Name:

Student number:

<table>
<thead>
<tr>
<th>Exercise</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>total</th>
</tr>
</thead>
<tbody>
<tr>
<td>points</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Notes: Please hand in this sheet at the end of the exam. You may keep the sheet with the exercises.
This exam consists of 6 exercises. You have from 14:00 – 17:00 to solve them. You can reach 50 points.
Make sure to justify your answers in detail and to give clear arguments.
Document all steps, in particular of algorithms; it is not sufficient to state the correct result without the explanation. If the problem requires usage of a particular algorithm other solutions will not be accepted even if they give the correct result.
All answers must be submitted on TU/e letterhead; should you require more sheets ask the proctor. State your name on every sheet.
Do not write in red or with a pencil.
You are allowed to use any books and notes. You are not allowed to use the textbooks of your colleagues.
You are allowed to use a simple, non-graphical pocket calculator. Usage of laptops and cell phones is forbidden.
1. What do the Gilbert-Varshamov, Singleton, Griesmer, and Hamming bound say about the dimension of a binary, linear code of length 11 and minimum distance 5.

2. Let the public key of user $U$ in the McEliece system be

$$G_U = \begin{pmatrix}
1 & 1 & 0 & 1 & 0 & 0 & 1 \\
1 & 0 & 1 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 1 & 1 & 1 & 1
\end{pmatrix}$$

over $\mathbb{F}_2$ and let $w = 1$ (the number of errors one can add in the encryption). Demonstrate the usage of the McEliece cryptosystem by encrypting $m = (100)$.

3. This exercise is about constructing codes starting from a Hamming code. Let $C$ be a binary Hamming code of dimension 4.

   (a) State the parameters (length, dimension, redundancy, minimum distance) and parity check matrix of $C$.

   (b) State the parameters (length, dimension, minimum distance) and parity check matrix of the extended code $C^{\text{ext}}$ of $C$.

   (c) Give the parameters of the concatenated code that one contains when using $C^{\text{ext}}$ as inner code and a $2^4$-ary Hamming code with redundancy 3 as outer code.

4. This exercise is about computing discrete logarithms in some groups.

   (a) The integer $p = 10037$ is prime. You are the eavesdropper and know that Alice and Bob use the Diffie-Hellman key-exchange in a cyclic subgroup of $(\mathbb{Z}/p, +)$ with generator $g = 1234$. You observe $h_a = 2345$ and $h_b = 4567$. What is the shared key of Alice and Bob?

   (b) The order of 5 in $\mathbb{F}_{73}^*$ is 72. Charlie uses the subgroup generated by $g = 5$ for cryptography. His public key is $g_c = 2$. Use the Pohlig-Hellman method to compute an integer $c$ so that $g_c \equiv g^c \pmod{73}$.
5. (a) Find all affine points on the Edwards curve 
\[ x^2 + y^2 = 1 - 3x^2y^2 \] over \( \mathbb{F}_{11} \).
4 points

(b) Verify that \( P = (2, 2) \) is on the curve. Compute the order of \( P \).
3 points

(c) Translate the curve and \( P \) to Montgomery form
\[ Bv^2 = u^3 + Au^2 + u. \]
2 points

6. The Hill cipher is a secret-key system based on matrices. It takes a message in the English alphabet (26 characters), translates the characters into numbers as given below, and then encrypts the message by encrypting \( n \) numbers at a time as follows:

Let the secret key \( M \) be an \( n \times n \) matrix over \( \mathbb{Z}/26\mathbb{Z} \) which is invertible and let the plaintext \( a \) be the vector \( (a_1, a_2, \ldots, a_n) \in (\mathbb{Z}/26\mathbb{Z})^n \).

The corresponding ciphertext is \( c^T = Ma^T \). To decrypt compute \( a^T = M^{-1}c^T \).

(a) Let
\[
M = \begin{pmatrix}
2 & 1 & 1 \\
1 & 3 & 2 \\
1 & 3 & 1
\end{pmatrix}.
\]
Encrypt the text CRYPTO
3 points

(b) Let \( M \) be a \( 2 \times 2 \) matrix. You know that \( (1, 3)^T \) was encrypted as \( (-9, -2)^T \) and that \( (7, 2)^T \) was encrypted as \( (-2, 9)^T \). Find the secret key \( M \).
6 points

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
<th>G</th>
<th>H</th>
<th>I</th>
<th>J</th>
<th>K</th>
<th>L</th>
<th>M</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>10</td>
<td>11</td>
<td>12</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>N</th>
<th>O</th>
<th>P</th>
<th>Q</th>
<th>R</th>
<th>S</th>
<th>T</th>
<th>U</th>
<th>V</th>
<th>W</th>
<th>X</th>
<th>Y</th>
<th>Z</th>
</tr>
</thead>
<tbody>
<tr>
<td>13</td>
<td>14</td>
<td>15</td>
<td>16</td>
<td>17</td>
<td>18</td>
<td>19</td>
<td>20</td>
<td>21</td>
<td>22</td>
<td>23</td>
<td>24</td>
<td>25</td>
</tr>
</tbody>
</table>