EXPERIMENT NUMBER: 3

Date of Performance :

Date of Submission :

AIM: Cryptanalysis or decoding Playfair, vigenere cipher.

THEORY:

The Playfair Cipher encryption technique can be used to encrypt or encode a message. It operates exactly like typical encryption. The only difference is that it encrypts a digraph, or a pair of two letters, instead of a single letter.

An initial 5×5 matrix key table is created. The plaintext encryption key is made out of the matrix's alphabetic characters. Be mindful that you shouldn't repeat the letters. There are 26 alphabets however, there are only 25 spaces in which we can place a letter. The matrix will delete the extra letter because there is an excess of one letter (typically J). Despite this, J is there in the plaintext before being changed to I.

This blog provides a full explanation of the Playfair Cipher, its advantages and disadvantages, its applicability, and the Playfair encryption and decryption algorithms.
The Algorithm consists of 2 steps:

1. **Generate the key Square(5×5):**
   - The key square is a 5×5 grid of alphabets that acts as the key for encrypting the plaintext. Each of the 25 alphabets must be unique and one letter of the alphabet (usually J) is omitted from the table (as the table can hold only 25 alphabets). If the plaintext contains J, then it is replaced by I.

   - The initial alphabets in the key square are the unique alphabets of the key in the order in which they appear followed by the remaining letters of the alphabet in order.

2. **Algorithm to encrypt the plain text:** The plaintext is split into pairs of two letters (digraphs). If there is an odd number of letters, a Z is added to the last letter.
   For example:

PlainText: "instruments"
After Split: 'in' 'st' 'ru' 'me' 'nt' 'sz'

1. Pair cannot be made with same letter. Break the letter in single and add a bogus letter to the previous letter.

Plain Text: “hello”

After Split: ‘he’ ‘lx’ ‘lo’

Here **‘x’** is the bogus letter.

2. If the letter is standing alone in the process of pairing, then add an extra bogus letter with the alone letter

Plain Text: “helloe”

AfterSplit: ‘he’ ‘lx’ ‘lo’ ‘ez’

Here **‘z’** is the bogus letter.

Rules for Encryption:

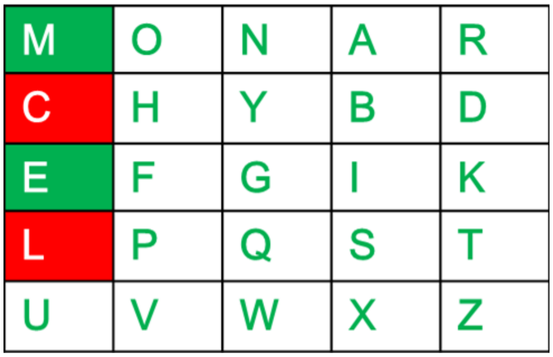
> **If both the letters are in the same column**: Take the letter below each one (going back to the top if at the bottom).
>
> **For example:**

Diagraph: "me"

Encrypted Text: cl

Encryption:

m -> c
e -> l



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

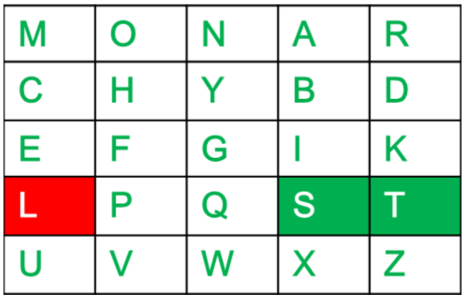
> **If both the letters are in the same row**: Take the letter to the right of each one (going back to the leftmost if at the rightmost position).
>
> **For example:**

Diagraph: "st"

Encrypted Text: tl

Encryption:

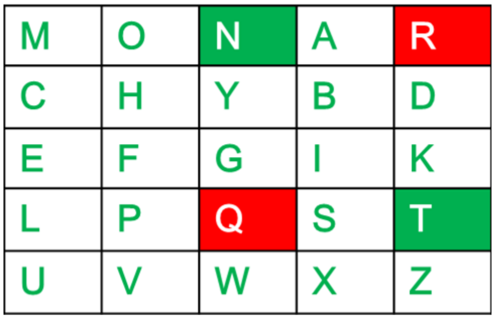
s -> t
t -> l



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

If neither of the above rules is true: Form a rectangle with the two letters and take the letters on the horizontal opposite corner of the rectangle.
For example:

