Alphonz George
T11-03

Assignment no. 2

Aim: To implement Playfair and Vigenere cipher.

Theory:

Playfair Cipher

The Playfair Cipher is a digraph substitution cipher, meaning it encrypts pairs of letters instead of single letters. Here’s how it works:

1. Create a 5x5 matrix using a keyword. For example, let’s use the keyword `MONARCHY`. The letters `I` and `J` are usually combined to fit the 25-letter grid.

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

- Fill in the keyword first, skipping duplicate letters.
- Then, fill in the remaining letters of the alphabet.

2. Encrypting a message: Let’s encrypt the message `HELLO`.

- Pair the letters: `HE` `LL` `O`. If a pair has the same letter (like `LL`), insert an `X` between them: `HE` `LX` `LO`.
- For each pair, find the letters in the grid:
- `H` and `E`: They form a rectangle, so take the letters on the opposite corners: `HF` → `BM`.
- `L` and `X`: They form a rectangle, so take the letters on the opposite corners: `LP` → `SU`.
- `L` and `O`: They are in the same row, so take the letters to their right: `LO` → `P`. - The encrypted message is: **BM SU PX**

Vigenère Cipher

The Vigenère Cipher is a method of encrypting alphabetic text by using a simple form of polyalphabetic substitution.

1. Choose a keyword: Let’s use `LEMON`.

2. Encrypt a message: Let’s encrypt the message `ATTACKATDAWN`.

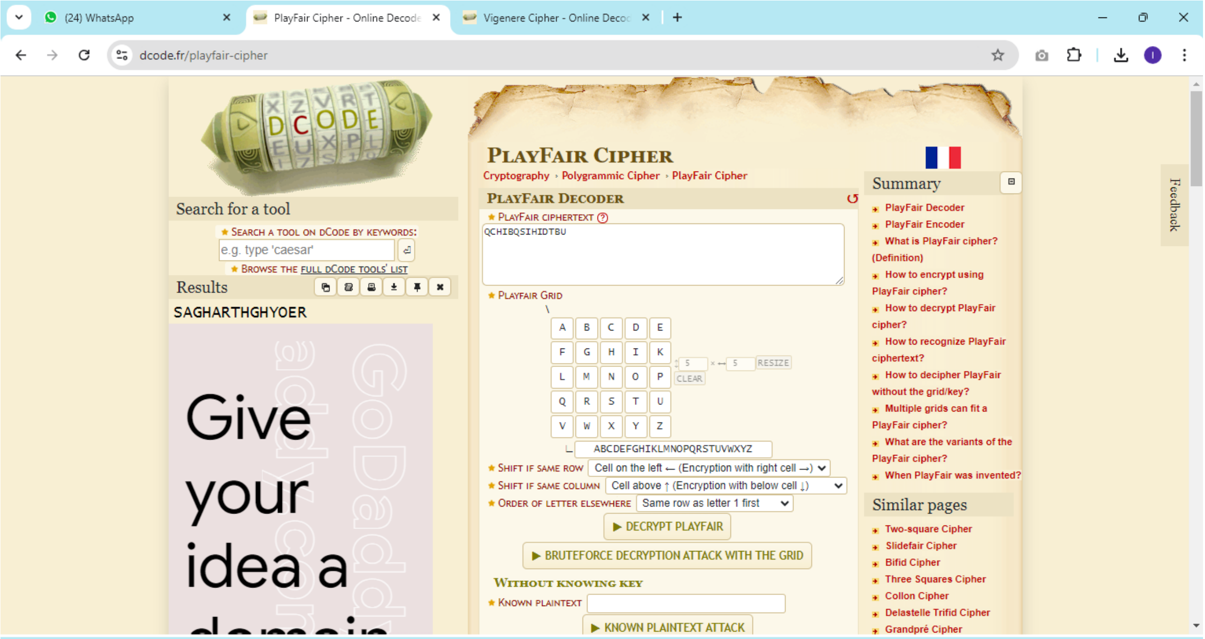
- Repeat the keyword to match the length of the message: `LEMONLEMONLE`.
- Align the plaintext with the keyword:

Plaintext: ATTACKATDAWN

Keyword: LEMONLEMONLE

- For each letter in the plaintext:
- Shift it by the value of the corresponding letter in the keyword using the Vigenère table or by simple Caesar shift.
- `A` + `L` = `L`
- `T` + `E` = `X`
- `T` + `M` = `F`
- `A` + `O` = `O`
- `C` + `N` = `P`
- `K` + `L` = `V`
- `A` + `E` = `E`
- `T` + `M` = `F` - `D` + `O` = `R`
- `A` + `N` = `N`
- `W` + `L` = `H`
- `N` + `E` = `R`

- The encrypted message is: LXFOPVEFRNHR.



