Prof. Dr. Rudolf Mathar, Dr. Michael Reyer

Tutorial 13

Friday, July 26, 2019

Problem 1. *(ExamSS18P1)* In this problem, we consider encryption as addition modulo 26, the size of the Latin alphabet.

Consider the following ciphertext:

VASB EZNG VBAV FGUR ERFB YHGV BABS HAPR EGNV AGL

a) Calculate the index of coincidence I_C.

b) Decide whether the ciphertext was encrypted using a monoalphabetic or a polyalphabetic cipher. Substantiate your answer.

A new ciphertext, unrelated to the one above, and the first four plaintext letters are given as follows.

Y	V	I	R	Y	B	A	T	N	A	Q	C	E	B	F	C	R	E
24	21	8	17	24	1	0	19	13	0	16	2	4	1	5	2	17	4
L	I	V	E	_	_	_	_	_	_	_	_	_	_	_	_	_	_
11	8	21	4	_	_	_	_	_	_	_	_	_	_	_	_	_	_

c) As shown, the first four letters of the plaintext message are known to be “LIVE”. Figure out which classical cipher was used for encryption and decrypt the ciphertext. *You may write your answer into the fields below the ciphertext.*

d) The method from the previous task is known as *known-plaintext attack.* Name two other types of attacks.

Let $\boldsymbol{m} = \begin{pmatrix} m_1 & \dots & m_{N\cdot k} \end{pmatrix}$ denote a message different from the one above. N denotes the number of blocks and k is the block length. The message $\boldsymbol{m}$ can then be written as $\boldsymbol{m} = \begin{pmatrix} \boldsymbol{m}_1 & \dots & \boldsymbol{m}_n & \dots & \boldsymbol{m}_N \end{pmatrix}$, where $\boldsymbol{m}_n = \begin{pmatrix} m_{(n-1)\cdot k+1} & \dots & m_{nk} \end{pmatrix}$ is a vector denoting one of the N blocks. For the *permutation cipher* with block length k, the encryption of the message block $\boldsymbol{m}_n$ can be written as a multiplication of a matrix $\boldsymbol{P}$ by the message block $\boldsymbol{m}_n$.

$$\boldsymbol{c}_n = e(\boldsymbol{m}_n) = \boldsymbol{m}_n \boldsymbol{P}$$

e) Characterize the matrix $\boldsymbol{P}$: What is its dimension? Name possible values of its elements. What is the sum of each row?

f) Modify the encryption function such that it uses cipher-block chaining.

Problem 2. *(ExamSS18P2)* Let $(\mathcal{M}, \mathcal{K}, \mathcal{C}, e, d)$ be a cryptosystem with message space $\mathcal{M}$, key space $\mathcal{K}$ and ciphertext space $\mathcal{C}$ given as

$$\mathcal{M} = \mathcal{K} = \mathcal{C} = \{1, 2, 3, 4\}.$$

The message, the key and the ciphertext are random variables denoted as $\hat{M}, \hat{K}$ and $\hat{C}$, respectively. Assume that $P(\hat{M} = M) > 0$ for all $M \in \mathcal{M}$ and $P(\hat{K} = K) > 0$ for all $K \in \mathcal{K}$. The message and the ciphertext are related as follows for some $\epsilon \in [0, 1]$:

$$P(\hat{C} = j \mid \hat{M} = i) = \begin{cases} 1 - \epsilon & \text{if } i = j \\ \frac{\epsilon}{3} & \text{if } i \neq j. \end{cases}$$

a) Find $H(\hat{C} \mid \hat{M})$ and $P(\hat{C} = C)$ for an arbitrary distribution over the message space.

In what follows, assume that the messages are uniformly distributed over the message space.

b) Find $H(\hat{C})$ and $H(\hat{M} \mid \hat{C})$.

c) Show that

$$H(\hat{M}) - H(\hat{M} \mid \hat{C}) = \log(4) - \epsilon \log(3) + (1 - \epsilon) \log(1 - \epsilon) + \epsilon \log(\epsilon).$$

d) For which ϵ is perfect secrecy achieved in this system?

Problem 3. *(ExamSS18P3)* Alice and Bob perform a Diffie-Hellman key exchange protocol with prime $p = 179$ and primitive element $a = 2$.

Alice chooses the random secret $x_A = 23$ and Bob the random secret $x_B = 31$.

a) Show that a is a primitive element.

b) Calculate the values exchanged between Alice and Bob. Also, calculate the shared key.

c) Oscar is planning an Intruder-in-the-Middle Attack against this Diffie-Hellman system. He intercepts the messages u and v exchanged between Alice and Bob, respectively. He applies u^z and v^z before the messages are received by Alice and Bob. Which $z \in \{2, \ldots, 178\}$ should he use so that the attack is effective? Determine the modified shared key.

d) How can Oscar's attack be avoided?

Problem 4. *(ExamSS18P4)* Consider the RSA-Cryptosystem.

a) Bob chooses prime numbers $p = 11$, $q = 13$ and his public key as $e = 7$. Alice encrypts a message m and sends it to Bob. Bob receives the ciphertext $c = 31$. What is the message m?

b) How many RSA keys exist for two given primes p and q?

c) Some message $m \in \{1, \ldots, n-1\}$ with $n = pq$ with two primes $p \neq q$ is encrypted using the RSA-Cryptosystem with public key (n, e). Show that it is possible to compute the secret key d if $p \mid m$ or $q \mid m$.

d) As a general result, show that -1 is a quadratic residue $\bmod p$ if and only if $p = 4k + 1$ for some $k \in \mathbb{N}$.