Diagraph: "nt"
Encrypted Text: rq
Encryption:
n -> r
t -> q

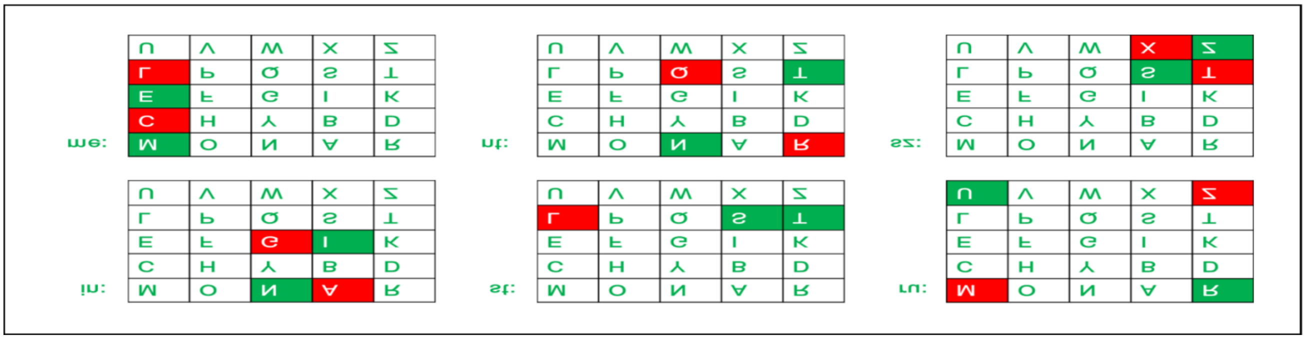


M	O	N	A	R
C	H	Y	B	D
E	F	G	I	K
L	P	Q	S	T
U	V	W	X	Z

For example:

Plain Text: "instrumentsz"
Encrypted Text: gatlmzclrqtx
Encryption:
i -> g
n -> a
s -> t
t -> l
r -> m
u -> z
m -> c
e -> l
n -> r
t -> q
s -> t

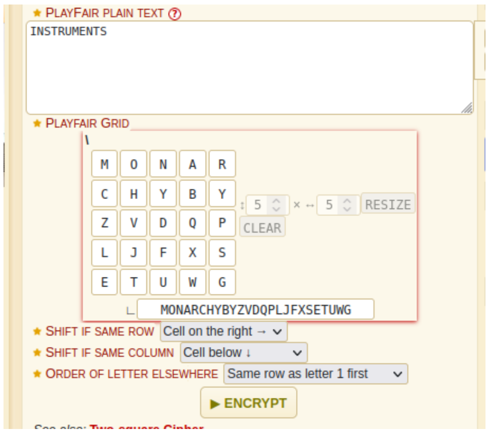
z -> x



Below is an implementation of Playfair Cipher using tool

https://www.dcode.fr/playfair-cipher#f1
https://www.dcode.fr/vigenere-cipher

Encryption process:-



★ PLAYFAIR PLAIN TEXT
INSTRUMENTS

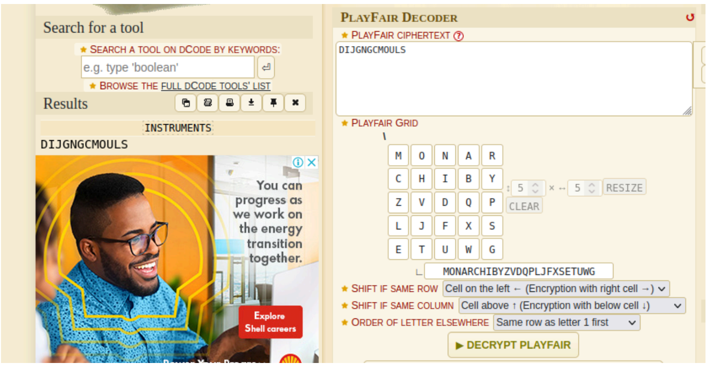
★ PLAYFAIR GRID

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

5 × 5 RESIZE
CLEAR

MONARCHYBYZVDQPLJFXSETUWG

★ SHIFT IF SAME ROW: Cell on the right →
★ SHIFT IF SAME COLUMN: Cell below ↓
★ ORDER OF LETTER ELSEWHERE: Same row as letter 1 first



