Security

Assignment 2, Friday, September 16, 2016

Handing in your answers: For the full story, see

`http://www.sos.cs.ru.nl/applications/courses/security2016/exercises.html`

To summarize:

- Include your name and student number **in** the document (they will be printed!), as well as the name of your teaching assistant (Hans or Joost). When working together, include **both** your names and student numbers.
- Submit one single **pdf** file – when working together, only hand in **once**.
- Hand in via Blackboard, before the deadline.

Deadline: Monday, September 26, 09:00 sharp!

Goals: After completing these exercises successfully you should be able to

- reason about characteristics of substitution and transposition ciphers;
- break mono-alphabetic substitution ciphers;
- break simple transposition ciphers.

Marks: You can score a total of 100 points.

1. **(35 points)** This exercise concerns mono-alphabetic substitution. Consider the following ciphertext:

```
vbpfaop qnvq csf ysoq xvbz vrsfq qnz bapnq qs ebadvxc rzxvftz csf nvdz
osqnaop qs nayz at os yakkzbzoq qnvo tvcaop csf ysoq xvbz vrsfq kbzz
tezzxn rzxvftz csf nvdz osqnaop qs tvc
```

   (a) Break the substitution cipher that was used to create the ciphertext. Explain your approach.

   (b) How many keys are possible for a substitution cipher using the (lowercase) English alphabet? Keys that leave some or all characters unchanged are allowed.

2. **(40 points)** Consider the following ciphertext, which is the result of a columnar transposition cipher:

```
svatxrmitxridoxoeidxidfaamarntyachx
```

   (a) Which property of columnar transposition ciphers can immediately be seen in the ciphertext?

   (b) What is the most likely key size? Explain your answer.

   (c) Find the plaintext. Explain your approach.

3. **(25 points)** In this exercise, we will look at the Rail Fence transposition cipher. To encrypt a message using this cipher, it is written along the 'rails' of a 'fence', zigzagging from top to bottom and back. Note that the number of rails can vary: this is the 'key'! As an example, the text "Attack the hill at dawn" on a fence with 3 rails is shown on the next page.

.... **The assignment continues on the next page!** ....

```
A . . . C . . . E . . . L . . . A . .
. T . A . K . H . H . L . A . D . W .
. . T . . . T . . . I . . . T . . . N
```

The ciphertext is obtained by reading along the fence from left to right, top to bottom. For the above example, the ciphertext would be `ACELATAKHHLADWTTITN`.

(a) Is there a limit to the number of rails that can be used before the cipher is trivially broken? Explain your answer.

(b) Given the ciphertext `DRTUUOESIRIMDSYLCTBEAMLEIGLRRN`, find the corresponding plaintext and explain/show how you found it.