

Name: Harsh Mishra

Roll no: 64

Batch: T21

Aim: To perform Cryptanalysis or decoding of polyalphabetic ciphers: Playfair & Vigenere cipher.

Theory:

Playfair Cipher :

The Playfair cipher is a classical encryption algorithm that uses a digraph (pair of letters) substitution technique to encode plaintext. It was invented by Charles Wheatstone in 1854 but is named after Lord Playfair, who promoted its use.

Key Preparation

1. Key Square Creation:

- Choose a keyword or phrase (e.g., "KEYWORD").
- Remove duplicates and combine the letters with the remaining letters of the alphabet (excluding 'J', which is usually combined with 'I').
- Construct a 5x5 grid with these letters.

For example, with the keyword "KEYWORD":

K E Y W O

R D A B C

F G H I/J L

M N P Q S

T U V X Z

Name: Harsh Mishra

Roll no: 64

Batch: T21

Encryption Process

1. Pairing Letters:

- Split the plaintext into digraphs (pairs of two letters). If there's an odd number of letters, add an extra letter (usually 'X') to the last pair.
- If a pair consists of the same letter (like "LL"), replace one letter with a different letter (e.g., "LX" or "YL").

2. Encryption Rules:

- **Same Row:** If both letters are in the same row of the grid, replace them with the letters immediately to their right. Wrap around to the beginning of the row if needed.
- **Same Column:** If both letters are in the same column, replace them with the letters immediately below. Wrap around to the top if needed.
- **Rectangle:** If the letters form a rectangle, replace each letter with the letter in its own row but in the column of the other letter of the pair.

Decryption Process

1. Pairing Letters:

- Similar to encryption, but the rules for substitution are reversed.

2. Decryption Rules:

- **Same Row:** Replace each letter with the letter immediately to its left. Wrap around to the end of the row if needed.
- **Same Column:** Replace each letter with the letter immediately above. Wrap around to the bottom if needed.
- **Rectangle:** Replace each letter with the letter in its own row but in the column of the other letter of the pair.

The Playfair cipher is more secure than simple substitution ciphers because it encrypts pairs of letters and provides more complexity, but it's still vulnerable to more advanced cryptanalysis techniques.

Name: Harsh Mishra

Roll no: 64

Batch: T21

Vigenere Cipher :

The Vigenère cipher is a method of encrypting alphabetic text using a series of different Caesar ciphers based on the letters of a keyword. It is a polyalphabetic substitution cipher. Here's a basic overview of how it works:

Encryption

1. **Choose a Keyword:** Select a keyword (e.g., "KEYWORD").
2. **Prepare the Text:** Write the plaintext (the text you want to encrypt) and repeat the keyword to match the length of the plaintext.

Example:

- Plaintext: HELLO
 - Keyword: KEYKE (repeated to match length)
3. **Encrypt Using the Vigenère Square:**
 - The Vigenère square is a table of 26 x 26 letters, where each row is a Caesar cipher shifted by one position more than the previous row.

To encrypt:

- Locate the letter of the plaintext in the column of the keyword letter in the Vigenère square.
- The intersecting letter in the row of the keyword letter is the ciphertext letter.

For example, if the plaintext letter is H and the keyword letter is K, you find H in the K column and the intersection gives you the ciphertext letter.

Decryption

To decrypt, you essentially reverse the process:

1. **Prepare the Text:** Write the ciphertext and repeat the keyword to match the length.
2. **Decrypt Using the Vigenère Square:**
 - Find the ciphertext letter in the row corresponding to the keyword letter in the Vigenère square.
 - The column intersection gives you the plaintext letter.

Name: Harsh Mishra

Roll no: 64

Batch: T21

Output:

Playfair Cipher:

Encryption:

The screenshot displays the dCode website's PlayFair Cipher tool. The interface is divided into several sections:

