Hash Cracker and PlayFair Cipher Decryption CTF:

Given Information:

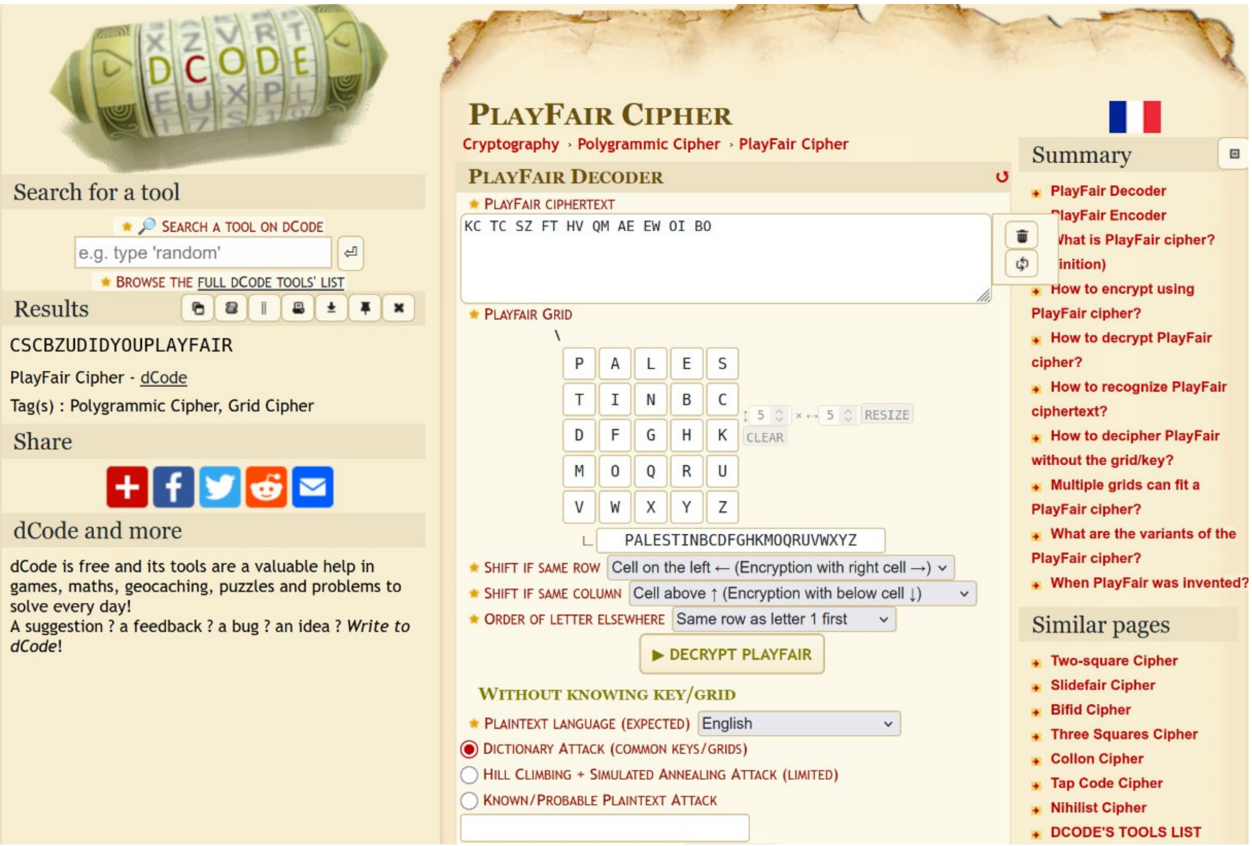
- Key Digest (MD5): 008ced81ddf77a45e35513f4459d7baf
- Encrypted Data: KCTCSZFTHVQMAEEWOIBO
- Flag Format: CSC-BZU{THIS_IS_FLAG_FORMATE}

Step1:

Crack Key digest (008ced81ddf77a45e35513f4459d7baf) by this tool and value will be Palestine

Step2:

Use this tool for PlayFair Cipher Decryption



Search for a tool

Results

CSCBZUDIDYOUPLAYFAIR

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

```
KC TC SZ FT HV QM AE EW OI BO
```

PlayFair Grid

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

PALESTINBCDFGHKMOQRUVWXYZ

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

Without knowing key/grid

Plaintext language (expected): English

● Dictionary attack (common keys/grids)

○ Hill climbing + simulated annealing attack (limited)

○ Known/probable plaintext attack

DCODE
Search a tool on dCode
e.g. type 'random'
Browse the full dCode tools' list
5 × 5 RESIZE
CLEAR
▶ DECRYPT PLAYFAIR
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
Bifid Cipher
Three Squares Cipher
Collon Cipher
Tap Code Cipher
Nihilist Cipher
DCODE'S TOOLS LIST

Then we get CSCBZUDIDYOUPLAYFAIR

Then apply flag form to CSCBZUDIDYOUPLAYFAIR and we get the flag CSC-BZU{DID_YOU_PLAY_FAIR}

Hill Cipher:

Given Information:

