SSN Practicum
week 1, part 1

E.P. Schatborn

31 October 2011

1 Introduction

You are to decoded your first cipher! In this the assignment you will look at encoding/decoding more closely... Update your log; give more than just an account of the questions/answers posed in this assignment. Especially during group work it should be clear form the logs who did what, why and when.

2 Installing Windows

1. Download the Windows Server 2003 VLK image from the OS3 website:

`http://software.os3.nl/`

Before you can install Windows Server 2003 to your server, you have to create an installation medium. You can burn the disk image to CD-ROM, or create a bootable USB stick. Perhaps there are more ways to get the job done?

2. Decide upon the installation medium to use. Create the installation medium and document the steps you took.

During the installation, Windows will ask you for a license key. Niels, the OS3 system administrator, will provide you with this key. Send him a PGP signed email with a request for the license key. If you do not use PGP, knock on his door and provide him with a piece of paper and a pen.

3. Install Windows to the second drive of your server.

Make sure that, as with Ubuntu, you can work remotely. You can use `rdp` for instance.

3 Crypto

Download and install the Simon Singh Codebook CD-ROM. You can find it in the SSN wiki page:
`https://www.os3.nl/2010-2011/courses/ssn/start`

Go through the Codebook CD-ROM. We will look at everything upto and including Vigenre ciphers.

1. Choose maincontents and go through the first three chapters of the Birth of cryptography upto and including Mechanising secrecy.
   (a) What is Affine?
   (b) What is Playfair?
   (c) What is ADFVGX?
   (d) On what principles of operation is the Bombe based?
2. Encrypt an english text of at least 80 words using the Vigenre cipher and exchange it with one of your fellow students.
3. Crack the crypted text of you fellow student using the Vigenre cipher tool.
4. Go through the previous two steps again, this time using a cipher of your own choosing. Do not tell your fellow student what cipher you used!
5. Go through the parts about Enigma from Mechanising secrecy insofar as you have not done that yet.
   (a) On what principles of operation is the Bombe based? (from last assignment)
   (b) Calculate how many permutations the Enigma can generate. Show the effects of Steckerbrett and the number of wheels.