188.339 Security VU, SS 2006

Assignment 4: Caesar and Linguistix - Break this cipher

Mode: solo, NO groups

Language: german or english

Grading: 10 points (3pt description of the principle of the cipher, 3pt description of the crypto-attack, 4pt correct key and plaintext)

Deadline: Fr. 12.05.06, 23:55

This assignment is part one of two assignments which are linked. In this first exercise you will break a cipher and decrypt a secret message. Your task in assignment two will be to write an algorithm which enables you to reply a message which is encrypted the same way and thus be able to correspond with the sender without him taking notice (and therefore be able to follow an encrypted correspondence and even alter messages).

The whole of Europe is under Roman rule, all except one tiny village…
You are Linguistix, a sharp witted and gifted scholar in a small village inhabited by a group of gauls, which to this time was still undefeated by the Roman troops. One day, when you are taking a little walk through the nearby woods you find a Roman soldier who has obviously lost the direction on his way to the Roman camp. When he takes notice of you he first turns to run away but on a second thought he looks at you and apparently identifies you as being no immediate threat to him (There have been rumours of incredibly powerful gauls in the roman camps lately). The moment he overbears his fear and is taking breath to ask you the way to the camp all of the sudden a giant menhir (an obelisk) falls from the sky and buries all of him but his head. As his helmet falls off, a letter appears which is sealed with Caesars seal. You get very excited, take the letter and run home. On your way you meet Obelix who asks you for his menhir which he had lost when he stumbled across his dog Idefix – you quickly point at the soldier behind you and hurry to come home.

“What could it be, that Caesar himself is writing a letter to the Roman camp nearby our village?” you keep asking yourself. In your cottage you lock yourself in your study – room and open the letter, but what you see is nothing to be excited about:

You find Caesar’s letter in the cipher x.txt file, where x is 0-9. Please choose the file with the number that corresponds to the last number of your matriculation number, e.g.:

0106417 chooses cipher 7.txt
0302659 chooses cipher 9.txt
0206520 chooses cipher 0.txt

Answer the following Questions and you will be able to read Caesar’s letter to the Romans!

- What kind of cipher was used by Caesar to make this message unreadable for those recipients who are not entitled to do so? Describe the principle and the actual key that was used.
- Describe in detail how you obtained the key (include every step of your analysis and tell which letters where obtained by which step).
- Write down the decrypted text in the pdf file.

DELIVERABLES:

Create one pdf file that contains the answers to the questions above.
If you wrote an application for decrypting, add the code to your pdf. (We don't care which programming language you use, but the second assignment has to be implemented in Java)

Load it up through the web interface until the deadline.
The pdf should be named as follows: **sec_4_matnr_surname.pdf** (example: sec_4_0043546_weippl.pdf)
Put down name, matriculation number and your email on the front page of your document.

Hints:

1) *You may know Caesar's Cipher, if you don't - look it up somewhere. It will give you a direction, but it's not as easy as Caesar's Cipher.*
2) *The plaintext is in English.*
3) *You might want to write some lines of code to examine the cipher.*
4) *Don't be intimidated by the length of the text! You know, the longer the text, the easier it is to decrypt. Again, you may find it easier if you write yourself a little program.*