- Block size 2
- C = K · P mod 26
- E(“HELP”) = BJUP
- E(Flag) = YUX-AFF{PDGV_CWSRBK_OIC_GN_UOVD}

Step1:

Can use this tool

$$P = \begin{bmatrix} 7 & 11 \\ 4 & 15 \end{bmatrix}, C = \begin{bmatrix} 1 & 20 \\ 9 & 15 \end{bmatrix}$$

C = K · P mod 26, then K = C · P^{-1}

$$P^{-1} = \begin{bmatrix} 15 & -11 \\ -4 & 7 \end{bmatrix} \cdot (7{\cdot}15 - 11{\cdot}4)^{-1} \text{ mod } 26$$

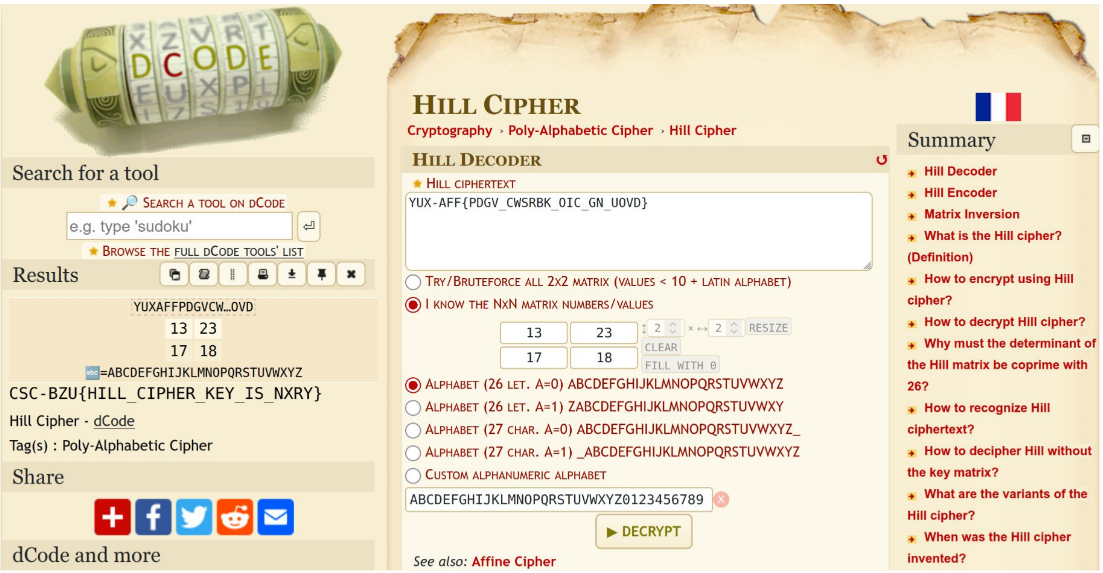
$$P^{-1} = \begin{bmatrix} 15 & -11 \\ -4 & 7 \end{bmatrix} \cdot (61)^{-1} \text{ mod } 26$$

$$P^{-1} = \begin{bmatrix} 15 & 15 \\ 22 & 7 \end{bmatrix} \cdot 3 \text{ mod } 26 = \begin{bmatrix} 19 & 19 \\ 14 & 21 \end{bmatrix}$$

$$K = \begin{bmatrix} 1 & 20 \\ 9 & 15 \end{bmatrix} \cdot \begin{bmatrix} 19 & 19 \\ 14 & 21 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 13 & 23 \\ 17 & 18 \end{bmatrix}$$

K = “NXRS”

Then use this key to decrypt encrypted Flag by this tool


DCODE
Search for a tool
SEARCH A TOOL ON DCODE
e.g. type 'sudoku'
BROWSE THE FULL DCODE TOOLS' LIST
Results
Share
dCode and more
HILL CIPHER
Cryptography › Poly-Alphabetic Cipher › Hill Cipher
Summary
Hill Decoder
Hill Encoder
Matrix Inversion
What is the Hill cipher? (Definition)
How to encrypt using Hill cipher?
How to decrypt Hill cipher?
Why must the determinant of the Hill matrix be coprime with 26?
How to recognize Hill ciphertext?
How to decipher Hill without the key matrix?
What are the variants of the Hill cipher?
When was the Hill cipher invented?
See also: Affine Cipher

Results

YUXAFFPDGVCW...OVD

13	23
17	18

🔤=ABCDEFGHIJKLMNOPQRSTUVWXYZ

```
CSC-BZU{HILL_CIPHER_KEY_IS_NXRY}
```

Hill Cipher - dCode

Tag(s) : Poly-Alphabetic Cipher

HILL DECODER

★ HILL CIPHERTEXT

```
YUX-AFF{PDGV_CWSRBK_OIC_GN_UOVD}
```

○ TRY/BRUTEFORCE ALL 2X2 MATRIX (VALUES < 10 + LATIN ALPHABET)

● I KNOW THE NXN MATRIX NUMBERS/VALUES

13	23
17	18

↕ 2 × ↔ 2 RESIZE CLEAR FILL WITH 0

● ALPHABET (26 LET. A=0) ABCDEFGHIJKLMNOPQRSTUVWXYZ

○ ALPHABET (26 LET. A=1) ZABCDEFGHIJKLMNOPQRSTUVWXY

○ ALPHABET (27 CHAR. A=0) ABCDEFGHIJKLMNOPQRSTUVWXYZ_

○ ALPHABET (27 CHAR. A=1) _ABCDEFGHIJKLMNOPQRSTUVWXYZ

○ CUSTOM ALPHANUMERIC ALPHABET

ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789

▶ DECRYPT

Then we have almostflag decryption CSC-BZU{HILL_CIPHER_KEY_IS_NXRY} but the right flag is CSC-BZU{HILL_CIPHER_KEY_IS_NXRS}. This happens because the tool adds a filler character “A” if the number of characters is not a multiple of 2.

