MTAT.07.006 Research Seminar in Cryptography
Comments on
"The Enigma Cipher Machine" survey by Kadri Hendla

Aleksandr Grebennik

December 3, 2005

1 Introduction

The purpose of this document is to give comments on Kadri Hendla's survey The Enigma Cipher Machine. Enigma is a portable cipher machine, famous for the role it played in World War II. The survey gives an in-depth overview of

- the construction of Enigma cipher machine,
- the techniques used in encoding messages with Enigma and
- some approaches used to decipher the encrypted messages.

2 General Remarks

The overall impression of the survey is good. It covers a lot of ground on Enigma-related topics.

The survey is structured in a logical way, describing the development of Enigma machine and cryptographic attacks to break Enigma code in the chronological order they appeared in.

The only thing that the reader is left wishing for are illustrations, as they would make understanding the inner structure of Enigma machine considerably easier. But one can always find these illustrations in [1].

3 Comments and questions

The Germans were never exposed to the risk of encoding different letters with the machine being in the same state (within one message). This is because the period of machine was much larger than the size of a message [1]. Otherwise, the attackers would have much more info about the initial position of the rotors. This fact is not mentioned in the survey.

It is also interesting how (fast?) could Enigma encryption be broken using the computational power available nowadays. Another question is what influence Engima has had on the present cryptography.

References

[1] Enigma Machine from Wikipedia, the Free Encyclopedia.
http://en.wikipedia.org/wiki/Enigma_machine

[2] K. Hendla. MTAT.07.006 Research Seminar in Cryptography: The Enigma Cipher Machine, November 28, 2005.