(24) WhatsApp
PlayFair Cipher - Online Decode
Vigenere Cipher - Online Decod
dcode.fr/playfair-cipher

Search for a tool

★ Search a tool on dCode by keywords:

e.g. type 'caesar'

★ Browse the full dCode tools' list

Results

SAGHARTHGHYOER

PlayFair Cipher

Cryptography › Polygrammic Cipher › PlayFair Cipher

PlayFair Decoder

★ PlayFair ciphertext

```
QCHIBQSIHIDTBU
```

★ PlayFair Grid

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

5 × 5 RESIZE CLEAR

ABCDEFGHIKLMNOPQRSTUVWXYZ

★ 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

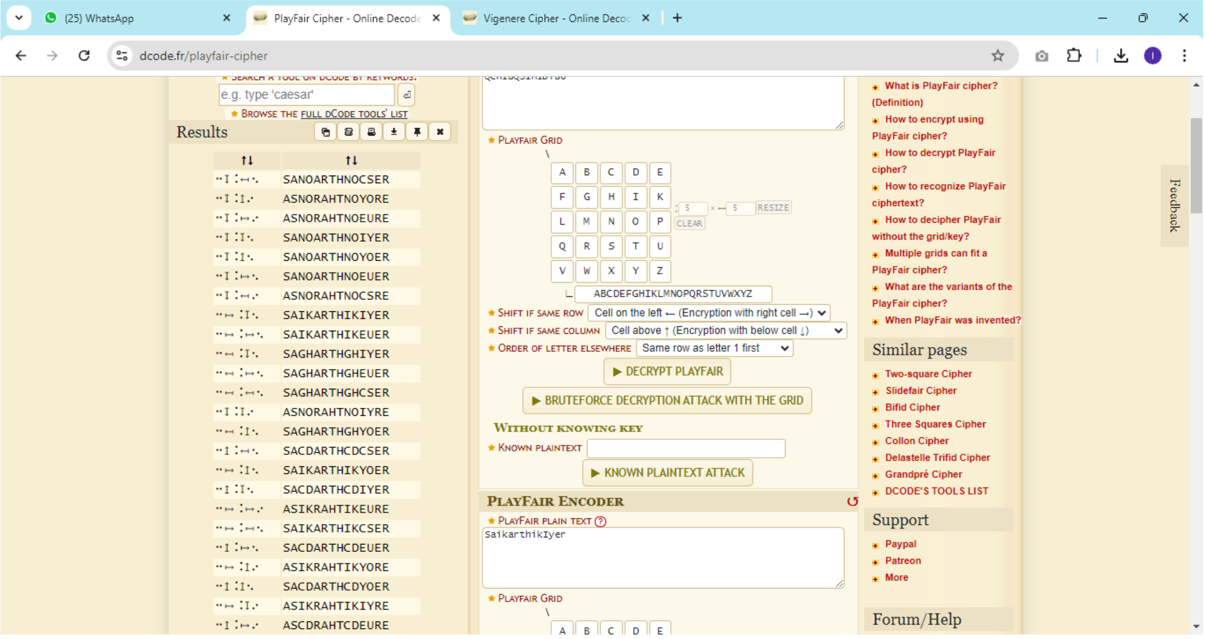
▶ KNOWN PLAINTEXT ATTACK

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
- Delastelle Trifid Cipher
- Grandpré Cipher



(25) WhatsApp
PlayFair Cipher - Online Decode
Vigenere Cipher - Online Decod
dcode.fr/playfair-cipher

★ Search a tool on dCode by keywords:

e.g. type 'caesar'

