Security

Assignment 2, Friday, September 22, 2017

Handing in your answers:

- Include your name and student number **in** the document (they will be printed!), as well as the name of your teaching assistant (Bart 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, October 2, 09:00 sharp!

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

- reason about characteristics of substitution and transposition ciphers;
- use and break substitution and transposition ciphers.

Marks: You can score a total of 100 points.

1. **(10 points)** Imagine that you are given a fragment of ciphertext based on some (sufficiently long) English plaintext. Assume it's the output of either a substitution or a transposition cipher. How can you tell which cipher was used, without breaking the code?
2. **(30 points)** Consider the following ciphertext output of a mono-alphabetic substitution:

   ```
   Dko hxyyxr goxglo gbct jxb bcnr, kocldkt hknlabor, cra c spyyob
   dkcd rovob oras. Nd ns rx ycddob dx dkoy nj dko knwk lxbas glct
   dkonb wcyo xj dkbxros, sx lxrw cs dkot cbo lojd nr gocho.
   Dkot rovob cbo.
   ```

   (a) Find the matching plaintext by breaking the substitution cipher. Describe your method.
   (b) How many keys are possible for a substitution cipher using the (lowercase) English alphabet? Keys that leave some or all characters unchanged are also allowed.
3. **(35 points)** Consider the following ciphertext, which is the result of a columnar transposition cipher:

   ```
   aeiycnwcmrneedvrt#irsgitaoear#peaos#rfsiegselnsh
   ```

   (a) Which two properties of transposition ciphers can be observed from the ciphertext?
   (b) What is the most likely key size? Explain your answer.
   (c) Find the plaintext. Explain and show your approach.
   (d) Sticking with the same key size, how could you make the scheme harder to break?
4. **(25 points)** Read about the Playfair cipher: `https://en.wikipedia.org/wiki/Playfair_cipher`. In this exercise, we will use the variant that uses 'I' for both 'I' and 'J'.

   (a) Using the key 'Albus Dumbledore', write down the 5x5 key grid.
   (b) Briefly explain how decryption works (i.e. how it differs from encryption)
   (c) Use the grid to decrypt the following ciphertext:

   ```
   CU XB TG PM BZ AI LK EG HM LQ MO XD TF PK GO CD DT RB QR IN
   FR RB CG MQ OR WM ZO OE OE EG IR QR QS MT MQ QI MB CH IQ
   ```