Aim: Cryptanalysis or decoding of polyalphabetic ciphers: Playfair, Vigenere cipher.

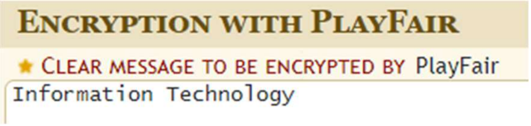
LO Mapped: LO1

Theory:

Playfair Cipher:

The Playfair Cipher is a substitution cipher that operates on pairs of letters. It uses a 5x5 matrix filled with a keyword to encode plaintext letters. Pairs of letters are replaced with corresponding letters from the matrix, following specific rules. It offers better security compared to simple substitution ciphers by using digraphs, and its key strength lies in the complexity of the matrix arrangement, making frequency analysis less effective.

Step1:

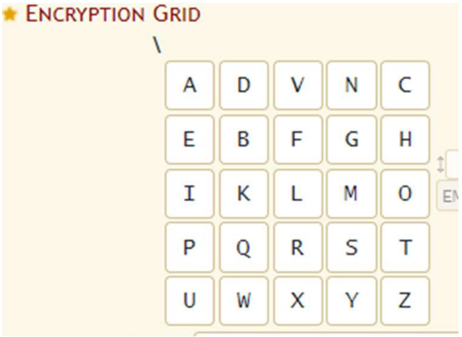


ENCRYPTION WITH PLAYFAIR

★ CLEAR MESSAGE TO BE ENCRYPTED BY PlayFair

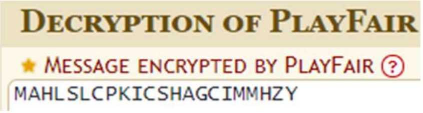
Information Technology

Step 2:



★ ENCRYPTION GRID

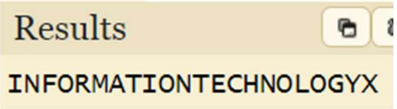
A	D	V	N	C
E	B	F	G	H
I	K	L	M	O
P	Q	R	S	T
U	W	X	Y	Z



DECRYPTION OF PLAYFAIR

★ MESSAGE ENCRYPTED BY PLAYFAIR ?

MAHLSLCPKICSHAGCIMMHZY

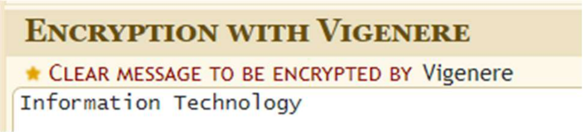


Results

INFORMATIONTECHNOLOGYX

Vigenere Cipher:

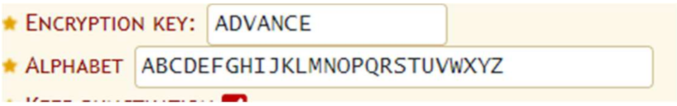
The Vigenère Cipher is a polyalphabetic substitution cipher that uses a keyword to shift letters of the plaintext. Each letter of the keyword determines the shift value for the corresponding letters in the plaintext. This creates multiple Caesar cipher variations within the text, making it more secure against frequency analysis. It was a significant advancement over monoalphabetic ciphers and introduced the concept of using a key for encryption.



Encryption with Vigenere

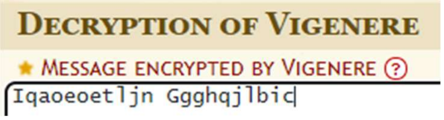
★ Clear message to be encrypted by Vigenere

Information Technology



★ Encryption key: ADVANCE

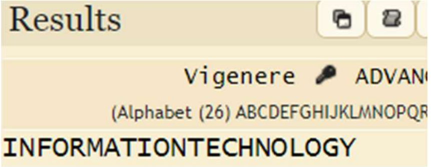
★ Alphabet ABCDEFGHIJKLMNOPQRSTUVWXYZ



Decryption of Vigenere

★ Message encrypted by Vigenere ?

Iqaoeoetljn Ggghqjlbic



Results

Vigenere 🔑 ADVAN

(Alphabet (26) ABCDEFGHIJKLMNOPQR

INFORMATIONTECHNOLOGY

Conclusion: In conclusion, the study of encryption techniques such as the Playfair Cipher and Vigenère Cipher provides valuable insights into the evolution of cryptography and its impact on data security. Both ciphers contributed innovative approaches to concealing information, offering varying levels of complexity and resistance against common cryptographic attacks.