Homework 3 in Cryptography I

Prof. Dr. Rudolf Mathar, Wolfgang Meyer zu Bergsten, Steven Corroy

10.11.2009

Exercise 7. Show that the set of regular $n \times n$ matrices over a field K together with the usual matrix multiplication is a group. Is it an abelian group?

Exercise 8. In order to prevent a frequency analysis of a Vigenère encryption with an english text as keystream, the plaintext is encrypted twice with two different keystreams.

(a) What is the probability that a character in the ciphertext results from the addition of the highly probable letters e, t, a, o, i, n?

(b) Instead of a keystream the message shall be encrypted using a keyword k_1 of length l_1 and afterwards with a second keyword k_2 of length l_2. This can be viewed as the addition of a single keyword. How long is this keyword? Choose two keywords to create a key of length $N = 35$.

Exercise 9. The plaintext of the following ciphertext is part of a famous english play. Determine the index of coincidence. What can you derive from it?

```
KPJDLCGS PVHQKWRK KCKRBKPJ DLCWILKR BGSKORKO VCVCNVEW OVQDLCIL YFIRRIGB
IVSXQKRB DLCSVCXX PKRAOWYX HMXIKKRG XLGCXGWI NVEWCQYX CNKVRC
```