Assignment 2

Aim: Cryptanalysis or decoding of polyalphabetic ciphers: Playfair, Vigenere Cipher

Theory:

Playfair Cipher:

The Playfair Cipher is a digraph substitution cipher that encrypts pairs of letters in the plaintext. It uses a 5x5 grid of letters known as the Playfair matrix. The key determines the initial arrangement of letters in the matrix.

Encryption:

1. Generate the Playfair matrix using the key.

2. Divide the plaintext into pairs of letters (digraphs).

3. If the letters in a digraph are in the same row, shift them to the right; if in the same column, shift them downwards; if not, form a rectangle and take the opposite corners.

4. Replace each digraph with the transformed digraph.

Decryption:

1. Use the same Playfair matrix generated from the key.

2. Apply the reverse process to transform the ciphertext back to plaintext.

Example:

Key: "KEYWORD"

Plaintext: "HELLO"

Ciphertext:* "ZHMZG"

Vigenère Cipher:

The Vigenère Cipher is a polyalphabetic substitution cipher that uses a keyword to determine multiple shift values. Each letter in the plaintext is shifted according to the corresponding letter in the keyword.

Encryption:

1. Replicate the keyword to match the length of the plaintext.

2. Shift each letter of the plaintext by the corresponding letter's position in the keyword.

3. Wraparound the alphabet if the shift exceeds 'Z'.

Decryption:

1. Replicate the keyword to match the length of the ciphertext.

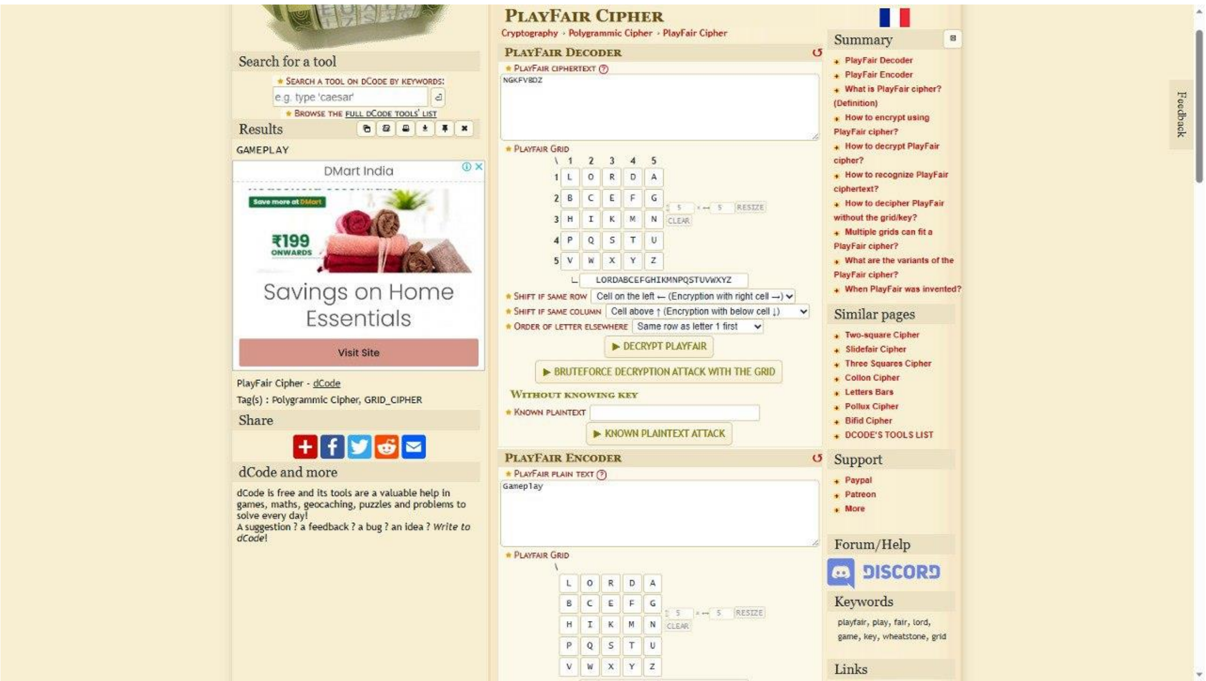
2. Reverse the shift by subtracting the corresponding keyword letter's position.

