Solution of Problem 1

a) With \( n = 39 \) and frequency analysis

\[
\begin{array}{|c|c|c|c|c|c|c|c|c|c|c|c|c|c|c|c|c|c|c|c|c|c|c|c|c|c|}
\hline
\ell & A & B & E & F & G & H & L & N & P & R & S & U & V & Y & Z \\
N_\ell & 5 & 5 & 3 & 2 & 5 & 2 & 1 & 2 & 1 & 3 & 2 & 1 & 5 & 1 & 1 \\
\hline
\end{array}
\]

we can calculate the index of coincidence as

\[
I_C = \frac{\sum_{\ell=0}^{25} N_\ell(N_\ell - 1)}{n(n - 1)} = \frac{4 \cdot (2 \cdot 1) + 2 \cdot (3 \cdot 2) + 4 \cdot (5 \cdot 4)}{39 \cdot 38} = \frac{100}{1482} \approx 0.06748
\]

b) \( I_C \) is close to \( \kappa_E = 0.0669 \), so it is likely that a monoalphabetic cipher was used.

c) From the first four letters, we can see that the Caesar cipher with a rotation of 13 was used. The plain text is calculated as follows.

\[
\begin{array}{cccccccccccccccccccc}
24 & 21 & 8 & 17 & 24 & 1 & 0 & 19 & 13 & 0 & 16 & 2 & 4 & 1 & 5 & 2 & 17 & 4 \\
L & I & V & E & L & O & N & G & A & N & D & P & R & O & S & P & E & R \\
\end{array}
\]

d) Some types of attacks are as follows.

- Ciphertext-only attack
- Known-plaintext attack
- Chosen-plaintext attack
- Chosen-ciphertext attack

e) \( P \in \{0, 1\}^{k \times k} \). The sum of each row (and column) needs to be one for \( P \) to be a permutation matrix.

f) Using some public initial vector \( c_0 \) the cryptograms for \( n \in \mathbb{N} \) are calculated as

\[
c_n = e(m_n \oplus c_{n-1}) = (m_n \oplus c_{n-1})P.
\]
Solution of Problem 2

a) It holds

\[ H(\hat{C} \mid \hat{M}) = \sum_{M \in \mathcal{M}} P(\hat{M} = M) H(\hat{C} \mid \hat{M} = M). \]

Calculate

\begin{align*}
H(\hat{C} \mid \hat{M} = M) &= -\sum_{C \in \mathcal{C}} P(\hat{C} = C \mid \hat{M} = M) \log P(\hat{C} = C \mid \hat{M} = M) \\
&= -(1 - \epsilon) \log(1 - \epsilon) - \frac{3}{4} \log \left( \frac{\epsilon}{3} \right) \\
&= -(1 - \epsilon) \log(1 - \epsilon) - \epsilon \log(\epsilon) + \epsilon \log(3)
\end{align*}

which is independent of \( P(\hat{M} = M) \), and hence

\[ H(\hat{C} \mid \hat{M}) = \sum_{M \in \mathcal{M}} P(\hat{M} = M) H(\hat{C} \mid \hat{M} = M) = -(1 - \epsilon) \log(1 - \epsilon) - \epsilon \log(\epsilon) + \epsilon \log(3). \]

For calculating \( P(\hat{C} = C) \) we condition on \( \hat{M} \).

\[ P(\hat{C} = C) = \sum_{M \in \mathcal{M}} P(\hat{M} = M) P(\hat{C} = C \mid \hat{M} = M) = (1 - \epsilon) P(\hat{M} = C) + \frac{\epsilon}{3} P(\hat{M} \neq C). \]

b) If \( \hat{M} \) is uniformly distributed, then

\[ P(\hat{C} = C) = (1 - \epsilon) \frac{1}{4} + \frac{\epsilon}{3} \frac{3}{4} = \frac{1}{4}, \]

and hence,

\[ H(\hat{C}) = \log(4). \]

Moreover, \( H(\hat{M}) = \log(4) \) since it is uniformly distributed. From the chainrule in Theorem 4.3 we get

\[ H(\hat{M} \mid \hat{C}) = H(\hat{C}) - H(\hat{C} \mid \hat{M}) \]

which implies that

\[ H(\hat{M} \mid \hat{C}) = H(\hat{C} \mid \hat{M}), \]

as \( H(\hat{C}) = H(\hat{M}) \).

c) Using the expression of \( H(\hat{M} \mid \hat{C}) \) from above, the expression follows.

d) The perfect secrecy is achieved when \( P(\hat{C} = C \mid \hat{M} = M) \) does not depend on \( M \) and \( C \). Hence:

\[ 1 - \epsilon = \frac{\epsilon}{3} \implies \epsilon = \frac{3}{4}. \]
Solution of Problem 3

a) We show that \( a = 2 \) is a primitive element utilizing Prop. 7.5

\[ a \text{ is PE modulo } p \iff a^{\frac{p-1}{p_i}} \not\equiv 1 \pmod{p} \forall p_i \]

where \( p - 1 = \prod_i p_i^{k_i} \) is the prime factorization of \( p - 1 \).

