Assignment 1

Phase1

(Deadline: 23rd May)

NOTE:- We have paired you up for this assignment. The work that you do now is individual work. DO NOT share any files, or any information with anyone (not even your partner).

General Instructions

- Consists of 2 sub-assignments.
- You will have to write computer programs (in any language) for encryption
- For all these assignments “use lower case english alphabets only” for message, key and cipher-text
- Different messages for each of following encryptions is recommended.
- The message, key, cipher-text and program should be present in separate files.
- The program can read message and key files and should output the cipher-text to another file. Do not store key or message in program file.

Steps to be followed:

1. Pull latest changes from GitHub.
2. Under IE/-NITK/Crypto-SMP-2019/Assignment1 , create a folder Yourname/
3. All your files are to be placed in Yourname/
4. Refer Example/ for sample directory structure

Questions

- Caesar Encryption:
Write a program to encrypt a message(about 200 words, just pick some random paragraphs from somewhere) of your choice using Caesar cipher.
The keyfile is not needed for this question
Name the:
Program file as yourname-caesar_encryption.extension
and
Cipher-text file as yourname-caesar_ciphertext.txt

- Vigenere Encryption:
Write a program to encrypt a message(about 200 words, just pick some random paragraphs from somewhere) of your choice using Vigenere cipher.

Name the:
Program file as yourname-vigenere_encryption.extension
and
Cipher-text file as yourname-vigenere_ciphertext.txt

Message and Keyfiles

Make sure you have these saved somewhere for the next Assignment. **DO NOT** push the message and keyfiles to GitHub.

Name them using this convention (No keyfile for Caesar's needed):
yourname-message-caesar.txt
yourname-keyfile-vigenere.txt
and so on.

Phase 2

(Deadline: 25th May)

In essence , you are carrying out a Cipher-Text(CT)-Only attack. The key is available to you (except for caesar). The task is made easier as you know beforehand what Cipher was used where.
=======
In essence , you are carrying out a Cipher-Text(CT)-Only attack. The key is not available to you (except for vigenere). The task is made easier as you know beforehand what Cipher was used where.

This is a team assignment. Proceed only once your partner's PR has been merged.
You may now help your partner in case he/she is unable to complete phase 1. Be honest, and provide only conceptual help. Sharing keyfiles and messagefiles defeats the fun and purpose!

If your PR has not been merged, but your partner's has, you may start this phase, but first ensure you complete Phase 1 so that your partner can also start working.

General Instructions

- Consists of 2 sub-assignments (one corresponding to each in Phase 1).
- You will have to write computer programs (in any language) for decryption.
- The decrypted message and program should be present in separate files.
- The program can read ciphertext and should output the message to another file. Do not store the message in program file.

Steps to be followed:

1. Pull latest changes from GitHub.
2. Confirm that your partner's files are in the repo. (Indicates his/her PR was merged)
3. Read your partner's ciphertext. DO NOT modify it.
3. All your files to be placed in Yourname/

4. Refer Example/ for _updated_ sample directory structure.

Tasks

- Caesar Attack:
Write a program to decrypt your partner's Caesar Ciphertext.
Name the:
Program file as yourname-caesar_decryption.extension
and
Decrypted Message file as yourname-caesar_decrypted.txt

- Vigenere Attack:
Write a program to decrypt your partner's Vigenere Ciphertext. For this **you are allowed to use the key file of your partner** (ask your partner for the key file) because decrypting vigenere without the key is quite challenging.
Name the:
Program file as yourname-vigenere_decryption.extension
and
Decrypted message file as yourname-vigenere_decrypted.txt

Good Luck!