- Search for a tool:** A search bar with the text "e.g. type 'caesar'" and a link to "BROWSE THE FULL dCODE TOOLS LIST".
- Results:** A list of tools including "SHAINDCOSTA", "PBNXRYHMTLBA", "PlayFair Cipher - dCode", and "Tag(s) : Polygrammic Cipher, GRID_CIPHER".
- Share:** Social media sharing icons for WhatsApp, Facebook, Twitter, Reddit, and Email.
- dCode and more:** A paragraph stating "dCode is free and its tools are a valuable help in games, maths, geocaching, puzzles and problems to solve every day!" and a link to "Write to dCode!".
- PLAYFAIR CIPHER:** The main section, titled "Cryptography · Polygrammic Cipher · PlayFair Cipher". It contains two sub-sections:
 - PLAYFAIR DECODER:** A text input field containing "PBNXRYHMTLBA". Below it is a 5x5 grid with the key "MONARCHYBDEFGIKLPQSTUVWXZ". The grid is labeled with numbers 1-5 and letters A-Z. There are buttons for "DECRYPT PLAYFAIR" and "BRUTEFORCE DECRYPTION ATTACK WITH THE GRID".
 - PLAYFAIR ENCODER:** A text input field containing "harshmitshra". Below it is a similar 5x5 grid with the same key. There is a button for "ENCRYPT".
- Summary:** A list of links including "PlayFair Decoder", "PlayFair Encoder", "What is PlayFair cipher?", "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?", and "When PlayFair was invented?".
- Similar pages:** A list of links including "Two-square Cipher", "Slidefair Cipher", "Colton Cipher", "Bifid Cipher", "Three Squares Cipher", "Delastalle Trifid Cipher", "ADFGX Cipher", and "dCODE'S TOOLS LIST".
- Support:** Links to "Paypal", "Patreon", and "More".
- Forum/Help:** A link to "DISCORD".
- Keywords:** A list of keywords including "playfair", "play", "fair", "lord", "game", "key", "wheatstone", and "grid".
- Links:** Links to "Contact", "About dCode", "dCode App", and "Wikipedia".

Batch: T21



Search for a tool

SEARCH A TOOL ON dCode BY KEYWORDS:
e.g. type "caesar"

BROWSE THE FULL dCODE TOOLS LIST

Results

II	II
SHAWNDOSTDR	
SHAWNDOSTAX	
SHAWNDOSTYN	
SHAWNDOSTIB	
SHAWNDCKEDR	
SHAWNDCKEYN	
HSWADNCKEDR	
SHAWNDCKETB	
SHAWNDCOLPDR	
SHAWNDCOLPAX	
HSWADNCKEYN	
SHAWNDCOLPTB	
SHAWNDCKEAX	
SHAWNDCOLPYN	
SHAWNDCOZUDR	
SHAWNDCOZUYN	
HSWADNCKETB	
SHAWNDCOZUB	
HSWADNCKEAX	
SHAWNDNOCSTYN	
SHAWNDCOZUAX	
SHAWNDNOCSTAX	
SHAWNDNOCSTB	
SHAWNDNOCSTR	
SHAWNDNCLPYN	
SHAWNDNCLPDR	
SHAWNDNCLPTB	
SHAWNDNCLPAX	
SHAWNDNOCZUYN	
SHAWNDNOCZUDR	
SHAWNDNOCZUB	
SHAWNDNOCZUAX	

#32

PLAYFAIR CIPHER

Cryptography · Polygrammic Cipher · PlayFair Cipher

PLAYFAIR DECODER

PLAYFAIR CIPHERTEXT (?)

PNBNKYHTLBA

PLAYFAIR GRID

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

MONARCHYBDFGKLPQSTUVWXYZ

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

▶ REFERENCE DECRYPTION ATTACK WITH THE GRID

WITHOUT KNOWING KEY

KNOWN PLAINTEXT

▶ KNOWN PLAINTEXT ATTACK

PLAYFAIR ENCODER

PLAYFAIR PLAIN TEXT (?)

harshatshra

PLAYFAIR GRID

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

MONARCHYBDFGKLPQSTUVWXYZ

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

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
- Colson Cipher
- Bifid Cipher
- Three Squares Cipher
- Delastelle Trifid Cipher
- ADFGVX Cipher
- dCODE's TOOLS LIST

Support

- Payspal
- Patreon
- More

Forum/Help

 DISCORD

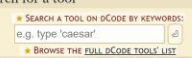
Keywords

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

Links

- Contact
- About dCode
- dCode App
- Wikipedia

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



Search for a tool

SEARCH A TOOL ON dCODE BY KEYWORDS:
e.g. type 'caesar'

BROWSE THE FULL dCODE TOOLS LIST

PLAYFAIR CIPHER

Cryptography · Polygrammic Cipher · PlayFair Cipher

PLAYFAIR DECODER

PLAYFAIR CIPHERTEXT (?)

PENKRYHTLBA

PLAYFAIR GRID

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

MONARCHYBDEFGZKLPGSTUVWXZ

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 (?)

