

Lab2: Cracking a Vigenere Cipher

Submission due: Monday, July 3, 2017

(updated on May 29, 2017)

Objective: Given a piece of ciphertext generated with a Vigenere cipher, find its encryption key and recover the corresponding plaintext.

Project procedure:

1. This is an individual based project. Download the [ciphertext assigned to you](#).
2. Use **Kerckhoff's method** in your computer program to find the key length and then the key to the Vigenere cipher.
3. Recover the plaintext.
4. Demonstrate your result to GA on a computer.
5. Organize your results in project report and submit the report before the submission deadline.

Programming language: C language

Project report contents:

1. Cover page:
 - course title and number, lab title, your name and student ID;
2. The result page includes
 - The ciphertext, encryption key (in the form of English letters), and the plaintext
 - The number of coincidences for different amount of shifts. A list or table can be used. Note that **this part has up to 50% marking weight**.
 - Amount of shifts can range from one shift to 3-4 times of expected key length.
 - [A sample result](#) can be found here.
3. Your program source code

Project report format:

1. Arrange the report in one single file in either word, pdf or txt format;
2. Filename should be coined as your ID, i.e., 103456789.pdf.

Submission Method:

- Submit your project report through Blackboard in the same way as submission of an assignment.

Project Grading:

- The full marks for Lab 2 are 100, which has 5% of the total course weight.