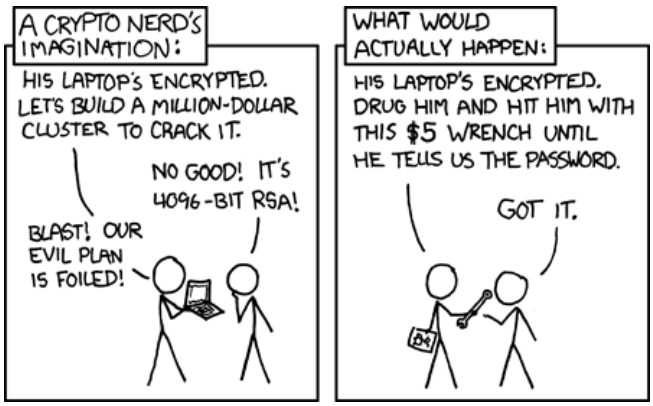
Cryptanalysis: Historical Ciphers

Lab 1 in TSIT03 Cryptography,
Institutionen för systemteknik, Linköpings universitet

Niklas Johansson*, Jonathan Jogenfors†

September 6, 2016



– http://xkcd.com/538/

*niklas.johansson@liu.se
†jonathan.jogenfors@liu.se

1 Introduction

In this laboratory work you will try to decipher three different ciphers: transposition, simple substitution and Vigenère ciphers. You have no knowledge of which method or key is used on your texts, except that you have one of each method. Before the laboratory you should read the instruction and the part of the course literature dealing with elementary ciphers. This will make the work easier. You have two hours scheduled with an assistant. Should you not finish in these two hours you can continue by yourself whenever a computer is available and report to the assistant later. If you have to use more then four hours to decipher your texts you should contact the assistant. Maybe you got a difficult text.

Do *not* hesitate to ask the assistant for help when you are stuck!

2 Goals of the lab

The goal is simple: perform a successful cryptanalysis and find the plaintexts!

3 Preparing for the lab

Before the lab you should have read up on the methods for breaking the historic ciphers as given in the lecture. It is important that you understand how the transposition, substitution, and the Vigenère cipher work, and that you have a basic idea of their weaknesses.

4 The software KNEKT

The software available to you is called KNEKT, and its main functionality is to perform frequency analysis on the given ciphers.

You can access the program at http://www.icg.isy.liu.se/courses/tsit03/knekt/

5 Performing the laboration

For each ciphertext given (as a number) to you by the assistant, you are supposed to

1. Find out (make an educated guess) which cipher method has been used (Substitution, Transposition or Vigenère).
2. Break the cipher and find the plaintext.

Begin by setting the language for the text. If you only speak English, you will be given an English text. However, if you speak Swedish, you might have been given a Swedish *or* an English text!

5.1 Hints

For the substitution cipher, the key is in the form of a word. This word is entered on the upper text line, and the rest of the alphabet follows. For instance, if the key is `HACKER`, the upper line should be `HACKERBDFGIJLMNOPQRSTUVWXYZ`. In other words, letters are picked up and moved to the left to form a word. Perhaps you can start comparing statistics from the right?

In Vigenère, the key repeats over and over again over the text. This is not a one-time pad! Instead, use the method taught in the lecture to find the key *length*, and then find the keyword with that length.