Search for a tool
★ SEARCH A TOOL ON DCODE BY KEYWORDS:
e.g. type 'boolean'
★ BROWSE THE FULL DCODE TOOLS' LIST
Results

INSTRUMENTS
DIJGNGCMOULS

PLAYFAIR DECODER
★ PLAYFAIR CIPHERTEXT
DIJGNGCMOULS

★ PLAYFAIR GRID

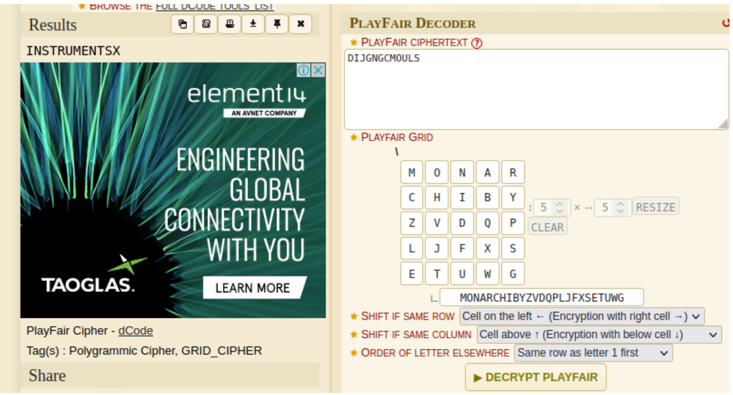
M	O	N	A	R
C	H	I	B	Y
Z	V	D	Q	P
L	J	F	X	S
E	T	U	W	G

5 × 5 RESIZE
CLEAR

MONARCHIBYZVDQPLJFXSETUWG

★ SHIFT IF SAME ROW: Cell on the left ← (Encryption with right cell →)
★ SHIFT IF SAME COLUMN: Cell above ↑ (Encryption with below cell ↓)
★ ORDER OF LETTER ELSEWHERE: Same row as letter 1 first

Decryption process



INSTRUMENTSX

PlayFair Cipher - dCode
Tag(s) : Polygrammic Cipher, GRID_CIPHER

PLAYFAIR DECODER
★ PLAYFAIR CIPHERTEXT
DIJGNGCMOULS

★ PLAYFAIR GRID

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

5 × 5 RESIZE
CLEAR

MONARCHIBYZVDQPLJFXSETUWG

★ SHIFT IF SAME ROW: Cell on the left ← (Encryption with right cell →)
★ SHIFT IF SAME COLUMN: Cell above ↑ (Encryption with below cell ↓)
★ ORDER OF LETTER ELSEWHERE: Same row as letter 1 first

Vigenere cipher. :-

Vigenere Cipher is a method of encrypting alphabetic text. It uses a simple form of polyalphabetic substitution. A polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets. The encryption of the original text is done using the *Vigenère square or Vigenère table*.

The table consists of the alphabets written out 26 times in different rows, each alphabet shifted cyclically to the left compared to the previous alphabet, corresponding to the 26 possible Caesar Ciphers.

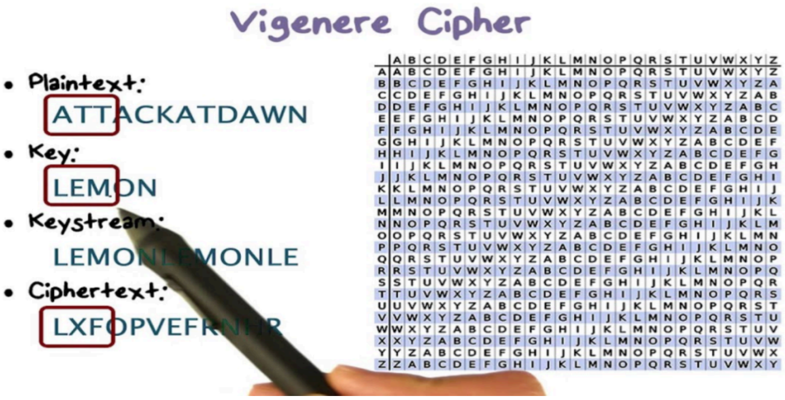
At different points in the encryption process, the cipher uses a different alphabet from one of the rows.

The alphabet used at each point depends on a repeating keyword.