★ Browse the full dCode tools' list

Results

↑↓	↑↓
··↕ ⁚↤⋱	SANOARTHNOCSER
··↕ ⁚↥⋰	ASNORAHTNOYORE
··↕ ⁚↦⋰	ASNORAHTNOEURE
··↕ ⁚↕⋱	SANOARTHNOIYER
··↕ ⁚↥⋱	SANOARTHNOYOER
··↕ ⁚↦⋱	SANOARTHNOEUER
··↕ ⁚↤⋰	ASNORAHTNOCSRE
··↦ ⁚↕⋱	SAIKARTHIKIYER
··↦ ⁚↦⋱	SAIKARTHIKEUER
··↤ ⁚↕⋱	SAGHARTHGHIYER
··↤ ⁚↦⋱	SAGHARTHGHEUER
··↤ ⁚↤⋱	SAGHARTHGHCSER
··↕ ⁚↕⋰	ASNORAHTNOIYRE
··↤ ⁚↥⋱	SAGHARTHGHYOER
··↥ ⁚↤⋱	SACDARTHCDCSER
··↦ ⁚↥⋱	SAIKARTHIKYOER
··↥ ⁚↕⋱	SACDARTHCDIYER
··↦ ⁚↦⋰	ASIKRAHTIKEURE
··↦ ⁚↤⋱	SAIKARTHIKCSER
··↥ ⁚↦⋱	SACDARTHCDEUER
··↦ ⁚↥⋰	ASIKRAHTIKYORE
··↥ ⁚↥⋱	SACDARTHCDYOER
··↦ ⁚↕⋰	ASIKRAHTIKIYRE
··↥ ⁚↦⋰	ASCDRAHTCDEURE

★ PlayFair Grid

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

5 × 5 RESIZE CLEAR

ABCDEFGHIKLMNOPQRSTUVWXYZ

★ 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

```
SaikarthikIyer
```

★ PlayFair Grid

A	B	C	D	E

- 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?

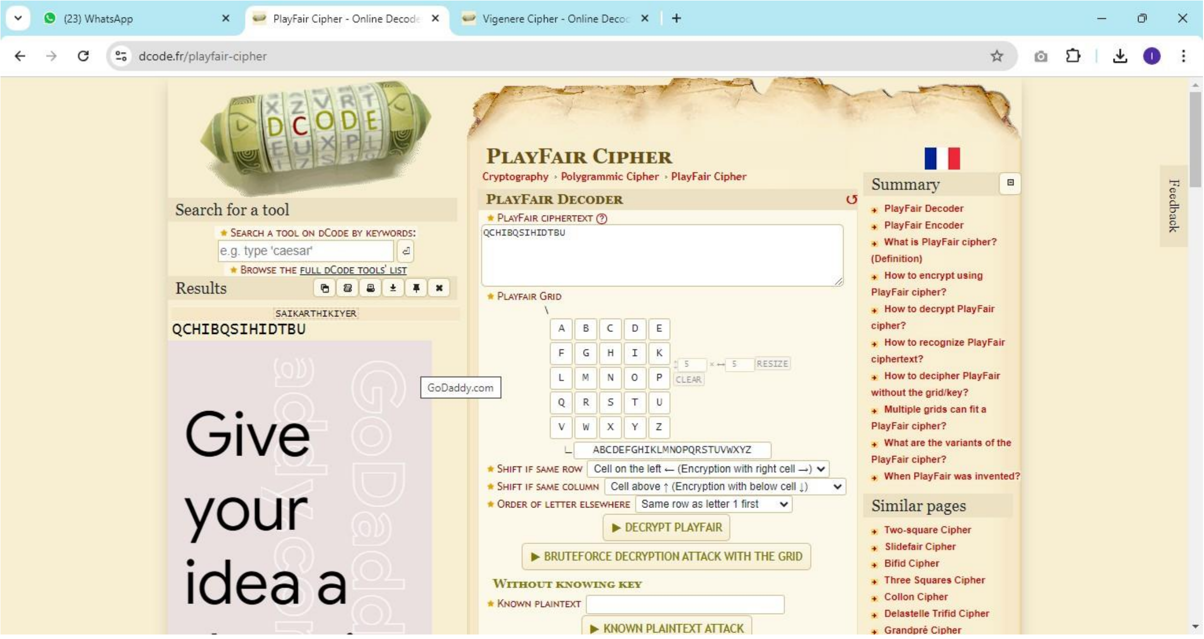
Similar pages

- Two-square Cipher
- Slidefair Cipher
- Bifid Cipher
- Three Squares Cipher
- Collon Cipher
- Delastelle Trifid Cipher
- Grandpré Cipher
- DCODE'S TOOLS LIST

Support

- Paypal
- Patreon
- More

Forum/Help


(23) WhatsApp
PlayFair Cipher - Online Decode
Vigenere Cipher - Online Deco
dcode.fr/playfair-cipher
DCODE
Feedback

Search for a tool

★ Search a tool on dCode by keywords:

e.g. type 'caesar'

★ Browse the full dCode tools' list

Results

SAIKARTHIKIYER

QCHIBQSIHIDTBU

PlayFair Cipher

Cryptography › Polygrammic Cipher › PlayFair Cipher

PlayFair Decoder

★ PlayFair ciphertext ?

