Security

Assignment 2, Wednesday, September 16, 2015

Handing in your answers: the full story, see

`http://www.sos.cs.ru.nl/applications/courses/security2015/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 (Brinda or Joost).

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

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

- encrypt and decrypt using simple substitution ciphers;
- break substitution ciphers;
- encrypt and decrypt using Vigenère cipher.

Marks: You can score a total of 100 points.

NOTE 1: For the following cipher decryption exercises, 'I used a computer' is not accepted as an explanation.
NOTE 2: All plaintext is in English.

1. **(30 points)** Consider the following simple substitution cipher.

   ```
   VG HFRQ GB OR RKCRAFVIR GB ZNXR GUVATF CHOYVP NAQ PURNC GB ZNXR GURZ CEVINGR ABJ
   VGF RKCRAFVIR GB ZNXR GUVATF CEVINGR NAQ PURNC GB ZNXR GURZ CHOYVP
   ```

   (a) Find the key and the plaintext. Briefly explain your approach.

   (b) What is the relation between encryption and decryption in this particular case?

2. **(30 points)** Break the substitution cipher (so, the key is a permutation of the English alphabet) used to generate the following ciphertext. Give the plaintext and briefly explain your approach to breaking the cipher.

   ```
   EMQQHGE WCJGE VHQT JQTMOP HP QTM MPPMGLM JF EMQQHGE
   WTMWA PSLLMPP IMHGE CHGBMA VHQT LJJKMOWQHJG
   ```

3. **(40 points)** Read about the Vigenère cipher: `http://en.wikipedia.org/wiki/Vigenere_cipher` and answer the following:

   (a) Decrypt the following Vigenère cipher text using the key 'franzk'.

   ```
   gpbrksjmiafzfjsvnxfkeyxssjozddmzntsrfksghvquorrxtkekhcynepqofkevs
   dmvnbmoczsgdxyzsjgkyvvrqgjyaidxtkshepntirmdqpdrrswvd
   ```

   Explain briefly how you did it.

   (b) A person called Brandon wants to encode the following message:

   ```
   The turtle wears a silver pair of gloves
   ```

   Brandon decides to encrypt it with a Vigenère cipher using his own name as the keyword. What will the secret message look like once it is encrypted? (Ignore the spaces and capital letters.)

   (c) Suppose we use Vigenère cipher and restrict the words that can be used as key to consist of only vowels (a,e,i,o,u). Does this affect the security of the encryption? Briefly explain.