, you will only use as many keys as there are unique letters in the key string, here just 5 keys, {L, E, M, O, N}. For successive letters of the message,wearegoingtotakesuccessivelettersofthekeystring,andenciphereachmessage

letter using its corresponding key row. Choose the next letter of the key, going that row to find the column heading that m atches the message character; the letter at the intersection of [key-row, msg-col] is the enciphered letter.

EXAMPLE:



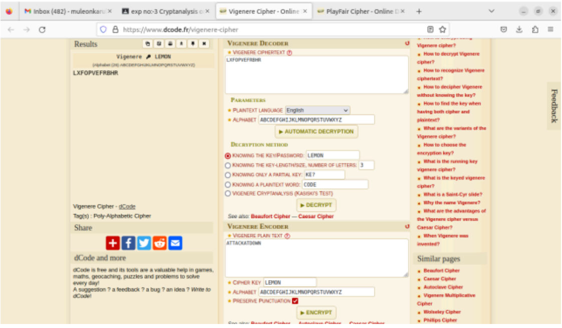
Vigenere Cipher

- Plaintext:
  ATTACKATDAWN
- Key:
  LEMON
- Keystream:
  LEMONLEMONLE
- Ciphertext:
  LXFOPVEFRNHR

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

●

Output



Results

Vigenere 🔑 LEMON

(Alphabet (26) ABCDEFGHIJKLMNOPQRSTUVWXYZ)

LXFOPVEFRBHR

VIGENERE DECODER

VIGENERE CIPHERTEXT: ATTACKATDOWN

PLAINTEXT LANGUAGE: English

ALPHABET: ABCDEFGHIJKLMNOPQRSTUVWXYZ

DECRYPTION METHOD

● KNOWING THE KEY/PASSWORD: LEMON

○ KNOWING THE KEY-LENGTH/SIZE, NUMBER OF LETTERS: 3

○ KNOWING ONLY A PARTIAL KEY: KE?

○ KNOWING A PLAINTEXT WORD: CODE

○ VIGENERE CRYPTANALYSIS (KASISKI'S TEST)

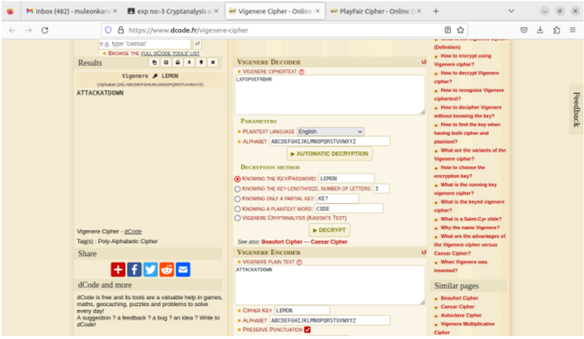
VIGENERE ENCODER

VIGENERE PLAIN TEXT: ATTACKATDOWN

CIPHER KEY: LEMON

ALPHABET: ABCDEFGHIJKLMNOPQRSTUVWXYZ

PRESERVE PUNCTUATION ☑



Results

Vigenere 🔑 LEMON

(Alphabet (26) ABCDEFGHIJKLMNOPQRSTUVWXYZ)

ATTACKATDOWN

VIGENERE DECODER

VIGENERE CIPHERTEXT: LXFOPVEFRBHR

PLAINTEXT LANGUAGE: English

ALPHABET: ABCDEFGHIJKLMNOPQRSTUVWXYZ

DECRYPTION METHOD

● KNOWING THE KEY/PASSWORD: LEMON

○ KNOWING THE KEY-LENGTH/SIZE, NUMBER OF LETTERS: 3

○ KNOWING ONLY A PARTIAL KEY: KE?

○ KNOWING A PLAINTEXT WORD: CODE

○ VIGENERE CRYPTANALYSIS (KASISKI'S TEST)

VIGENERE ENCODER

VIGENERE PLAIN TEXT: ATTACKATDOWN

CIPHER KEY: LEMON

ALPHABET: ABCDEFGHIJKLMNOPQRSTUVWXYZ

PRESERVE PUNCTUATION ☑

CONCLUSION/ Outcome:

we successfully Playfair, vigenere cipher.

Marks & Signature:

R1 (5 Marks)	R2 (5 Marks)	R3 (5 Marks)	Total (15 Marks)	Signature