Exercise 1.
Bob's public ElGamal key is $(p, a, y) = (101, 2, 11)$.

(a) Find the plaintext of the message $(c_1, c_2) = (64, 79)$ sent to Bob without finding his private key.

(b) Find Bob's private ElGamal key.

Exercise 2.
Consider a Hill cipher over the alphabet $\mathbb{Z}_p$, p prime, with block length $m \geq 2$.

(a) Which conditions need to be fulfilled such that the key $U \in \mathbb{Z}_p^{m\times m}$ is feasible?

(b) What is the cardinality of the key space for $m = 2$ and p prime? What is the cardinality if $p = 29$?

For $p = 29$ a known-plaintext attack for the message

a	l	l	t	h	e	b	e	s	t	f	o	r	y	o	u	i	n	h	e	r	e	(in letters)
0	11	11	19	7	4	1	4	18	19	5	14	17	24	14	20	8	13	7	4	17	4	(in numbers)

shall be executed. The corresponding cryptogram is given as

e	e	p	z	j	s	y	r	m	c	p	j	p	m	z	o	t	v	j	s	n	k	(in letters)
4	4	15	25	9	18	24	17	12	2	15	9	15	12	25	14	19	21	9	18	13	10	(in numbers)

(c) Which key U has been used for encryption?

Now consider the alphabet $\mathbb{Z}_{26}$, i.e., $p = 26$ is no longer a prime.

(d) Is the key $U = \begin{pmatrix} 15 & 11 \\ 1 & 8 \end{pmatrix}$ appropriate for executing the Hill cipher? Determine the decryption function, if applicable.

Exercise 3.
Consider a block cipher with $N \in \mathbb{N}$ Feistel rounds. Each round $1 \leq n \leq N$ is structured as given in the following figure.
The message $\mathbf{m}$ is decomposed into two parts of the same size $\mathbf{m} = (L_1, R_1)$. It holds that

$$L_{n+1} = R_n,$$
$$R_{n+1} = f_n(K_n, R_n) \oplus L_n,$$

where the round keys are denoted as K_n. The resulting cryptogram is given as

$$\mathbf{c} = (R_{N+1}, L_{N+1}).$$

(a) Describe a decryption method. Is it possible to apply the same algorithm for decryption? What are the round keys, if applicable?

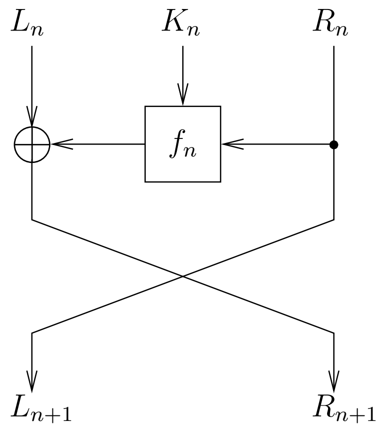

Abbildung 3.1: Feistel round

Consider a specific block cipher with input length of 8 and key length of 4 bits. The functions f_n are given as

$$f_n(R_n, K_n) = g(R_n \oplus K_n).$$

Analogously to SubBytes of AES the function $g(a_3, a_2, a_1, a_0) = (r_3, r_2, r_1, r_0)$, $a_i, r_i \in \{0, 1\}$, is defined by

$$\begin{pmatrix} r_0 \\ r_1 \\ r_2 \\ r_3 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \end{pmatrix} \oplus \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix},$$

where $(y_3, y_2, y_1, y_0) \in \mathbb{F}_{2^4}$ is determined by the inverse polynomial of $\sum_{i=0}^{3} a_i\, x^i$ modulo the irreducible polynomial $h(x) = x^4 + x^3 + 1$.
The resulting function g is given by the following table.

$\mathbf{a}$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$g(\mathbf{a})$	1	10	2	12	8	14	15	5	13	9	0	11	6	7	3	4

In this table, $\mathbf{a} = (a_3, a_2, a_1, a_0)$ and $g(\mathbf{a}) = (r_3, r_2, r_1, r_0)$ are represented by $\sum_{i=0}^{3} a_i\, 2^i$ and $\sum_{i=0}^{3} r_i\, 2^i$.

