Univ.-Prof. Dr. rer. nat. Rudolf Mathar

1	2	3	4	$\sum$
15	15	15	15	60

Written Examination

Cryptography

Tuesday, August 29, 2017, 01:30 p.m.

Name: ______________________ Matr.-No.: ______________

Field of study: ______________________________

Please pay attention to the following:

1) The exam consists of **4 problems**. Please check the completeness of your copy. **Only** written solutions on these sheets will be considered. Removing the staples is **not** allowed.

2) The exam is passed with at least **30 points**.

3) You are free in choosing the order of working on the problems. Your solution shall clearly show the approach and intermediate arguments.

4) **Admitted materials:** The sheets handed out with the exam and a non-programmable calculator.

5) The results will be published on Wednesday, the 06.09.17, 16:00h, on the homepage of the institute.

The corrected exams can be inspected on Friday, 08.09.17, 10:00h. at the seminar room 333 of the Chair for Theoretical Information Technology, Kopernikusstr. 16.

Acknowledged: ______________________________

(Signature)

Problem 1. (15 points)
Let $(\mathcal{M}, \mathcal{K}, \mathcal{C}, e, d)$ be a cryptosystem with the message space $\mathcal{M} = \{1, 2\}$, the key space $\mathcal{K} = \{k_1, k_2, k_3\}$ and the ciphertext space $\mathcal{C} = \{1, 2, 3, 4\}$. The following table contains the encryption rules:

	k_1	k_2	k_3
1	1	2	3
2	2	3	4

, e.g., $e(1, k_1) = 1$.

Let the message $\hat{M}$ and the key $\hat{K}$ be stochastically independent random variables defined over the space $\mathcal{M}$ and $\mathcal{K}$, respectively. $\hat{C}$ is the random variable corresponding to the ciphertext.

a) Suppose that $P(\hat{M} = 1) = p$ and $\hat{K}$ is uniformly distributed over the key space. Determine $H(\hat{M}), H(\hat{K}), H(\hat{C})$.

b) Find $H(\hat{M} \mid \hat{C})$ and the key equivocation $H(\hat{K} \mid \hat{C})$.
Hint: $H(\hat{M} \mid \hat{C}) = H(\hat{C} \mid \hat{M}) + H(\hat{M}) - H(\hat{C})$

c) Show that this cryptosystem does not have perfect secrecy. Is there a probability distribution over the key space so that the perfect secrecy is achieved?

Problem 2. (15 points)
Let $n = pq$, $p \neq q$ distinct odd primes.

a) Suppose that for some $r \in \mathbb{Z}_n^*$ the quadratic equation $x^2 \equiv r^2 \mod n$ has a non-trivial solution, i.e., $a \neq \pm r \mod n$. Show that in this case

$$\gcd(a + r, n) \in \{p, q\}.$$

Consider an RSA cryptosystem with two prime numbers $p = 13$ and $q = 19$. The public key is given by $(n = 13 \times 19 = 247, e = 59)$.

b) Determine the decryption exponent d.

c) Decrypt the ciphertext $c = 10$ using the square-and-multiply algorithm.

Consider an RSA cryptosystem with the public key (n, e) with $n = pq$ and $p \neq q$ distinct primes.

d) Show that if the plaintext m is chosen such that $\gcd(n, m) = p$ or q, the secret key d can be computed only from the ciphertext c and the public key (n, e).

e) Consider an RSA cryptosystem with the public key $(n = 143, e = 7)$. For the ciphertext $c = 22$, compute the secret key d.

Problem 3. (15 points)
Consider the following *Linear Feedback Shift Register* (LFSR) based *stream cipher*. Messages are bit sequences of arbitrary length, i.e., character sequences over the alphabet $\mathbb{F}_2 = \{0, 1\}$. Let the message be $m = m_1 m_2 \ldots m_l$. Keys are also bit sequences $k = k_1 k_2 \ldots k_n$ of fixed length $n < l$. Now, a key stream $z = z_1 z_2 \ldots z_l$ is recursively generated depending on the key as follows:

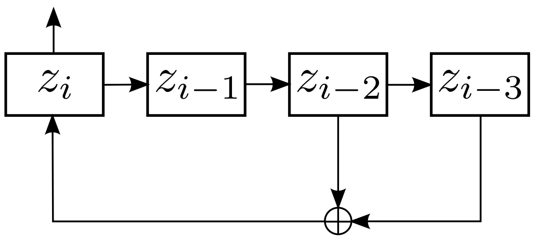
$$\begin{aligned} z_i &= k_i, \quad 1 \leq i \leq n, \\ z_i &= \sum_{j=1}^{n} s_j z_{i-j} \pmod 2, \quad n < i \leq l. \end{aligned}$$

The bits $s_1, \ldots, s_n$ are fixed and given in advance. We encrypt $c_i := m_i \oplus z_i$ for $1 \leq i \leq l$.

a) How does decryption work for this cryptosystem? What happens if $k = 00\ldots0$ is chosen as the key?

b) Encrypt the message $m = 10110001010011010100$ with $n = 4$, $s_2 = s_3 = 0$, $s_1 = s_4 = 1$ using the key $k = 0110$.

c) How long is the period[1] of the key stream z in **b)**? And how many zeros and ones occur in this key stream z within one period? What is the maximal period $p_{\max}$ of an LFSR with a key k of length n?



d) Derive the feedback polynomial $f(x) = 1 + \sum_{i=1}^{n} s_i\, x^i$ of the LFSR given in the figure above. It is known that the LFSR has the maximal period $p_{\max}$ if the feedback polynomial of z_i is primitive[2] in $\mathbb{F}_2$. Show that the above LFSR fulfils this requirement.

[1]The period p of an LFSR is defined as $p = \min\{k \in \mathbb{N} | \exists i_0 \in \mathbb{N}, i \in \mathbb{N}, \forall i \geq i_0 : z_{i_0+k} = z_i\}$.
[2]A polynomial $f(x)$ of degree n is called *primitive* if and only if the smallest $q \in \mathbb{N}$ for which $f(x)$ divides the polynomial $x^q + 1$ is $q = 2^n - 1$.

Problem 4. (15 points)
Consider a modified Rabin cryptosystem in which the encryption function e_K is defined as $e_K(m) = m \cdot (m + B) \mod n$, where m is the message. $B \in \mathbb{Z}_n$ and $n = pq$ (for primes $p \neq q$) constitute the public key. Supposing that $p = 199$, $q = 211$, and $B = 1357$, perform the following computations.

a) Compute the encryption $y = e_K(32767)$.

b) Determine the four possible decryptions of the ciphertext y.

Alice and Bob use Shamir's no-key protocol to exchange a secret message. They agree to use the prime $p = 31883$ for their communication. Alice wants to send the message m to Bob. She chooses the random number $a = 8647$ while Bob chooses $b = 10931$. It is known that Bob receives the first exchanged value $c_1 = 26843$.

c) Calculate the remaining values c_2, c_3, and decipher the message m for Bob.
Hint: You may use the following values :

$$27084^{12046} \equiv 24532 \pmod{31883}, \quad 27084^{30315} \equiv 13230 \pmod{31883},$$
$$26843^{8647} \equiv 14913 \pmod{31883}, \quad 14913^{10931} \equiv 868 \pmod{31883}.$$

Additional sheet

Problem:

Additional sheet

Problem:

Additional sheet

Problem: