Aim:-Cryptanalysis or decoding of polyalphabetic ciphers

Theory:-

How Vigenere cipher works?

This is done using a table called the Vigenère square or Vigenère tableau. The Vigenère square is a grid of alphabets, where each row represents a shift of the previous row by one position. The letter at the intersection of the keyword letter and plaintext letter in the Vigenère square gives the encrypted letter.

Lets take an example to demonstrate the process. Suppose we want to encrypt the plaintext

&quot;HELLO WORLD&quot; with the keyword &quot;KEY.&quot; First, we convert both to numbers:

- Plaintext: H(7) E(4) L(11) L(11) O(14) (space)(18) W(22) O(14) R(17) L(11) D(3)

- Repeated Keyword: K(10) E(4) Y(24) K(10) E(4) Y(24) K(10) E(4) Y(24) K(10) E(4)

Now, add the numbers modulo 26 (in parentheses):

- Ciphertext: Q(17) I(8) V(21) V(21) A(0) (space)(18) M(12) A(0) L(11) V(21) H(7)

Explain in brief how kesiski’s Test is used to break the vigener cipher

The Kasiski method uses repetitive cryptograms found in the ciphertext to determine the key length. Modification of the vigenere cipher solves strengthen the cipher by using arranged keys to make it difficult to crack the keys against the Kasiski method attacks

How playfair cipher works?

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.

How Cryptanalysis of playfair can be done?

The playfair cipher is more complicated than a substitution cipher, but still easy to crack using automated approaches. It is known as a digraphic substitution cipher because pairs of letters are replaced by other pairs of letters. This obliterates any single letter frequency statistics, but the digraph statistics remain unchanged (frequencies of letter pairs). Unfortunately letter pairs have a much 'flatter' distribution than the single letter frequencies, so this complicates matters for solving the cipher using pen and paper methods

Encrypting a Message with Playfair Cipher

Let&#39;s use the following key table (5x5 matrix) as our encryption key:

K E Y W O

R D A B C

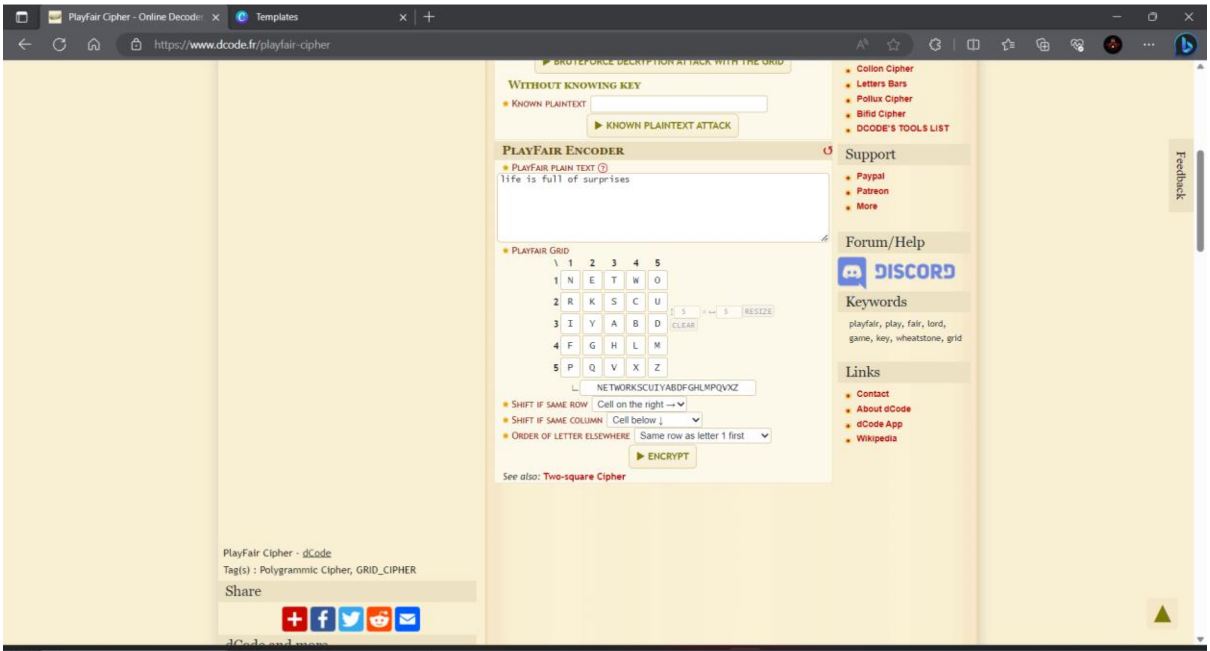
F G H I L

M N P Q S

T U V X Z

Note: The letters &quot;J&quot; and &quot;V&quot; are typically combined with &quot;I&quot; and &quot;U,&quot; respectively, in the key table

for convenience. In this example, we use &quot;I&quot; instead of &quot;J&quot; and &quot;V&quot; instead of &quot;U.&quot;output-


PlayFair Cipher - Online Decoder
Templates
https://www.dcode.fr/playfair-cipher
Feedback

▶ BRUTEFORCE DECRYPTION ATTACK WITH THE GRID

Without knowing key

Known plaintext

▶ KNOWN PLAINTEXT ATTACK

PlayFair Encoder

PlayFair plain text

```
life is full of surprises
```

PlayFair Grid

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

NETWORKSCUIYABDFGHLMPQVXZ

Shift if same row: Cell on the right →

Shift if same column: Cell below ↓

Order of letter elsewhere: Same row as letter 1 first

▶ ENCRYPT

See also: Two-square Cipher

PlayFair Cipher - dCode

Tag(s) : Polygrammic Cipher, GRID_CIPHER

Share

- Collon Cipher
- Letters Bars
- Pollux Cipher
- Bifid Cipher
- DCODE'S TOOLS LIST

Support

- Paypal
- Patreon
- More

Forum/Help

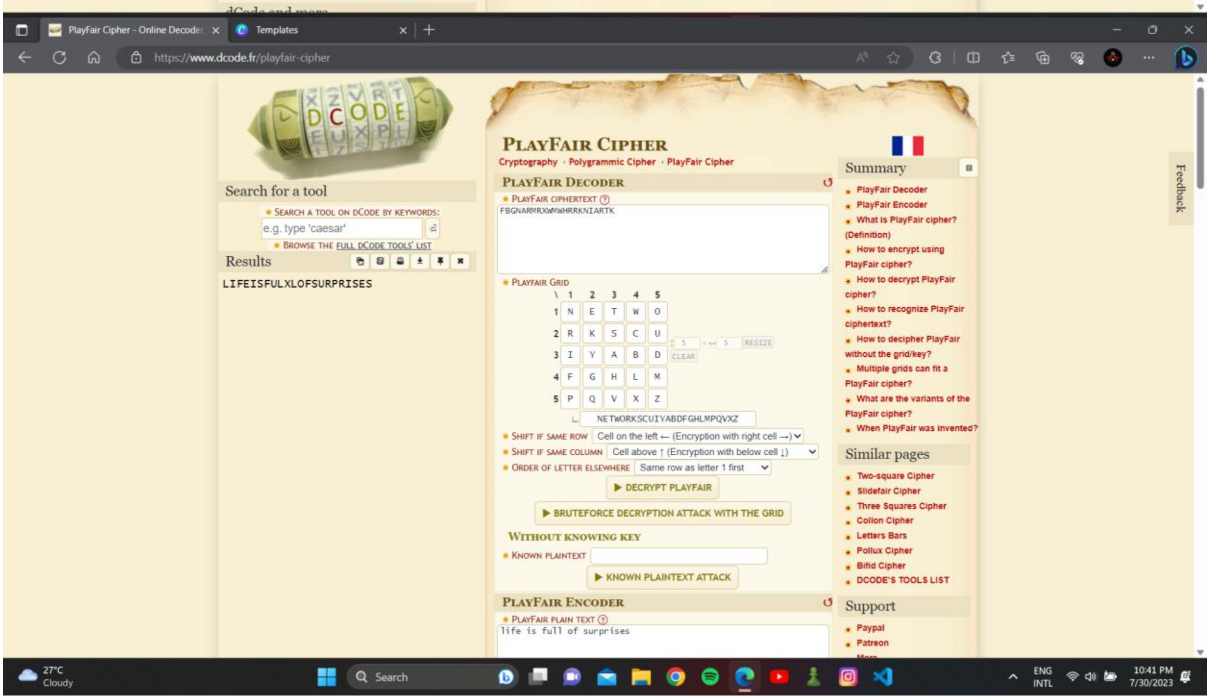
DISCORD

Keywords

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

Links

- Contact
- About dCode
- dCode App
- Wikipedia


PlayFair Cipher - Online Decoder
Templates
https://www.dcode.fr/playfair-cipher
Feedback
DCODE
27°C
Cloudy
Search
ENG
INTL
10:41 PM
7/30/2023

Search for a tool

Search a tool on dCode by keywords:

e.g. type 'caesar'

Browse the full dCode tools' list

Results

```
LIFEISFULXLOFSURPRISES
```

PlayFair Cipher

Cryptography › Polygrammic Cipher › PlayFair Cipher

PlayFair Decoder

PlayFair ciphertext

```
FBGNARMRXWMWHRRKNIARTK
```

PlayFair Grid

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

NETWORKSCUIYABDFGHLMPQVXZ

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

```
life is full of surprises
```

Summary

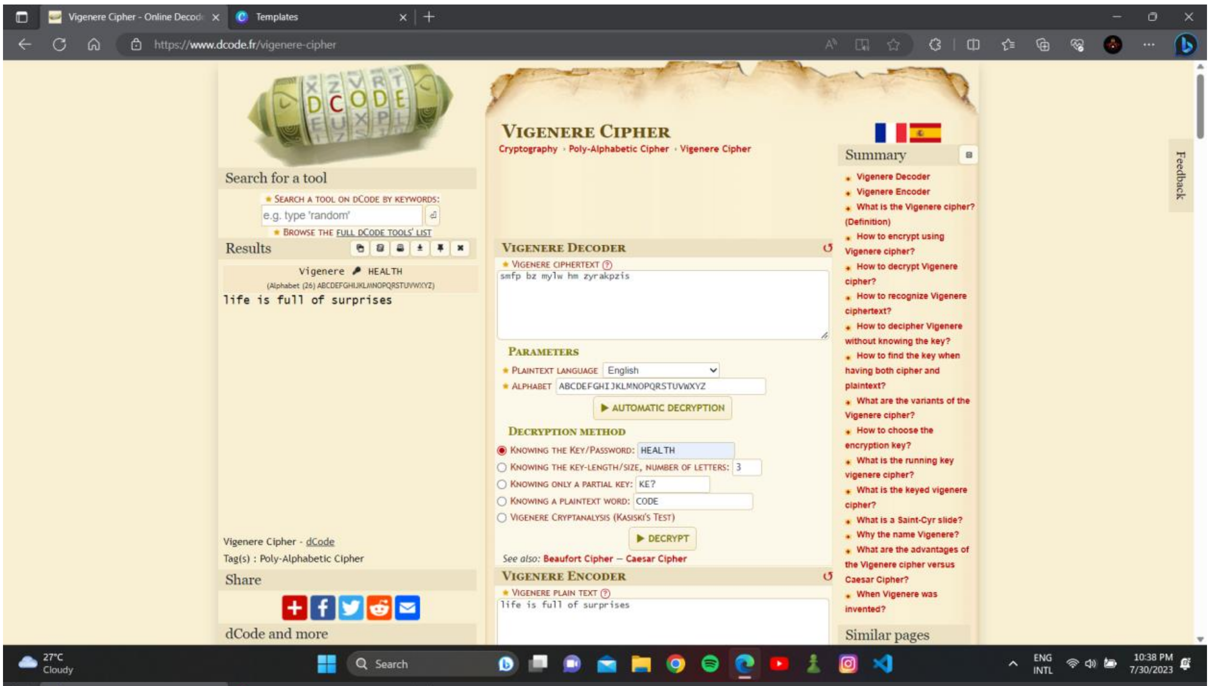
- PlayFair Decoder
- PlayFair Encoder
- What is PlayFair cipher? (Definition)
- How to encrypt using PlayFair cipher?
- How to decrypt PlayFair cipher?
- How to recognize PlayFair ciphertext?
- How to decipher PlayFair without the grid/key?
- Multiple grids can fit a PlayFair cipher?
- What are the variants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



https://www.dcode.fr/vigenere-cipher

Vigenere Cipher
Cryptography › Poly-Alphabetic Cipher › Vigenere Cipher

Results

Vigenere HEALTH
(Alphabet (26) ABCDEFGHIJKLMNOPQRSTUVWXYZ)

```
life is full of surprises
```

