Exercise 1. An archaeologist found a secret entrance to an ancient English pyramid. The inscription of the massive door reveals:

<table>
<thead>
<tr>
<th>A</th>
<th>I</th>
<th>V</th>
<th>Z</th>
<th>Z</th>
<th>Q</th>
<th>U</th>
<th>V</th>
<th>K</th>
<th>V</th>
<th>Q</th>
<th>Q</th>
<th>V</th>
<th>I</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>8</td>
<td>21</td>
<td>25</td>
<td>25</td>
<td>16</td>
<td>20</td>
<td>21</td>
<td>10</td>
<td>21</td>
<td>16</td>
<td>16</td>
<td>21</td>
<td>8</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Z</th>
<th>W</th>
<th>F</th>
<th>S</th>
<th>E</th>
<th>H</th>
<th>Q</th>
<th>J</th>
<th>J</th>
<th>A</th>
<th>V</th>
<th>S</th>
<th>B</th>
<th>V</th>
</tr>
</thead>
<tbody>
<tr>
<td>25</td>
<td>22</td>
<td>5</td>
<td>18</td>
<td>4</td>
<td>16</td>
<td>9</td>
<td>9</td>
<td>0</td>
<td>21</td>
<td>18</td>
<td>1</td>
<td>21</td>
<td></td>
</tr>
</tbody>
</table>

The archaeologist already found out that the ciphertext space is $C = \{A, B, \ldots, Z\}$ and that an affine cipher is used.

(a) What is the cardinality of the message space $M$ and of the key space $K$?

(b) Calculate the estimator of the index of coincidence $I_c$ and decide if this is a monoalphabetic or a polyalphabetic cipher.

(c) Help the archaeologist to decipher the inscription: Give the encryption and decryption rule and decipher the first eight letters of the cryptogram to verify your results. What is the key?

Hint: The most frequent letters in English are:

<table>
<thead>
<tr>
<th>letter</th>
<th>E</th>
<th>T</th>
<th>A</th>
<th>O</th>
<th>I</th>
<th>N</th>
</tr>
</thead>
<tbody>
<tr>
<td>frequency</td>
<td>12.2</td>
<td>9.10</td>
<td>8.12</td>
<td>7.68</td>
<td>7.31</td>
<td>6.95</td>
</tr>
</tbody>
</table>

Exercise 2. Let $\varphi$ be the Euler function. Moreover, let $p \neq q$ be prime numbers and $n = pq$.

(a) Show that $\varphi(pq) = \varphi(p) \varphi(q)$ holds.

(b) Show that $n$ may be efficiently factorized if $\varphi(n)$ is known.

(c) Factorize $n = 367080319$ by means of $\varphi(n) = 367042000$.

Another variant for factorization of a natural number $m$ was developed by Pierre de Fermat. He has utilized

$$m = x^2 - y^2 = (x - y)(x + y) \quad x, y \in \mathbb{N}_0 \quad (1)$$

for factorization.
(d) Factorize $n = 367080319$ utilizing (1).

(e) Is it possible to find $x, y \in \mathbb{N}_0$ for all natural numbers $m > 2$ such that (1) is fulfilled? Give a reason.

Exercise 3. Alice wants to use the triple $(p, a, y) = (137, 3, 97)$ as public ElGamal key.

(a) Show that this is a valid ElGamal key.

(b) Determine the plaintext of Alice’s message $(c_1, c_2) = (81, 7)$ without calculating the private key $x$.

Alice utilizes this key for signing the messages $h(m_1) = 106$ and $h(m_2) = 99$ with the signatures $(r_1, s_1) = (13, 63)$ and $(r_2, s_2) = (13, 62)$.

(c) What did Alice do wrong?

(d) Calculate her private key $x$.

Exercise 4. Consider the following function:

$$E : Y^2 = X^3 + 2X + 6.$$ 

(a) Does $E$ describe an elliptic curve in the field $\mathbb{F}_7$? Give a reason.

(b) Determine all points and their inverses in the group.

(c) What is the order of the group?

It is difficult to obtain the discrete logarithm $a$ of $Q$ to the base $P$ for two points $P, Q$ of an elliptic curve $E$. A possible approach is the application of the Pollard $\rho$-factoring method. The idea behind this method is to find numbers $c, d, c', d' \in \mathbb{Z}$ for two given points $P, Q$ on the elliptic curve with $\gcd(d - d', \text{ord}(P)) = 1$ such that the following equation holds:

$$cP + dQ = c'P + d'Q. \quad (2)$$

(d) Compute the discrete logarithm $a$ of $Q$ to base $P$ by means of (2).

An oracle provides us the values $c = 2, d = 4, c' = -1, d' = -3, P = (4, 1), Q = (1, 3), 4Q = (3, 5), \text{ and } -3Q = (5, 6)$. Assume that $P$ is a generator.

(e) Show that equation (2) is fulfilled for these values and compute the discrete logarithm $a$ of $Q$ to base $P$. 