Review Exercise Cryptography I

Prof. Dr. Rudolf Mathar, Michael Reyer, Henning Maier

31.07.2012, WSH 24 A 407, 9:00h

Problem 1.

(a) State four main attacks of cryptanalysis.

(b) Consider the following ciphertext in $\{A, \dots, Z\}$:

IAENS SPEEC TRDSE SNMTA GNEER VAYOT SHELO RYKSE EI

Compute the index of coincidence and determine if this is a mono- or polyalphabetic cipher. There are 9 letters occurring more often than once.

Let n be a positive integer. Consider an $n \times n$ matrix $\mathbf{L}$ with entries $l_{i,j}$ such that each element of the set $\{0, \dots, n-1\}$ occurs exactly once in each row $i \in \{0, \dots, n-1\}$ and in each column $j \in \{0, \dots, n-1\}$. This encryption matrix is used to determine a cipher for a plaintext $m \in \mathcal{M} = \{0, \dots, n-1\}$ and a key $k \in \mathcal{K} = \{0, \dots, n-1\}$ as follows:

$$c = E_k(m) = l_{m,k}.$$

(c) What is the cardinality of the ciphertext space $\mathcal{C}$?

(d) The following matrix $\tilde{\mathbf{L}}$ does not satisfy the conditions given above:

$$\tilde{\mathbf{L}} = \begin{pmatrix} 1 & 3 & 2 & 0 \\ 2 & 0 & 1 & 2 \\ 1 & 2 & 0 & 1 \\ 0 & 1 & 3 & 2 \end{pmatrix}.$$

Generate a matrix $\hat{\mathbf{L}}$ which satisfies the above conditions by changing exactly two entries.

Now, the following encryption matrix is used:

$$\mathbf{L} = \begin{pmatrix} 2 & 1 & 3 & 0 \\ 3 & 0 & 2 & 1 \\ 1 & 3 & 0 & 2 \\ 0 & 2 & 1 & 3 \end{pmatrix}.$$

(e) Compute the corresponding decryption matrix $\mathbf{D} = (d_{c,k})$ with $m = E_k^{-1}(c) = d_{c,k}$ for the given matrix $\mathbf{L}$.

(f) A block cipher in Cipher-Block-Chaining mode with blocks of length $n = 4$ was used to encrypt the following ciphertext:

$$\mathbf{c} = (1032\ 3210).$$

Decrypt the ciphertext with key $k = 2$ and the initial vector $\mathbf{c}_0 = (2103)$. Addition is in the finite field $\mathbb{F}_4$.

(g) Show that this cryptosystem has perfect secrecy if the key is uniformly distributed.

Problem 2.

The prime number $p = 149$ and $a = 2$ are given.

a) How many primitive elements exist for a prime number in general? How many exist for the p given above?

b) Show that the pair of parameters (p, a) can be used for the Diffie-Hellman key-exchange protocol (DH-protocol).

Alice and Bob choose the secret keys $x_A = 87$ and $x_B = 50$, respectively.

c) Describe the DH-protocol. Determine the values that are sent by Alice and Bob.

d) Compute the shared key.

The prime number p and the set

$$\mathcal{A} = \left\{ \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix} \middle| \; a \in \mathbb{F}_p \right\} \subseteq \mathbb{F}_p^{2\times 2}$$

are given.

e) Show that the set $\mathcal{A}$ is a cyclic group with respect to matrix multiplication. Determine a generator and the group order.

f) Formulate the DH-protocol for $\mathcal{A}$ and determine the shared key.

g) Why is this protocol insecure?

Problem 3.

a) Let $n \in \mathbb{Z}$ be odd and $a \in \mathbb{Z}_n^*$. Prove the following statement:
If $a^{\frac{n-1}{2}} \not\equiv \pm 1 \pmod{n}$ holds, then n is composite.

b) Formulate a probabilistic prime number test based on the statement given above.

c) Does the test always provide the correct answer if n is prime?

d) Is n actually composite, if the test states „n composite“?