With \( p - 1 = 178 = 2 \cdot 89 \) it holds

\[ a^2 \equiv 4 \pmod{179}, \]
\[ a^{89} \equiv ((2^7)^2 \cdot 2^5 \equiv (95^2) \cdot 32 \equiv (75)^2 \cdot 75 \cdot 32 \equiv 76 \cdot 73 \equiv -1 \pmod{179}, \]

which verifies the claim.

<table>
<thead>
<tr>
<th>Bit</th>
<th>S</th>
<th>M</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>-</td>
</tr>
<tr>
<td>0</td>
<td>4</td>
<td>-</td>
</tr>
<tr>
<td>1</td>
<td>16</td>
<td>32</td>
</tr>
<tr>
<td>1</td>
<td>129</td>
<td>79</td>
</tr>
<tr>
<td>0</td>
<td>155</td>
<td>-</td>
</tr>
<tr>
<td>0</td>
<td>39</td>
<td>-</td>
</tr>
<tr>
<td>1</td>
<td>89</td>
<td>178</td>
</tr>
</tbody>
</table>

b) First Alice calculates \( u = a^{x_A} \mod p \):

\[ u = a^{x_A} \equiv 2^{23} = 2^{14} \cdot 2^9 \equiv 95 \cdot 154 \equiv 131 \pmod{179}, \]

hence, \( u = 131 \). Bob equally finds \( v = a^{x_B} \mod p \):

\[ a^{x_B} \equiv 2^{31} \equiv 2^{23} \cdot 2^8 \equiv 131 \cdot 77 \equiv 63 \pmod{179}, \]

hence \( v = 63 \).

<table>
<thead>
<tr>
<th>Bit</th>
<th>S</th>
<th>M</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>-</td>
</tr>
<tr>
<td>0</td>
<td>4</td>
<td>-</td>
</tr>
<tr>
<td>1</td>
<td>16</td>
<td>32</td>
</tr>
<tr>
<td>1</td>
<td>129</td>
<td>79</td>
</tr>
<tr>
<td>1</td>
<td>155</td>
<td>131</td>
</tr>
<tr>
<td>1</td>
<td>89</td>
<td>178</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Bit</th>
<th>S</th>
<th>M</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>-</td>
</tr>
<tr>
<td>1</td>
<td>4</td>
<td>8</td>
</tr>
<tr>
<td>1</td>
<td>64</td>
<td>128</td>
</tr>
<tr>
<td>1</td>
<td>95</td>
<td>11</td>
</tr>
<tr>
<td>1</td>
<td>121</td>
<td>63</td>
</tr>
</tbody>
</table>

It holds \( 31 \cdot 23 \mod p - 1 = 1 \), and hence,

\[ v^{x_A} \equiv (2^{31})^{23} \equiv 2^1 \equiv 2 \pmod{179}. \]

c) Oscar should use \( z = 89 \). He sends \( u^{89} \mod 179 \) in place of \( u \) to Bob. Oscar sends as well \( v^{89} \mod 179 \). The shared key will be either +1 or -1.

d) A simple solution would be to exclude \( \pm 1 \).
Solution of Problem 4

a) \( n = p \cdot q = 143 \), \( \varphi(n) = \varphi(p \cdot q) = (p - 1)(q - 1) = 10 \cdot 12 = 120. \)

\[ d = e^{-1} \mod \varphi(n) = e^{-1} \mod 120 \]

It holds \( 1 = 1 \cdot 120 - 17 \cdot 7 \), and hence, \( d = 103. \)

\[ m = c^d \mod n = 31^{103} \mod 143 \]

Use square and multiply to calculate \( m = 47. \)

\begin{center}
\begin{tabular}{c|cc|c}
Bit & S & M \\
1 & 31 & - \\
1 & 103 & 47 \\
0 & 64 & - \\
0 & 92 & - \\
1 & 27 & 122 \\
1 & 12 & 86 \\
1 & 103 & 47 \\
\end{tabular}
\end{center}

b) Keys are generated such that

\[ d = e^{-1} \mod \varphi(n). \]

It follows that there are \( \varphi(\varphi(n)) \) such numbers.

c) The public parameters and the received ciphertext are:

\[ \begin{align*} 
&\bullet \ e = d^{-1} \mod \varphi(n), \\
&\bullet \ n = pq, \\
&\bullet \ c = m^e \mod n. 
\end{align*} \]

The plaintext \( m \) is not relatively prime to \( n \), i.e., \( p \mid m \) or \( q \mid m \) and \( p \neq q \). Hence, \( \gcd(m, n) \in \{p, q\} \) holds. The \( \gcd(m, n) \) can be easily computed such that both primes can be calculated by either \( q = \frac{n}{p} \) or \( p = \frac{n}{q} \).

The private key \( d \) can be computed since the factorization of \( n = pq \) is known.

\[ d = e^{-1} \mod \varphi(pq) = e^{-1} \mod (p - 1)(q - 1). \]

This inverse is computed using the extended Euclidean algorithm.

d) Using Euler’s criterion, \(-1\) is a quadratic residue if and only if \((-1)^{\frac{p-1}{2}} = 1\), which means \( \frac{p-1}{2} = 2k \) or equivalently \( p = 4k + 1. \)