CSC 541 Cryptography and Network Security

Instructor: Dr. Natarajan Meghanathan

Project 1

Implementing the Encryption and Decryption Algorithm using Vignere Cipher

Assigned: September 14, 2015 **Due: October 14, 2015, 4 PM**

Goal of the Project

In this project, you will develop the code to encrypt and decrypt using Vignere Cipher. Given a plaintext and a string of characters as key, you will implement the Vignere Cipher encryption algorithm to compute the ciphertext. Similarly, given the ciphertext and a string of characters as key, you will implement the Vignere Cipher decryption algorithm to generate back the plaintext.

Vignere Cipher

In this project, you will implement the Vignere Cipher, a stream cipher: so, you will encrypt one character at a time. Assume for simplicity, all characters to be encrypted and decrypted are only uppercase characters (A-Z). The Vignere Cipher takes a character-string (all uppercase characters: A-Z) as the key.

Encryption algorithm

A key string is written parallel along with the plaintext. If the end of the key is reached, the key string is continued by repeating the key. This is continued till the last plaintext character is reached.

If you encounter a non-uppercase plaintext character, do not use the character from the key string, just skip that plaintext character and proceed to the next plaintext character. In other words, the non-uppercase plaintext character appears as it is in the ciphertext too.

For every character index i, $C[i] = P[i] + K[i]$

Decryption algorithm

A key string is written parallel along with the ciphertext. If the end of the key is reached, the key string is continued by repeating the key. This is continued toll the last ciphertext character is reached.

If you encounter a non-uppercase ciphertext character, do not use the character from the key string, just skip that ciphertext character and proceed to the next ciphertext character. In other words, the non-uppercase ciphertext character appears as it is in the plaintext too.

For every character index i, $P[i] = C[i] - K[i]$

Example on the working of Vignere Cipher

Key: ZEBRA

Plaintext: NATARAJAN MEGHANATHAN
Ciphertext: MEURRZNBE MDKI RNZX I RN

Plaintext	N	A	T	A	R	A	J	A	N		M	E	G	H	A	N	A	T	H	A	N
KeyString	Z	E	B	R	A	Z	E	B	R		A	Z	E	B	R	A	Z	E	B	R	A
Ciphertext	M	E	U	R	R	Z	N	B	E		M	D	K	I	R	N	Z	X	I	R	N

Plaintext and Key to be Used:

The Plaintext is your first name followed by your last name (with a blank space in between) as my name in the example shown in the previous page.
Key to be used: the city where you reside (e.g., BRANDON)

What is required for you to do?

You need to implement the encryption algorithm and decryption algorithm for Vignere Cipher as described above, as two separate programs (one program for encryption and another for decryption).

Your encryption algorithm should input the plaintext (your full name, with a blank space in between your first name and last name) as a string of uppercase characters and a one-word character string as the key (the city you reside). Implement the encryption algorithm as described above to generate the ciphertext. **Your encryption algorithm program should output the ciphertext**.

Your decryption algorithm should input the ciphertext generated from the encryption algorithm as a string of uppercase characters and the one-word character string as the key (the city you reside). Implement the decryption algorithm as described above to get back the plaintext.
Your decryption algorithm program should output the plaintext.

What to submit?

Hardcopy (submit in class on the due date/time) and
Softcopy (email me: natarajan.meghanathan@jsums.edu)

(1) The code for the encryption algorithm
(2) A sample screenshot showing the encryption algorithm taking the input plaintext and the one-word character string as the key to generate the ciphertext.
(3) The code for the decryption algorithm
(4) A sample screenshot showing the decryption algorithm taking the ciphertext generated from the encryption algorithm and the one-word character string as the key to get back the plaintext.

Video
A Desktop recorded video (displaying your code, in full or in parts) with your explanation on the different sections of the code (starting from the execution in the main function) and walk through the code explaining how it will be executed starting from the input phase to the output phase (both for the encryption and decryption algorithms). You should show the execution of the programs for the input assigned to you.
Note that even though I am not specifying a minimum time for your video, your video explanation is expected to last at least for 8-10 minutes and should cover all of the above required explanations. Note that the contents of the desktop/programs captured through your video should be clearly readable.

Upload the video to your JSU email account using Google Drive and email me (natarajan.meghanathan@jsums.edu) the link to download it.

You could try using one of the desktop recording software (or anything of your choice):
CamStudio: http://sourceforge.net/projects/camstudio/files/legacy/
Debut: http://www.nchsoftware.com/capture/index.html