RIT Dubai

CSCI 462: Introduction to cryptography

Project1

Objective:

Students will be able to understand the way classical encryption algorithms works, demonstrated via a GUI (optional) that explains the detailed steps followed to implement that algorithm, as well as the importance of having efficient and strong encryption and decryption algorithms. They will be able propose a decryption algorithm that corresponds to a certain encryption algorithm and implement it. The ability to analyze such techniques using frequency analysis of single letters, diagrams, trigrams is a key skill in this project.

[CLO1. Implement and cryptanalyze classical ciphers.]

What is the project?

Consider an encryption algorithm that works as follows

1- An initial key is exchanged based on a mono-alphabetic initial substitution table or configuration that is shared between the two communicating parties in addition to a number that represents the location of the shift-key SK in the cipher text.
2- Encryption is done by substituting the first (SK-1) plain text letters with cipher text letters according to the initial configuration.
3- The letter number SK is added to the plaintext to represent the number of shifts of letters in the initial configuration in a cyclic manner, i.e. mod 26. The added letter is also encrypted using the initial configuration.
4- The second set of (SK-1) plain text letters should be mapped to cipher letters according to the new configuration of the mono-alphabetic substitution. A new letter is added to represent the number of shifts of the letters to produce the third configuration or table. Again this added letter is encrypted using the second configuration.
5- This process repeats for the rest of the characters. The selection of the shift letters that are added to the text should be based on a static set of letters chosen by the party that encrypts the plain text. The use of these letter can be

repeated for more than one round in case the plain text is longer than what can be supported by one round.

Example:

Assume the following initial configuration (red table) that represents the key along with the SK=9 which mean the 9th character is the shiftkey.

abcdefghijklmnopqrstuvwxyz
hilwmkbdpcvazusjgrynqxofte

Now consider the following plain text and its corresponding cipher text. Since we have SK=9 then the first 8 letters have been encrypted using the first table (in red). Assume that the sender has chosen {e, b, d} as the set of shift letters. Letter **e** represents a shift of 4 and results with the second table (in blue). Accordingly, the second part of 8 letters are encrypted based on the second table. The next SK letter is b=1 and results in the third table (in green) which is used in encrypting the third part of 8 letters according to the substitution specified in that table. The last SK is d=3 that produces the fourth table according to which the last 7 letters are encrypted.

Plain text: green car has been detected on campus
Plain text-with shift letters: green car**e** has been d**b**etected o**d**n campus
Cipher text: brmmu lhr**m** wos fhhc e**f** esefset c**t**k qymdzv

abcdefghijklmnopqrstuvwxyz
oftehilwmkbdpcvazusjgrynqx

abcdefghijklmnopqrstuvwxyz
xoftehilwmkbdpcvazusjgrynq

abcdefghijklmnopqrstuvwxyz
ynqxoftehilwmkbdpcvazusjgr

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

The **deliverables and Rubrics** of this project are the following:

1. write a pseudo code that represents the encryption and decryption algorithms (15%).
2. Implement the encryption and decryption algorithms using any Programming language and using good programming practices. (30%)
3. Third: Implement an automated frequency analysis technique using frequency analysis of single letters, diagrams, trigrams and other elements of frequency analysis. (30%)
4. Implement a GUI or a console interface to communication with the user. This interface should present to the user how the encryption and decryption algorithms work step by step for any initial substitution table and shiftkey provided by the user. (15%)
5. Write a report to document all the steps above. This report should contain all the elements of a well-organized report such as introduction, objectives, description of the algorithm and the development of the decryption algorithm, implementation specifications, analysis and discussion of results, summary, references, and add your code as an appendix. (10%)