Security

Assignment 2, Thursday, September 18, 2014

Handing in your answers: the full story, see

`http://www.sos.cs.ru.nl/applications/courses/security2014/exercises.html`

Briefly,

- submission via Blackboard (`http://blackboard.ru.nl`);
- one single pdf file;
- make sure to write all names and student numbers and the name of your teaching assistant (Gergely or Fabian).

Deadline: Thursday, September 25, 24:00 (midnight) sharp!

Goals: After completing these exercises successfully you should

- be able to encrypt and decrypt using simple substitution ciphers;
- be able to break simple monoalphabetic substitution ciphers;
- be able to encrypt and decrypt using simple transposition ciphers;
- be able to break simple transposition ciphers.

Marks: You can score a total of 10 points.

1. **(2 points)** You are newly employed at the military intelligence. Your first job is to distribute incoming ciphertexts over the correct departments. So, ciphertexts made with substitution ciphers should go to the substitution cipher department (Caesar, mono-alphabetic, Vigenère, etc.), while ciphertexts made with transposition ciphers should go to the transposition cipher department (Scytale, railfence, simple block-based, etc.). You are given some ciphertext (the middle part of a long ciphertext). How can you tell the type of encryption without actually breaking the code?
   (a) If it is a substitution cipher ...
   (b) If it is a transposition cipher ...
2. **(4 points)** Break the mono-alphabetic substitution cipher (so, the key is just a permutation of the English alphabet) used to generate the following ciphertext. The plaintext is written in English. Explain your approach to breaking the cipher.

```
gsvkzgslugsvirtsgvlfhnzmrhyvhvglmzoohrwvhybgsvrmrjfrgrvhlugsvhvourhszmwgsvgbizmm
bluveronvmyovhhvwrhsvdslrmgsvmznvluxszirgbzmwtllwdroohsvksviwhgsvdvzpgsilftsgsve
zoovblugsvwzipmvhhulisvrhgifobsrhyilgsvihpvvkvizmwgsvurmwviluolhgxsrowivmzmwrdro
ohgirpvwldmfklmgsvvdrgstivzgevmtvzmxvzmwufirlfhzmtvigslhvdslzggvnkgglklrhlmzmwwv
hgilbnbyilgsvihzmwblfdroopmldrzngsvoliwdsvmrozbnbevmtvzmxvfklmblf
```

3. **(4 points)** You are given the following ciphertext encrypted with a transposition cipher:

```
mocianommeattshtakloekpmeapnhwiertyedtggnseioeosnnhtimpocegeltm
ofyolplroswfnootuasreaditmeeteetnighyiuonfocttlpomfeoexxsxlxxxx
```

   (a) How can you immediately tell, by only looking at the ciphertext that a transposition cipher was used?
   (b) What is the probable block length? How would a simple change of the scheme (no change of the permutation) make it much harder to figure out the block length?
   (c) Exploit this vulnerability. Find the plaintext, explain briefly how you did it.