ST. FRANCIS INSTITUTE OF TECHNOLOGY
DEPARTMENT OF INFORMATION TECHNOLOGY
SECURITY LAB

Experiment – 3: Implementation of Vignere Cipher

Aim: To simulate and analyze the process of Vignere Cipher.

Objective: After performing the experiment, the students will be able to understand the steps of vignere cipher encryption and decryption.

Lab objective mapped: L502.1: Students should be able to apply the knowledge of symmetric key cryptography to analyse secrecy of simple ciphers.

Prerequisite: Basic knowledge of cryptography.

Requirements: C/C++/Java/PYTHON any suitable programming language

Pre-Experiment Theory:

The Vigenère cipher is a method of encrypting alphabetic text by using a simple form of polyalphabetic substitution. It is a way of encoding a message using a keyword as the key. The Vigenère cipher was developed by Giovan Battista Bellaso in the 16th century and later misattributed to Blaise de Vigenère.

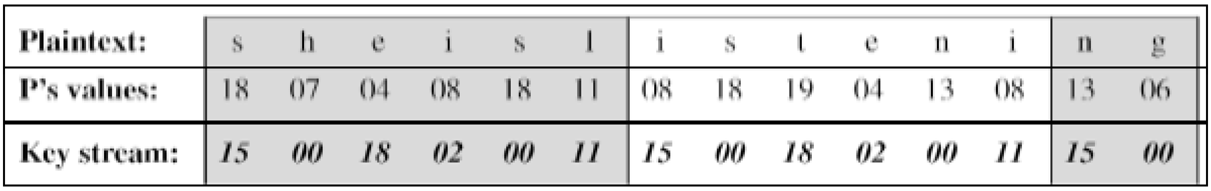
Here's how the Vigenère cipher works:

1. Key Setup:

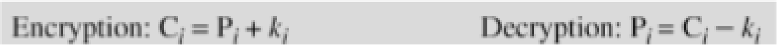
   Choose a keyword that both the sender and the receiver agree upon in advance. The keyword is repeated as necessary to match the length of the plaintext message.
   E.g. let the keyword be ‘pascal’.
   Convert it into corresponding key stream. E.g. keyword ‘pascal’ = key stream ‘15 00 18 02 00 11’

2. Encryption Process:

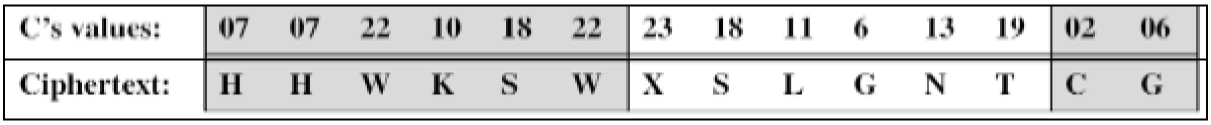
   Let Plaintext= message = “She is Listening”
   To encrypt the message, following method is used.



Plaintext:	s	h	e	i	s	l	i	s	t	e	n	i	n	g
P’s values:	18	07	04	08	18	11	08	18	19	04	13	08	13	06
Key stream:	*15*	*00*	*18*	*02*	*00*	*11*	*15*	*00*	*18*	*02*	*00*	*11*	*15*	*00*



Encryption: $C_i = P_i + k_i$ Decryption: $P_i = C_i - k_i$



C’s values:	07	07	22	10	18	22	23	18	11	6	13	19	02	06
Ciphertext:	H	H	W	K	S	W	X	S	L	G	N	T	C	G

The encrypted message becomes "HHWKSWXSLGNTCG"

3. Decryption Process:

To decrypt any message, the receiver needs to know the Ciphertext and the keyword. Then he needs to subtract the key value from the ciphertext value. This is represented with an equation in the figure above.

The Vigenère cipher was an advancement over the more straightforward Caesar cipher since it uses a keyword, making it more challenging to break through frequency analysis. However, it is still a relatively weak cipher compared to modern encryption methods.

Procedure:

1. Write a program in C/C++/Java or Python to encrypt and decrypt the given input using vignere cipher.
2. Test the output of program for following Inputs:
   a. Plaintext = "She is Listening" with keyword: Pascal. Also check if decryption works.
   b. Plaintext = "The house is being Sold Tonight" with keyword: Dollars
   c. Plaintext = Your complete name with keyword: Hello
3. Test the output of program for following Inputs:
   a. Ciphertext = "SMFPBZMYLWHMZYRAKPZIS " with keyword: HEALTH
   b. Ciphertext = "OINCMMBLSRKHJMVSJIYIITW " with keyword: security

Output:

1. Attach the complete code performing encryption and decryption.
2. Attach the program output for encryption and decryption of all the inputs given above.

Post Experimental Exercise-

Solve following on the journal sheets.

1. Encrypt and decrypt your complete name with keyword 'Hello' using vignere cipher.
2. Write in detail the strength and weaknesses of vignere cipher.

Conclusion:

We studied the procedure of polyalphabetic vignere cipher encryption and decryption in this experiment. The software implementation of this cipher is completed. We also explored the advantages and limitations of this cipher.

References: *(Add your references here)*

1. Behrouz A. Forouzan, "Cryptography & Network Security", Tata Mc Graw Hill.
2.