Vigenere Decoder

Vigenere ciphertext

```
smfp bz mylw hm zyrakpzis
```

Parameters

- Plaintext language: English
- Alphabet: ABCDEFGHIJKLMNOPQRSTUVWXYZ

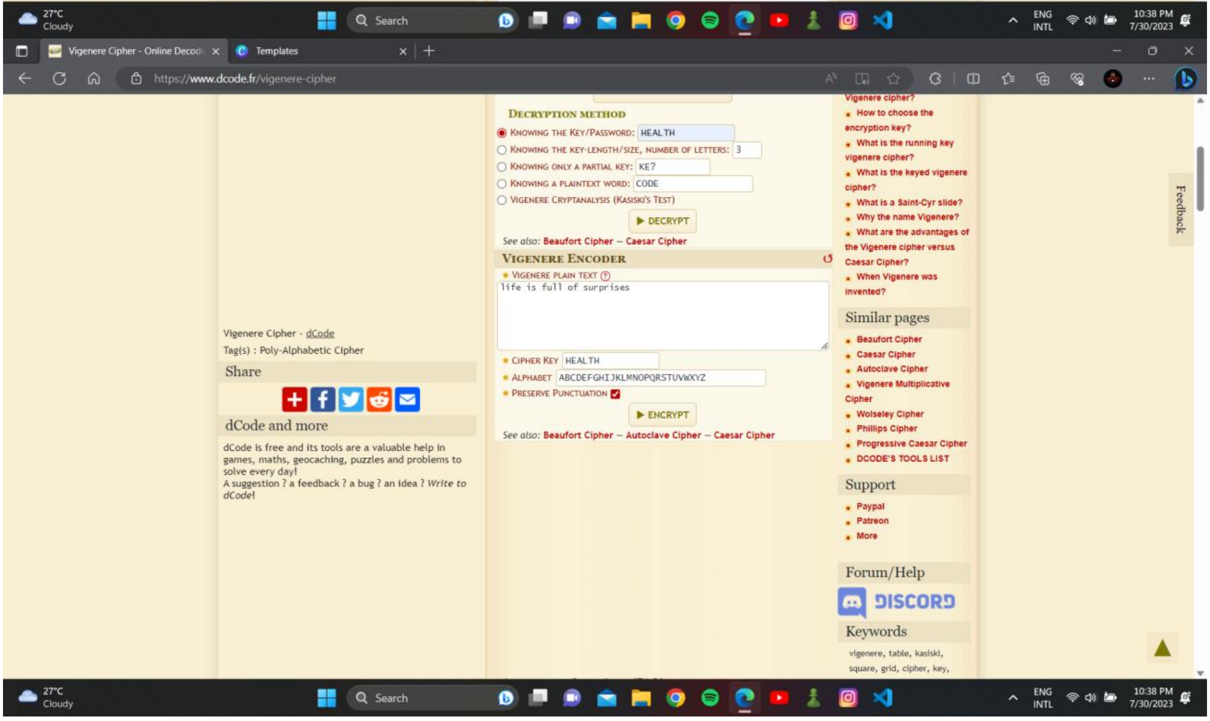
Decryption method

- ● Knowing the Key/Password: HEALTH
- ○ 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

```
life is full of surprises
```



https://www.dcode.fr/vigenere-cipher

Decryption method

- ● Knowing the Key/Password: HEALTH
- ○ 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

```
life is full of surprises
```

- Cipher Key: HEALTH
- Alphabet: ABCDEFGHIJKLMNOPQRSTUVWXYZ
- Preserve Punctuation: ☑

Conclusion–

With help of vigenere cryptanalysis and kesiski's test we culd

Decrypt ciphertetx to plaintext