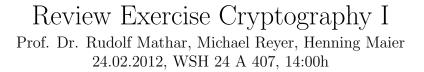
Lehrstuhl für Theoretische Informationstechnik



Problem 1.

RNNTHAACHEI

- (a) Describe Kerkhoff's principle.
- (b) We use the modified Roman alphabet \mathbb{Z}_{29} with the additional letters $\alpha = 26$, $\beta = 27$ and $\gamma = 28$. A Hill cipher was used to encrypt the following message \mathbf{m}_1 into the ciphertext \mathbf{c}_1 :

$$\mathbf{m}_1 = CODE, \ \mathbf{c}_1 = XN\beta A.$$

Determine the key matrix $\mathbf{U} \in \mathbb{Z}_{29}^{2 \times 2}$ and compute its inverse $\mathbf{U}^{-1} \in \mathbb{Z}_{29}^{2 \times 2}$.

(c) In the following, we use the common Roman alphabet \mathbb{Z}_{26} . The plaintext $\hat{\mathbf{m}}_2$ is given in English. Each blank is substituted by a random uniformly distributed letter in \mathbb{Z}_{26} . The resulting plaintext is denoted by \mathbf{m}_2 . \mathbf{m}_2 is encrypted by a Caesar cipher. Determine the key k_2 , decrypt the following ciphertext \mathbf{c}_2 and reveal $\hat{\mathbf{m}}_2$. As sideinformation it is known that the word *NOISE* occurs in the plaintext.

				N 13				
				M 12				

Problem 2.

Consider the following cryptosystem with message space \mathcal{M} and cryptogram space \mathcal{C} with $\mathcal{M} = \mathcal{C} = \{0, 1\}^4$. A message $\mathbf{m} = (m_1, m_2, m_3, m_4)$ is encrypted to a cryptogram $\mathbf{c} = (c_1, c_2, c_3, c_4)$ as follows.

$$c_1 = (a m_1 + m_2) \mod 2$$

$$c_2 = (b m_1 + c m_2) \mod 2$$

$$c_3 = (d m_3 + e m_4) \mod 2$$

$$c_4 = (m_3 + f m_4) \mod 2$$

The key is given as $\mathbf{k} = (a, b, c, d, e, f) \in \{0, 1\}^6$, i.e., it holds $\mathbf{c} = e(\mathbf{m}, \mathbf{k})$.

- (a) Specify the maximal key space \mathcal{K} and its cardinality.
- (b) Has the given system perfect secrecy, if the keys follow a uniform distribution over \mathcal{K} ? State a reason for your answer.

Consider the above system with given key $\mathbf{k}_0 = (0, 1, 1, 0, 1, 1)$.

(c) Specify the decryption rule $\mathbf{m} = d(\mathbf{c}, \mathbf{k}_0)$ with that key \mathbf{k}_0 . Decrypt the cryptogram $\mathbf{c} = (0, 0, 0, 1, 1, 0, 1, 1)$.

The above system may be used as block cipher on texts with arbitrary length.

- (d) Decrypt the cryptogram $\mathbf{c} = (0, 1, 0, 0, 0, 1, 1, 1)$ in the output feedback mode (OFB) with $C_0 = (0, 1, 1, 0)$.
- (e) Encrypt the message $\mathbf{m} = (1, 0, 0, 1, 0, 0, 1, 1)$ in the cipher feedback mode (CFB) using the same C_0 .

Finally, answer the following general questions about block ciphers.

- (f) Which other operation modes alongside OFB und CFB have been covered in the lecture?
- (g) Name the steps which are executed in the rounds $1, \ldots, r-1$ of the block cipher AES. What is the difference between those rounds and the last one?

Problem 3.

(a) Let $p \neq q$ prime and $x, y \in \mathbb{N}$. Prove that

 $x \equiv y \pmod{p}$ and $x \equiv y \pmod{q} \Leftrightarrow x \equiv y \pmod{p \cdot q}$

holds.

Consider the following primality test (a proof of validity is not needed): Let n > 1 be an integer such that

- (1) there exists a q prime with $q \mid (n-1)$ and $q > \sqrt{n} 1$,
- (2) there exists an a such that $a^{n-1} \equiv 1 \pmod{n}$, and
- (3) $gcd(a^{(n-1)/q} 1, n) = 1$ holds

then n is prime.

- (b) Show that 83 is prime by using the given primality test and choose a = 11.
- (c) Name three further primality tests.

In the following, we consider an RSA-cryptosystem with public parameters n = 9179and e = 4321. Furthermore, suppose you sneak into Bobs' office and find a notice saying $\varphi(n^2) = 82390704$.

- (d) Show¹ for $a, b \in \mathbb{N}$ that $\varphi(ab) = \varphi(a)\varphi(b)$ holds if gcd(a, b) = 1.
- (e) Show without factoring n that $\varphi(n) = 8976$.
- (f) Determine the private key d without factoring n.
- (g) Factorize n using $\varphi(n)$.

¹**Remark**: If gcd(a, b) = 1, it holds that gcd(ab, m) = gcd(a, m)gcd(b, m).