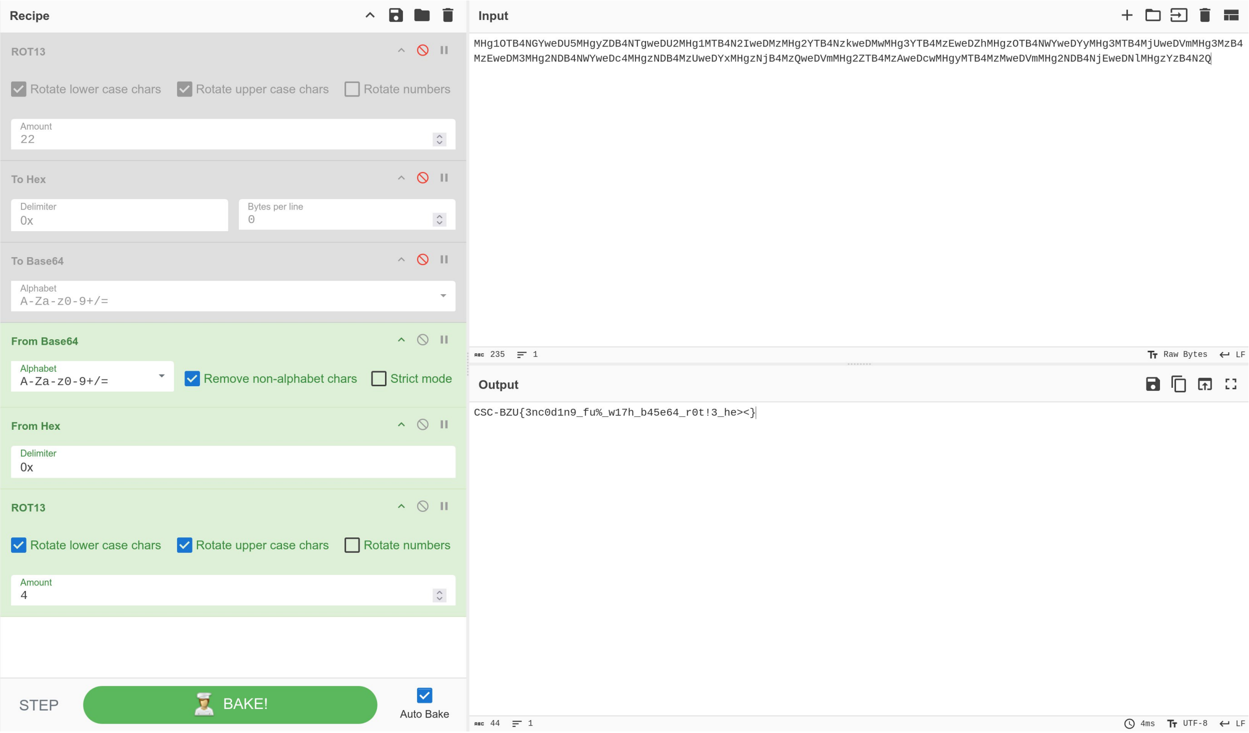
Encoding

Given Information:

- Power lies in multi-layered encoding
- File name
- File content

Step1:

Use this tool to decoding file name



Recipe

ROT13
☑ Rotate lower case chars ☑ Rotate upper case chars □ Rotate numbers
Amount: 22

To Hex
Delimiter: 0x
Bytes per line: 0

To Base64
Alphabet: A-Za-z0-9+/=

From Base64
Alphabet: A-Za-z0-9+/=
☑ Remove non-alphabet chars □ Strict mode

From Hex
Delimiter: 0x

ROT13
☑ Rotate lower case chars ☑ Rotate upper case chars □ Rotate numbers
Amount: 4

Input

```
MHg1OTB4NGYweDU5MHgyZDB4NTgweDU2MHg1MTB4N2IweDMzMHg2YTB4NzkweDMwMHg3YTB4MzEweDZhMHgzOTB4NWYweDYyMHg3MTB4MjUweDVmMHg3MzB4
MzEweDM3MHg2NDB4NWYweDc4MHgzNDB4MzUweDYxMHgzNjB4MzQweDVmMHg2ZTB4MzAweDcwMHgyMTB4MzMweDVmMHg2NDB4NjEweDNlMHgzYzB4N2Q
```

Output

```
CSC-BZU{3nc0d1n9_fu%_w17h_b45e64_r0t!3_he><}
```

Then read story