Example:

Keyword: "KEY"

Plaintext: "HELLO"

Ciphertext: "RIJVS"



Search for a tool

SEARCH A TOOL ON DCODE BY KEYWORDS:

e.g. type 'caesar'

BROWSE THE FULL DCODE TOOLS' LIST

Results

GAMEPLAY

PlayFair Cipher - dCode

Tag(s) : Polygrammic Cipher, GRID_CIPHER

Share

dCode and more

dCode is free and its tools are a valuable help in games, maths, geocaching, puzzles and problems to solve every day!
A suggestion ? a feedback ? a bug ? an idea ? *Write to dCode*!

PLAYFAIR CIPHER

Cryptography › Polygrammic Cipher › PlayFair Cipher

PLAYFAIR DECODER

PLAYFAIR CIPHERTEXT ⓘ

```
NGKFVBDZ
```

PLAYFAIR GRID

\	1	2	3	4	5
1	L	O	R	D	A
2	B	C	E	F	G
3	H	I	K	M	N
4	P	Q	S	T	U
5	V	W	X	Y	Z

5 × 5 RESIZE CLEAR

LORDABCEFGHIKMNPQSTUVWXYZ

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

▶ DECRYPT PLAYFAIR

▶ BRUTEFORCE DECRYPTION ATTACK WITH THE GRID

WITHOUT KNOWING KEY

KNOWN PLAINTEXT

▶ KNOWN PLAINTEXT ATTACK

PLAYFAIR ENCODER

PLAYFAIR PLAIN TEXT ⓘ

```
Gameplay
```

PLAYFAIR GRID

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

5 × 5 RESIZE CLEAR

Summary

- PlayFair Decoder
- PlayFair Encoder
- What is PlayFair cipher? (Definition)
- How to encrypt using PlayFair cipher?
- How to decrypt PlayFair cipher?
- How to recognize PlayFair ciphertext?
- How to decipher PlayFair without the grid/key?
- Multiple grids can fit a PlayFair cipher?
- What are the variants of the PlayFair cipher?
- When PlayFair was invented?

Similar pages

- Two-square Cipher
- Slidefair Cipher
- Three Squares Cipher
- Collon Cipher
- Letters Bars
- Pollux Cipher
- Bifid Cipher
- DCODE'S TOOLS LIST