BRHAIH DCDSTA

PLAYFAIR GRID

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

MONARCHYBDEFGZKLPGSTUVWXZ

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

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!

Results

HARSHMISHRAX

PlayFair Cipher · dCode

Tag(s) : Polygrammic Cipher, GRID_CIPHER

Share



Summary

- PlayFair Decoder
- PlayFair Encoder
- What is PlayFair cipher? (Definition)
- How to encrypt using PlayFair cipher?
- How to recognize PlayFair cipher?
- How to decrypt PlayFair cipher?
- How to recognize PlayFair ciphertext?
- How to decipher PlayFair without the grillekey?
- 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
- Colton Cipher
- Blind Cipher
- Three Squares Cipher
- Delastelle Tridid Cipher
- ADFGX Cipher
- dCODE'S TOOLS LIST

Support

- Paypal
- Patreon
- More

Forum/Help

 DISCORD

Keywords

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

Links

- Contact
- About dCode
- dCode App
- Wikipedia

See also: Two-square Cipher

Name: Harsh Mishra

Roll no: 64

Batch: T21

Vignere Cipher:

Encryption:



The screenshot shows the 'VIGNERE CIPHER' web application interface. The main heading is 'VIGNERE CIPHER' with a subtitle 'Cryptography · Poly-Alphabetic Cipher · Vignere Cipher'. The interface is divided into three main sections: a left sidebar, a central workspace, and a right sidebar.

Left Sidebar:

- Search for a tool:** A search bar with the text 'e.g. type 'caesar'' and a button 'BROWSE THE FULL dCODE TOOLS' LIST'.
- Results:** A list of tools including 'Vignere Cipher - dCode', 'Vignere Cipher - dCode', and 'Vignere Cipher - dCode'.
- Share:** Social media sharing icons for Facebook, Twitter, and Email.
- dCode and more:** A paragraph stating '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!'.

Central Workspace:

- VIGNERE DECODER:** A section for decoding, with a text input field containing 'CLYGR BMSQDE' and a button 'AUTOMATIC DECRYPTION'.
- PARAMETERS:** A section for setting parameters, including 'PLAINTEXT LANGUAGE' (English), 'ALPHABET' (ABCDEFGHIJKLMNOPQRSTUVWXYZ), and 'PRESERVE PUNCTUATION' (checked).
- DECRYPTION METHOD:** A section for choosing a decryption method, with options: 'KNOWING THE KEY/PASSWORD: KEY', 'KNOWING THE KEY-LENGTH/SIZE, NUMBER OF LETTERS: 3', 'KNOWING ONLY A PARTIAL KEY: KE?', 'KNOWING A PLAINTEXT WORD: CODE', and 'VIGNERE CRYPTANALYSIS (KASISKI'S TEST)'. The 'KEY' method is selected.
- VIGNERE ENCODER:** A section for encoding, with a text input field containing 'SHAWN DCOSTA' and a button 'ENCRYPT'.
- PARAMETERS:** A section for setting parameters, including 'PLAINTEXT LANGUAGE' (English), 'ALPHABET' (ABCDEFGHIJKLMNOPQRSTUVWXYZ), and 'PRESERVE PUNCTUATION' (checked).
- DECRYPTION METHOD:** A section for choosing a decryption method, with options: 'KNOWING THE KEY/PASSWORD: KEY', 'KNOWING THE KEY-LENGTH/SIZE, NUMBER OF LETTERS: 3', 'KNOWING ONLY A PARTIAL KEY: KE?', 'KNOWING A PLAINTEXT WORD: CODE', and 'VIGNERE CRYPTANALYSIS (KASISKI'S TEST)'. The 'KEY' method is selected.

Right Sidebar:

- Summary:** A list of links to various resources, including 'Vignere Decoder', 'Vignere Encoder', 'What is the Vignere cipher? (Definition)', 'How to encrypt using Vignere cipher?', 'How to decrypt Vignere cipher?', 'How to recognize Vignere ciphertext?', 'How to decipher Vignere without knowing the key?', 'How to find the key when having both cipher and plaintext?', 'What are the variants of the Vignere cipher?', 'How to choose the encryption key?', 'What is the running key vignere cipher?', 'What is the keyed vignere cipher?', 'What is a Saint-Cyr slide?', 'Why the name Vignere?', 'What are the advantages of the Vignere cipher versus Caesar Cipher?', 'When Vignere was invented?', and 'Similar pages'.
- Feedback:** A button labeled 'Feedback'.