(b) Show that the inverse of $x^3 + x$ modulo $h(x)$ in $\mathbb{F}_{2^4}$ is given by $x^3 + x + 1$.

(c) Assume g to be known and $N = 2$ Feistel rounds are executed. Calculate the keys K_1 and K_2 for a given message $\mathbf{m} = (0, 0, 1, 1, 1, 1, 0, 0)$ and a cryptogram $\mathbf{c} = (1, 0, 1, 0, 0, 1, 1, 0)$. Is security improved by introducing a third round?

(d) Which block cipher of the lecture has the same structure as illustrated in Figure 3.1? Specify the blocks within the functions f_n which are executed in that block cipher.

Exercise 4.

(a) Show by means of the Miller Rabin primality test (MRPT) that $n = 301$ is composite. Utilize the square and multiply algorithm. Is 2 a strong witness for the compositeness of n?

(b) One run of the MRPT for a given odd number $n = 1+q\,2^k$, $k, q \in \mathbb{N}$, q odd, consists of an exponentiation and a couple of squarings. The exponentiation shall be performed by means of the square and multiply algorithm. Assume that the chosen number a is a strong witness for compositeness of n. How many multiplications m and squarings s are needed during one run of the MRPT? Determine the minimum and maximum number of multiplications and squarings.

(c) All odd numbers up to $N \in \mathbb{N}$ are tested on primality with one run of the MRPT ($M = 1$). Assume there are $\lfloor N/\ln(N) \rfloor$ primes which are less or equal to N. Compute an upper bound for the expectation of the number of runs for which the test states „prime“.

(d) Consider a composite number $n = p \cdot q = 3365753$ with primes p and q. Factorize n by means of the knowledge $\varphi(n) = 3361920$.

Exercise 5.
Consider the RSA cryptosystem.

(a) Show the correctness of the RSA decryption.

(b) Is $e = 2$ a valid RSA key? Justify your answer.

(c) Decrypt the ciphertext $c = 8$ which was encrypted with the public key $(n, e) = (9797, 1477)$.

Consider the Rabin cryptosystem with parameters $p = 43$ and $q = 71$.

(d) Decrypt the ciphertext $c = 144$.

Hints:

- Calculate the square roots of $2 \mod 71$ and $15 \mod 43$.
- It holds that $20 \cdot 71 - 33 \cdot 43 = 1$.
- Assume that the least significant bits of the message are 101.

Exercise 6.
Consider the following proposal for a hash function.
Given is a message $M = m_1, m_2, \ldots, m_n$ consisting of blocks $m_i \in \{0, 1, ..., q-1\}$. Let q be prime and b be a primitive element $\pmod q$.

Given: $f(t) := b^t \pmod q$

Initialise: $h_0 := 0$

for $i := 1$ to n:

$h_i := f(h_{i-1} + m_i)$

return h_n

(a) Find a collision for the proposed hash function.

(b) Is $f(t)$ for $t \in \{2, ..., q-2\}$ preimage resistant? Justify your answer.

(c) The ElGamal signature scheme and the hash function above shall be used for signing a document. Parameters are $p = 461, a = 2, x = 99$ and $k = 3$, and for the hash function $q = 131$ and $b = 2$. Sign the message $M = (14, 5, 122, 12)$.

Exercise 7.
Consider the elliptic curve

$$E : y^2 = x^3 + 2x + 4.$$

The curve is defined over $\mathbb{F}_7$.

(a) Calculate all points of the curve. How many points are in $E(\mathbb{F}_7)$?

(b) Identify the inverses $-P$ for all points $P \in E(\mathbb{F}_7)$.

Now the Diffie-Hellman key exchange is performed on E. The discrete logarithm problem on elliptic curves is to find a such that $Q = aP$ holds with given points P and Q.

(c) Describe the Diffie-Hellman key exchange protocol on elliptic curves and corresponding parameters.

Perform the key exchange on $E(\mathbb{F}_7)$ and generator $P = (0, 2)$. Alice chooses $x = 4$ as her secret and Bob chooses $y = 3$.

(d) Calculate the messages xP and yP of the key exchange and the common key.