Computer Security (22C:169) Spring 2016

Assignment 1. **Deadline**: Monday, February 22, 23:59.

Submission format:

To make the submissions easier to process, please submit your assignments as a single archived file with your full name and the assignment number on it, e.g. Lastname_Firstname_Assignment_1.zip
Submit all files, except from the source code and input files, in a PDF format to preserve the layout.

Part 1 (Spaces). In this assignment you are given three encryption algorithms discussed in the class. You are asked to select two of them and implement.

- **Implementation:** implement your selected algorithms in either C/C++/C#, Java or Python. If you have problems with programming in these languages, please contact me right away. **INPUT** – pass all input files to your code either as external text files or from the command line.

Then, you will need to select plaintexts to encrypt using your implemented algorithms.

- **Plaintext:** The text should be in English and from the classic literature. The **lengths** of the plaintexts vary for different algorithms and are specified below.

Note: *You can select two plaintexts – one for each algorithm, or use the same plaintext for both algorithms (if appropriate). Just make sure the lengths of the plaintexts meet the requirements for the algorithms as given below.*

Choose two of the following algorithms:

1. **Vigenèr cipher**, *use a keyword of no longer than 7 letters, and a plaintext of approximately* 2 000 *letters.*
2. **Permutation cipher**, *use a key of no longer than 7 letters, and a plaintext of approximately* 2 000 *letters.*
3. **Simple Enigma machine**: *with one rotor only. The rotor is initialized by a shuffled alphabet and performs a shift after each letter is encrypted. That is, the rotor gets to the initial position after encrypting 26 letters. If you chose this algorithm, select a longer plaintext of up to* 15 000 *letters.*

However, you will need to preprocess your planetext to make the attack harder. First do a naive preprocessing:

- **Preprocessing:** Replace all capital letters with lower-case ones and remove the punctuation marks, but **keep spaces.** To simplify the assignment: if your text contains **numbers** or **special characters** remove them or select a plaintext with no numbers and special characters. In general, if you want to encrypt texts with special characters and numbers the common approach is to extend the alphabet with these symbols and agree on their order. Then use the original algorithms.

- **Keep the spaces** in the ciphertext in their original positions (just as they are in the plaintext). Remember the first shift cipher breaking example we had in the class -- the encryption was preserving the lengths of the words. This contributed to breaking of the cipher.

Encrypt your plaintext(s) using **two** of the three encryption algorithms given above.

What you need to provide in your submission: **Read the next page...**

You need to provide:

1. **Algorithm Description:** A brief description of the algorithms you choose;
2. **I/O:** Plaintexts you chose and corresponding ciphertexts in separate text files;
3. **Keys:** The secret keys used;
4. **Source Code:** Submit your source codes and additional input files (if any used);
5. **How to run/compile:** Giving ALL the necessary instructions for execution (command line compilation/execution options, etc.) so that your submission can be reproduced. Specify the compiler version you used.

Part 2 (No Spaces). Same task, but with different preprocessing to make the attack even harder.

- **Plaintext:** This time select a different plaintext(s), with the same length requirements as in Part 1 of the assignment. As before, the text should be in English and from the classic literature.

- **Preprocessing:** This time, **remove the spaces,** and do the rest as before: remove the punctuation marks, replace capital letters with lower-case ones; if your text contains **numbers** or **special characters** remove them or select the original plaintext with no numbers and special character.

- **Encrypt the new plaintext(s):** using the **same two** algorithms that you have selected and implemented in Part 1, but use **new keys** (with the same length restriction - no longer than 7 letters for Vigenèr and Permutation ciphers).

Note: *as in Part 1, you can either select two different plaintexts - one for each encryption algorithm, or use one plaintext for both algorithms if appropriate.*

You need to provide:

1. **I/O:** Plaintexts and the corresponding ciphertexts used for the Part 2 in separate text files.

2. **Keys:** The secret keys used for the Part 2 of the assignment.

In a follow-up assignment you will be breaking each-other's ciphertexts.