Decryption:



The screenshot shows the 'VIGNERE CIPHER' web application interface, specifically the decryption section. The main heading is 'VIGNERE CIPHER' with a subtitle 'Cryptography · Poly-Alphabetic Cipher · Vignere Cipher'.

Left Sidebar:

- Search for a tool:** A search bar with the text 'e.g. type 'caesar'' and a button 'BROWSE THE FULL dCODE TOOLS' LIST'.
- Results:** A list of tools including 'Vignere Cipher - dCode', 'Vignere Cipher - dCode', and 'Vignere Cipher - dCode'.
- Share:** Social media sharing icons for Facebook, Twitter, and Email.
- dCode and more:** A paragraph stating '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!'.


Central Workspace:

- VIGNERE DECODER:** A section for decoding, with a text input field containing 'CLYGR BMSQDE' and a button 'AUTOMATIC DECRYPTION'.
- PARAMETERS:** A section for setting parameters, including 'PLAINTEXT LANGUAGE' (English), 'ALPHABET' (ABCDEFGHIJKLMNOPQRSTUVWXYZ), and 'PRESERVE PUNCTUATION' (checked).
- DECRYPTION METHOD:** A section for choosing a decryption method, with options: 'KNOWING THE KEY/PASSWORD: KEY', 'KNOWING THE KEY-LENGTH/SIZE, NUMBER OF LETTERS: 3', 'KNOWING ONLY A PARTIAL KEY: KE?', 'KNOWING A PLAINTEXT WORD: CODE', and 'VIGNERE CRYPTANALYSIS (KASISKI'S TEST)'. The 'KEY' method is selected.
- VIGNERE ENCODER:** A section for encoding, with a text input field containing 'SHAWN DCOSTA' and a button 'ENCRYPT'.
- PARAMETERS:** A section for setting parameters, including 'PLAINTEXT LANGUAGE' (English), 'ALPHABET' (ABCDEFGHIJKLMNOPQRSTUVWXYZ), and 'PRESERVE PUNCTUATION' (checked).
- DECRYPTION METHOD:** A section for choosing a decryption method, with options: 'KNOWING THE KEY/PASSWORD: KEY', 'KNOWING THE KEY-LENGTH/SIZE, NUMBER OF LETTERS: 3', 'KNOWING ONLY A PARTIAL KEY: KE?', 'KNOWING A PLAINTEXT WORD: CODE', and 'VIGNERE CRYPTANALYSIS (KASISKI'S TEST)'. The 'KEY' method is selected.

Right Sidebar:


- Summary:** A list of links to various resources, including 'Vignere Decoder', 'Vignere Encoder', 'What is the Vignere cipher? (Definition)', 'How to encrypt using Vignere cipher?', 'How to decrypt Vignere cipher?', 'How to recognize Vignere ciphertext?', 'How to decipher Vignere without knowing the key?', 'How to find the key when having both cipher and plaintext?', 'What are the variants of the Vignere cipher?', 'How to choose the encryption key?', 'What is the running key vignere cipher?', 'What is the keyed vignere cipher?', 'What is a Saint-Cyr slide?', 'Why the name Vignere?', 'What are the advantages of the Vignere cipher versus Caesar Cipher?', 'When Vignere was invented?', and 'Similar pages'.
- Feedback:** A button labeled 'Feedback'.

Batch: T21



VIGENERE CIPHER

Cryptography · Poly-Alphabetic Cipher · Vigenere Cipher



Search for a tool

[SEARCH A TOOL ON dCode BY KEYWORDS:](#)

[BROWSE THE FULL dCODE TOOLS LIST](#)


Results

Vigenere	KE
(Alphabet) (26)	ABCDEFGHIJKLMNOPQRSTUVWXYZ
I I	
KEY SHAWN DCOSTA	
KU SHEN HCOWTA	
KX SHWN ECOTTA	
KEQ SHWN LCOATA	
KEN SHLWN OCODTA	

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 DECODER

[VIGENERE CIPHTEXT \(?\)](#)

CLYGR BMSQIE

PARAMETERS

PLAINTEXT LANGUAGE English

ALPHABET ABCDEFGHIJKLMNOPQRSTUVWXYZ

[AUTOMATIC DECRIPTION](#)

DECRIPTION METHOD

☐ KNOWING THE KEY/PASSWORD: KEY

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

☒ KNOWING ONLY A PARTIAL KEY: KE?

