $11T = Q$, $7S = 3R$ and $7T = 8R$. Find $\log_S T$.

Problem 3 Lattices are becoming more important for cryptography. The following problems consider the basic mathematics of lattices and applications in cryptography.

Let $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k \in \mathbb{R}^n$, $k \leq n$, be linearly independent vectors. The *lattice* generated by $\{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k\}$ is the set

$$\Lambda = \{\sum_i a_i \mathbf{b}_i \mid a_i \in \mathbb{Z}\}.$$

The set $\{\mathbf{b}_1, \ldots, \mathbf{b}_k\}$ is a *basis* for Λ. If $k = n$, then Λ is a *full rank* lattice.

If we let B be the $k \times n$ matrix where the rows are the vectors $\mathbf{b}_1, \ldots, \mathbf{b}_k$, we see that

$$\Lambda = \{\mathbf{a}B \mid \mathbf{a} \in \mathbb{Z}^k\}.$$

We say that B *generates* Λ.

a) Suppose B and B' are $n \times n$ invertible matrices that generate the same lattice Λ. Show that there exists an invertible matrix U with integer entries such that $B' = UB$.

For $\mathbf{z} \in \mathbb{R}^n$, the *closest lattice point* is a vector $\mathbf{y} \in \Lambda$ such that for all $\mathbf{x} \in \Lambda$, $\|\mathbf{z}-\mathbf{x}\| \geq \|\mathbf{z}-\mathbf{y}\|$. The distance from $\mathbf{z}$ to the closest lattice point is an important notion.

For $z \in \mathbb{R}$, let $\lfloor z \rceil$ be the integer closest to z (with halves rounding upwards). For $\mathbf{z} = (z_1, z_2, \ldots, z_n) \in \mathbb{R}^n$, let $\lfloor \mathbf{z} \rceil = (\lfloor z_1 \rceil, \ldots, \lfloor z_n \rceil) \in \mathbb{Z}^n$.

It can be shown that if $\mathbf{b}_1, \ldots, \mathbf{b}_n$ is a "nice" basis, there exists a number $\delta > 0$ such that when the distance from $\mathbf{z}$ to its closest lattice point is less than δ, then $\lfloor \mathbf{z}B^{-1} \rceil B$ *is* the lattice point closest to $\mathbf{z}$.

Let $(\mathcal{K}_s, \mathcal{P}, \mathcal{C}, \mathcal{E}_s, \mathcal{D}_s)$ be a symmetric cryptosystem, and let $h : \mathbb{R}^n \times \mathbb{R}^n \to \mathcal{K}_s$ be a hash function. Consider the following three algorithms:

$\mathcal{K}$ Choose a "nice" basis for a full rank lattice Λ, and let B be the corresponding matrix. Choose an invertible matrix U with integer entries and let $B' = UB$. The public encryption key is $ek = B'$, the private decryption key is $dk = (B, U)$.

$\mathcal{E}$ To encrypt a message $m \in \mathcal{P}$ using the encryption key B', choose vectors $\mathbf{a} \in \mathbb{Z}^n$ and $\mathbf{e} \in \mathbb{R}^n$ such that $\|\mathbf{e}\| < \delta$. Let $\mathbf{x} = \mathbf{a}B' + \mathbf{e}$ and

$$w = \mathcal{E}_s(h(\mathbf{a}, \mathbf{e}), m).$$

$\mathcal{D}$ To decrypt a ciphertext $(\mathbf{x}, w)$ using the decryption key (B, U), let $\mathbf{d} = \lfloor \mathbf{x}B^{-1} \rceil U^{-1}$ and

$$m = \mathcal{D}_s(h(\mathbf{d}, \mathbf{x} - \mathbf{d}UB), w).$$

b) Show that $(\mathcal{K}, \mathcal{E}, \mathcal{D})$ is a public key encryption scheme.