Problem 1.

a) What does a Friedman Test decide?

b) Compute the expectation of the index of coincidence over the alphabet \( \mathcal{A} = \{A, B, C\} \) if the sequence of characters in the ciphertext is independent and identically distributed and each character is uniformly distributed.

Consider a Vigenère cipher with message space \( \mathcal{M} = \mathcal{A}^n, n \in \mathbb{N} \), and key space \( \mathcal{K} = \mathcal{A}^w, w \in \mathbb{N}, \) with \( w \mid n \). The messages and keys are both uniformly distributed.

c) Why has the cryptosystem perfect secrecy for \( w = n \)? Why has it no perfect secrecy for \( w < n \)?

d) Estimate the index of coincidence \( I_c \) over the alphabet \( \mathcal{A} \) for the following ciphertext \( c \) of length \( n = 24 \):
\[
c = \text{CAAABBCACBCABACAABCCCACA}.
\]

e) Assume the characters of the plaintext occur with the following frequencies: \#A = 16, \#B = 5, and \#C = 3. Determine the key \( k \) of the Vigenère cipher and decrypt the ciphertext \( c \) for \( w = 4 \) by identifying the frequencies from the ciphertext.

f) State four more classical cryptosystems from the lecture.

Problem 2.

A key stream \( \mathbf{z} = (z_i)_{i \in \mathbb{N}} \) is generated from a key \( \mathbf{k} = (k_1 \ldots k_q) \) by the following recursion:
\[
\begin{align*}
z_i &= k_i, & 1 \leq i \leq q, \\
z_i &= \sum_{j=1}^{q} p_j z_{i-j}, & q < i.
\end{align*}
\]

All computations are in the finite field \( \mathbb{F}_2 \). Consider the following linear feedback shift register (LFSR) for stream ciphers to generate a key stream:
a) Derive the feedback polynomial \( p(x) = 1 + \sum_{i=1}^{q} p_i x^i \) of the LFSR given in the figure above. Show that the polynomial \( p(x) \) is primitive\(^1\) in \( \mathbb{F}_2 \) to ensure that the LFSR has the maximal period.

The plaintext symbols \( m_i \) are encrypted into the ciphertext symbols \( c_i \) as follows:

\[ c_i = z_i \oplus m_i. \]

b) A key \( k \) is called weak, if \( c = m \) for all \( m \in \mathcal{M} \) holds. Find a weak key for the given LFSR.

c) Encrypt \( m = (m_1 \ldots m_{10}) = (0100101101) \) with the key \( k = (k_1 k_2 k_3) = (100) \).

d) What is the length of the (maximal) period of \( z \)? How many zeros and ones occur within one period?

Now consider the following key stream generator with three independent LFSRs of period lengths \( l_1, l_2, l_3 \):

```
\[ \begin{aligned}
\text{LFSR}_1 & \quad a_i \\
\text{LFSR}_2 & \quad b_i \\
\text{LFSR}_3 & \quad c_i
\end{aligned} \]
```

Answer the following questions without giving an explicit proof:

e) What is the period length of the sequence of triples \( ((a_i, b_i, c_i))_{i \in \mathbb{N}} \) for the key stream generator? What are the minimal and maximal period lengths? How should \( l_1, l_2, l_3 \) be chosen to maximize the period length?

The function \( f \) is defined by:

\[ y_i = f(a_i, b_i, c_i) = (a_i \land b_i) \oplus (c_i \land c_i). \]

f) Compute the probabilities \( \Pr(b_i \mid y_i) \) assuming that \( (a_i, b_i, c_i) \) is uniformly distributed over \( \mathbb{F}_2^3 \). Which estimate for \( b_i \) ensures a success probability of \( \frac{3}{4} \), if \( y_i \) is given?

**Problem 3.**

In the following an RSA cryptosystem with public key \( (n, e) \) is considered.

a) Does a valid RSA public key exist with \( e = 2 \)? Substantiate your answer.

The message \( m \) is encrypted by means of the public key \( (n, e) = (4819, 3343) \) resulting in the cryptogram \( c = 1219 \).

b) Factorize \( n \) and determine the private key.

c) What is the original message \( m \)?

---

\(^1\) A polynomial \( p(x) \) of degree \( q \) is called primitive if and only if the smallest \( n \in \mathbb{N} \) for which \( p(x) \) divides the polynomial \( x^n + 1 \) is \( n = 2^q - 1 \).
In an RSA cryptosystem the public key \((n', e') = (391, 7)\) and the corresponding private key \(d' = 151\) are known.

**d)** Compute the prime factors \(p\) and \(q\) of \(n'\) by means of the following steps:

i) Determine a multiple \(x\) of \(\varphi(n')\), i.e., an \(x \in \mathbb{Z}\) with \(x = k \cdot \varphi(n')\) for a \(k \in \mathbb{N}\).

ii) Compute the prime factorization of \(x\).

iii) Use the prime factorization to determine \(k, p,\) and \(q\).