☐ KNOWING A PLAINTEXT WORD: CODE

☐ VIGENERE CRYPTANALYSIS (KASIKI'S TEST)

[DECRYPT](#)

See also: Beaufort Cipher – Caesar Cipher

VIGENERE ENCODER

[VIGENERE PLAIN TEXT \(?\)](#)

SHAWN DCOSTA

CIPHER KEY KEY

ALPHABET ABCDEFGHIJKLMNOPQRSTUVWXYZ

PRESERVE PUNCTUATION ☒

[ENCRYPT](#)

See also: Beaufort Cipher – Autoclave Cipher – Caesar Cipher

Answers to Questions (FAQ)

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

Name: Harsh Mishra

Roll no: 64

Batch: T21

The screenshot displays the dCode Vigenere Cipher tool interface. On the left, a sidebar contains a search bar, a list of results for 'Vigenere', and social media sharing options. The main area is titled 'VIGENERE CIPHER' and includes sections for 'VIGENERE DECODER' and 'VIGENERE ENCODER'. The decoder section has input fields for 'VIGENERE CIPHERTEXT' (containing 'CLYGR BMSQDE'), 'PLAINTEXT LANGUAGE' (set to 'English'), and 'ALPHABET' (set to 'ABCDEFGHIJKLMNOPQRSTUVWXYZ'). It also features a 'DECRYPTION METHOD' section with radio buttons for 'KNOWING THE KEY/PASSWORD', 'KNOWING THE KEY-LENGTH/SIZE, NUMBER OF LETTERS', 'KNOWING ONLY A PARTIAL KEY', 'KNOWING A PLAINTEXT WORD', and 'VIGENERE CRYPTANALYSIS (KASISKI'S TEST)'. The encoder section has input fields for 'VIGENERE PLAIN TEXT' (containing 'SHAWN DCOSTA'), 'CIPHER KEY' (set to 'KEY'), 'ALPHABET' (set to 'ABCDEFGHIJKLMNOPQRSTUVWXYZ'), and a 'PRESERVE PUNCTUATION' checkbox. Both sections have 'AUTOMATIC DECRYPTION' and 'ENCRYPT' buttons. A right sidebar contains a 'Summary' section with a list of links and a 'Similar pages' section with links to 'Beaufort Cipher', 'Caesar Cipher', and 'Autoclave Cipher'. A 'Feedback' button is located on the far right.

VIGENERE CIPHER
Cryptography · Poly-Alphabetic Cipher · Vigenere Cipher

VIGENERE DECODER

VIGENERE CIPHERTEXT
CLYGR BMSQDE

PARAMETERS

PLAINTEXT LANGUAGE English

ALPHABET ABCDEFGHIJKLMNOPQRSTUVWXYZ

AUTOMATIC DECRYPTION

DECRYPTION METHOD

☐ KNOWING THE KEY/PASSWORD: KEY

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

☐ KNOWING ONLY A PARTIAL KEY: KE?

☒ KNOWING A PLAINTEXT WORD: DCOSTA

☐ VIGENERE CRYPTANALYSIS (KASISKI'S TEST)

DECRYPT

See also: Beaufort Cipher – Caesar Cipher

VIGENERE ENCODER

VIGENERE PLAIN TEXT
SHAWN DCOSTA

CIPHER KEY KEY

ALPHABET ABCDEFGHIJKLMNOPQRSTUVWXYZ

PRESERVE PUNCTUATION ☒

ENCRYPT

See also: Beaufort Cipher – Autoclave Cipher – Caesar Cipher

Answers to Questions (FAQ)

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

Search for a tool

SEARCH A TOOL ON dCODE BY KEYWORDS:
e.g. type 'caesar'

BROWSE THE FULL dCODE TOOLS' LIST

Results

Vigenere ?
(Alphabet (26) ABCDEFGHIJKLMNOPQRSTUVWXYZ)

II	II
KEYKEY	SHAWN DCOSTA
UZQDPN	IMIDC OSTAAP
YAXDOZ	ELBDD COSTAQ
ZJKOYB	DCOST ANJGPG
MIWSZI	QDCOS TAKULF
TSVEDJ	JTDCO STAVZB
#6	

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!

Conclusion: Illustration of symmetric cryptography by implementing classical ciphers (Shift and Mono-alphabetic) is achieved (LO1 is achieved).