Support

- Paypal
- Patreon
- More

Forum/Help

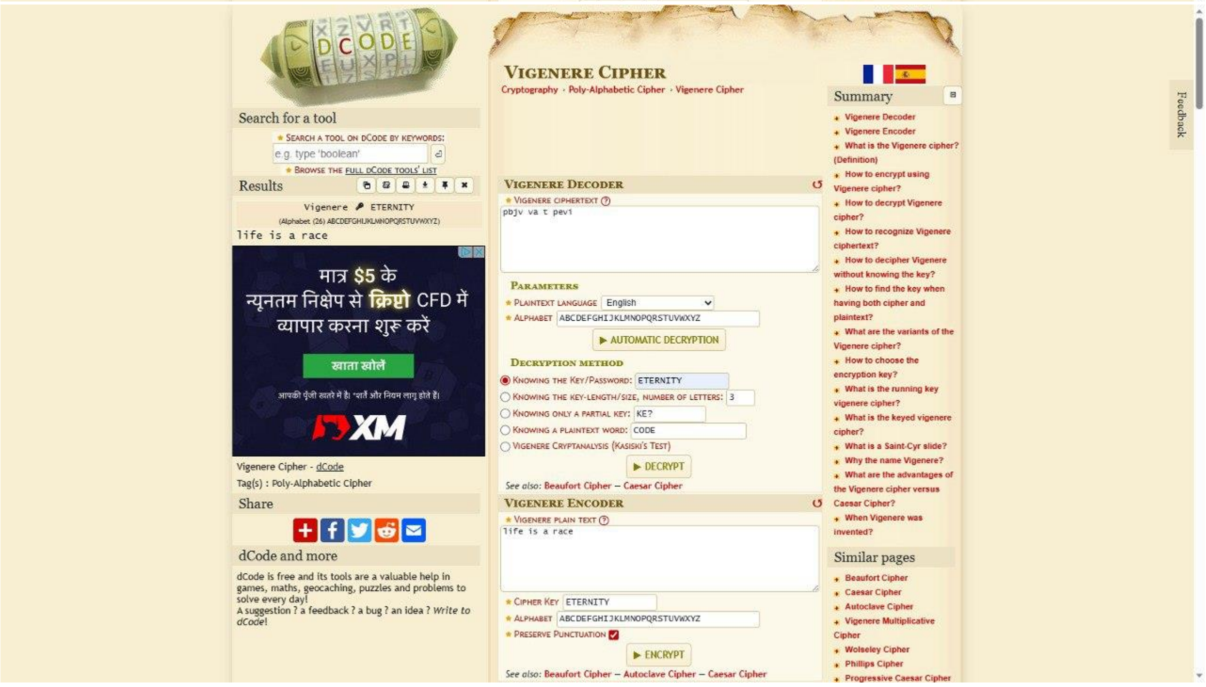
DISCORD

Keywords

playfair, play, fair, lord, game, key, wheatstone, grid

Links

Feedback



Search for a tool

SEARCH A TOOL ON DCODE BY KEYWORDS:

e.g. type 'boolean'

BROWSE THE FULL DCODE TOOLS' LIST

Results

Vigenere 🔑 ETERNITY
(Alphabet (26) ABCDEFGHIJKLMNOPQRSTUVWXYZ)

```
life is a race
```

Vigenere Cipher - dCode

Tag(s) : Poly-Alphabetic Cipher

Share

dCode and more

dCode is free and its tools are a valuable help in games, maths, geocaching, puzzles and problems to solve every day!
A suggestion ? a feedback ? a bug ? an idea ? *Write to dCode*!

VIGENERE CIPHER

Cryptography › Poly-Alphabetic Cipher › Vigenere Cipher

VIGENERE DECODER

VIGENERE CIPHERTEXT ⓘ

```
pbjv va t pevi
```

PARAMETERS

PLAINTEXT LANGUAGE: English

ALPHABET: ABCDEFGHIJKLMNOPQRSTUVWXYZ

▶ AUTOMATIC DECRYPTION

DECRYPTION METHOD

- ● KNOWING THE KEY/PASSWORD: ETERNITY
- ○ 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)

▶ DECRYPT

See also: Beaufort Cipher – Caesar Cipher

VIGENERE ENCODER

VIGENERE PLAIN TEXT ⓘ

```
life is a race
```

CIPHER KEY: ETERNITY

ALPHABET: ABCDEFGHIJKLMNOPQRSTUVWXYZ

PRESERVE PUNCTUATION ☑

▶ ENCRYPT

See also: Beaufort Cipher – Autoclave Cipher – Caesar Cipher

Summary

- Vigenere Decoder
- Vigenere Encoder
- What is the Vigenere cipher? (Definition)
- How to encrypt using Vigenere cipher?
- How to decrypt Vigenere cipher?
- How to recognize Vigenere ciphertext?
- How to decipher Vigenere without knowing the key?
- How to find the key when having both cipher and plaintext?
- What are the variants of the Vigenere cipher?
- How to choose the encryption key?
- What is the running key vigenere cipher?
- What is the keyed vigenere cipher?
- What is a Saint-Cyr slide?
- Why the name Vigenere?
- What are the advantages of the Vigenere cipher versus Caesar Cipher?
- When Vigenere was invented?

Similar pages

- Beaufort Cipher
- Caesar Cipher
- Autoclave Cipher
- Vigenere Multiplicative Cipher
- Wolseley Cipher
- Phillips Cipher
- Progressive Caesar Cipher

Feedback

<u>Conclusion:</u> Thus we learnt and implemented polyalphabetic ciphers which are playfair and vigenere ciphers