Kryptography Sheet 2

hhu Düsseldorf
Winter term 23/24

Hand in: until monday 23.10.2023, before the lecture starts

Vorlesungswebseite: `http://reh.math.uni-duesseldorf.de/~khalupczok/krypto/`

Exercise 1: Affinlinear encryption

Consider the affinlinear encryption $E : \mathbb{Z}_n^4 \to \mathbb{Z}_n^4$, $x \mapsto Ax+b$, with $n = 26$, $b \in \mathbb{Z}_n^4$ and consider the matrix

$$A = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

We code the alphabet `A,...,Z` by `A` $\mapsto 1$, `B` $\mapsto 2$, ..., `Z` $\mapsto 0$.

(a) Describe the functionality of the encryption for $b = 0$.

(b) Give the decryption function D, for which $E \circ D = D \circ E = \mathrm{id}_{\mathbb{Z}_n^4}$, if b denotes the vector of the key word "`FLAU`".

(c) Encrypt with this b a short text of about 10 words.

(d) How many invertible matrices $A \in \mathbb{Z}_4^{2\times 2}$ are there?

(e) How many invertible matrices $A \in \mathbb{Z}_p^{2\times 2}$ are there, if p is an arbitrary prime?

Exercise 2: Riffling

Take a card deck of 2^n many cards and shuffle them as follows: Take the bottom and top cards of the deck and place them on the table to start a new deck. Then take the remaining bottom and top cards and place them on the newly started pile. Continue this procss until all cards are gone from the original pack.
For example, if the original deck has 8 cards $1, 2, \ldots, 8$, the new deck will be in ascending order $4, 5, 3, 6, 2, 7, 1, 8$.
After how many such shuffles will the cards in a deck return to their original position?

Exercise 3: Encryption with rotating stancils

We consider a square with $n \times n$ many fields, some of them are cutted holes. This stancil will be positioned on a secret text of $n \times n$ letters, such that the plain text will be read off the holes. Then the stancil is rotated by 90°, the holes will show then new letters continuing the plain text. The stancil will be rotated another two times and positioned, such that the whole text is read off.

(a) How needs such a stancil to be configured? How many such stancils are there?

(b) Give an example for such a stancil with $n = 8$, and a secret text being encrypted with it, including the plain text.

(c) What weak keys are there, i.e. what kind of stancils make an easy kryptographic attack possible?