Mittuniversitetet
MID SWEDEN UNIVERSITY

Laboratory Assignment: May the (Small) Force Be with You

Daniel Bosk

monoalph.tex 2169 2015-01-14 22:37:01Z danbos

Contents

1 Introduction

The idea of this assignment is to introduce the concept of brute forcing security mechanisms. The mechanism in question here is a simple monoalphabetic cryptographic algorithm.

2 Aims

The aim of this assignment is to examine that you are:

- Able to reason about the security of basic security mechanisms.
- Have an understanding for plausible deniability.
- Able to make a proof of concept of how to break a simple and insecure mechanism.

3 Theory

If you do not have probability theory and statistics fresh in memory you are recommended to revise that. The text *Sannolikhetsteori* by Arnlind and Enblom [1] (in Swedish) treats this subject, sections 1 to 4 are recommended.

If you have previously take (or are currently taking) a course on cryptography, the material from that course covering classical cryptography is enough. Otherwise you are recommended to read *Introduktion till några klassiska chiffer* [2] (in Swedish) or chapter 1 in *Cryptography: Theory and Practice* by Stinson [3].

4 Assignment

The first part of the assignment is to break a monoalphabetic cipher. The intercepted text is the following:

> TSVCFMSFQ OÅ CFMMB LVQT TLB UBQB UÄK EÖQSQPHMB
> NFC OQPHQBNNFQJMH PDG NBSFNBSJL PDG LQXOSPHQBEJ.

Find the corresponding plaintext of this ciphertext. When you have found a plaintext and the key, think about how certain you can be that this is indeed the correct key (and thus correct plaintext).

The second part of the assignment is about spurious keys [3, Ch. 2]. By spurious keys we mean a set of n keys $k_1, k_2, \dots, k_n$ which all decrypt a ciphertext c to valid plaintexts. Your job is to construct such a ciphertext with two spurious keys k_1 and k_2 for the cryptosystem used in the first part of the assignment. The texts should be as long as possible (try to create at least a sentence), and they do not have to be both in Swedish or English – one plaintext in English and one in Swedish is fine.

Algorithmically finding a spurious key should be possible, in this case, by generating plaintext using n-grams. However, using pen and paper is probably the most straightforward way, and probably the fastest for this assignment.

5 Examination

You must submit your solutions to the assignment in a report (PDF-format) in the course platform. The report must contain the following:

1. The plaintext from the cryptotext given above with an explanation of what makes you sure this is the correct plaintext.

2. One ciphertext c, two keys k_1 and k_2 and the corresponding plaintexts m_1 and m_2, such that $E_{k_1}(m_1) = c = E_{k_2}(m_2)$. Also explain your method for creating $c, k_1, k_2, m_1.m_2$ and why we want to have spurious keys. Also, how is the length of the message affecting the spurious keys?

References

[1] Joakim Arnlind and Andreas Enblom. “Sannolikhetsteori”. KTH:s matematiska cirkel 2007–2008, Kungliga Tekniska högskolan. 2007. URL: `http://www.math.kth.se/cirkel/2007/kompendium07.pdf`.

[2] Daniel Bosk. “En introduktion till kryptografi”. 2013. URL: `http://ver.miun.se/courses/infosak/compendii/introcrypt.pdf`.

[3] Douglas R. Stinson. *Cryptography : theory and practice*. 3rd ed. Boca Raton: Chapman & Hall/CRC, 2006. ISBN: 1-58488-508-4 (Hardcover).