Semester : VI Subject : CSS Academic Year: 2023-2024

VIGENERE CIPHER :

Vigenere Cipher is an example of a polyalphabetic substitution cipher.

Blaise de Vigenere developed what is now called the Vigenere Cipher.

In addition to plain text, the Vigenere cipher also requires a keyword, is repeated so that the total length is equal to that of the plaintext.

He used a table known as the Vigenere square to encipher messages.

To encrypt, pick a letter in the plaintext and its corresponding letter in the keyword, use the keyword letter and the plaintext letter as the row index and coloumn index, respectively, and the entry at the row-coloumn intersection is the letter in the ciphertext.

The general formula of encryption using Vigenere Cipher is : $C_i = (P_i + K_i) \bmod 26$.

The general formula of decryption using Vigenere Cipher is : $P_i = (C_i - K_i) \bmod 26$.

Example :-

~~The general formula of encrypting using Vigenere cipher is:~~

$C_i = (P_i + K_i) \bmod 26$.

Use the Vigenere Cipher with keyword "HEALTH" to encipher the message "LIFE IS FULL OF SURPRISES".

Semester : 4 Subject : CNS Academic Year: 2023-2024

Solution :-

The general formula of encryption using Vigenere cipher is:

$C_i = (P_i + K_i) \bmod 26$.

Given Keyword : HEALTH.

Plain Text : LIFE IS FULL OF SURPRISES.

Plain Text	L	I	F	E	I	S	F	U	L	L	O	F	S	U	R	P	R	I	S	E	S
Pi Values	11	08	05	04	08	18	05	20	11	11	14	05	18	20	17	15	17	08	18	04	18
Key Stream	H	E	A	L	T	H	H	E	A	L	T	H	H	E	A	L	T	H	H	E	A
Ki Value	07	04	00	11	19	07	07	04	00	11	19	07	07	04	00	11	19	07	07	04	00
Ci Value	18	12	5	15	1	25	12	24	11	22	7	12	25	24	17	00	10	15	25	08	18
Cipher Text	S	M	F	P	B	Z	M	Y	L	W	H	M	Z	Y	R	A	K	P	Z	I	S

The encrypted text is
"SMFPBZMYLWHMZYRAKPZIS".

Example :2 :-

Use the Vigenere cipher with keyword "DECEPTIVE" to encipher the message "WE ARE DISCOVERED SAVE YOURSELF".

Solution:

Given Keyword :- DECEPTIVE, PlainText :- WE ARE DISCOVERED SAVE YOURSELF.

Plain Text	W	E	A	R	E	D	I	S	C	O	V	E	R	E	D	S	A	V	E	Y	O	U	R	S	E	L	F
Pi Value	22	4	0	17	4	3	8	18	2	14	21	4	17	4	3	18	0	21	4	24	14	20	17	18	04	11	5
Key Stream	D	E	C	E	P	T	I	V	E	D	E	C	E	P	T	I	V	E	D	E	C	E	P	T	I	V	E
Ki Value	3	4	2	4	15	19	8	21	4	3	4	2	4	15	19	8	21	4	3	4	2	4	15	19	8	21	4
Ci Value	25	8	2	21	19	22	16	13	6	17	25	6	21	19	22	00	21	25	7	2	16	24	6	11	12	6	9
Cipher Text	Z	I	C	V	T	W	Q	N	G	R	Z	G	V	T	W	A	V	Z	H	C	Q	Y	G	L	M	G	J