QCHIBQSIHIDTBU

★ Playfair Grid

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

5 × 5 RESIZE CLEAR

ABCDEFGHIKLMNOPQRSTUVWXYZ

★ 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

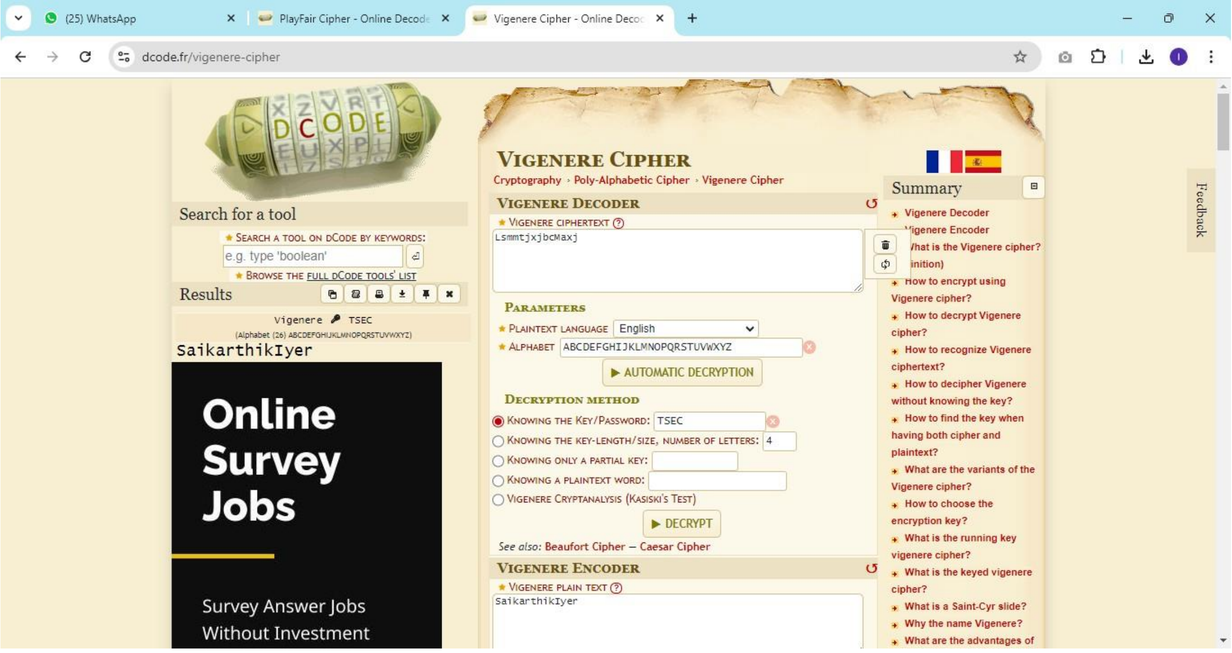
▶ KNOWN PLAINTEXT ATTACK

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
- Delastelle Trifid Cipher
- Grandpré Cipher


(25) WhatsApp
PlayFair Cipher - Online Decode
Vigenere Cipher - Online Deco
dcode.fr/vigenere-cipher
Feedback

Search for a tool

★ SEARCH A TOOL ON DCODE BY KEYWORDS: e.g. type 'boolean'

★ BROWSE THE FULL DCODE TOOLS' LIST

Results

```
Vigenere 🔑 TSEC
(Alphabet (26) ABCDEFGHIJKLMNOPQRSTUVWXYZ)
SaikarthikIyer
```

VIGENERE CIPHER

Cryptography › Poly-Alphabetic Cipher › Vigenere Cipher

VIGENERE DECODER

★ VIGENERE CIPHERTEXT ⓘ

```
LsmmtjxjbcMaxj
```

PARAMETERS

★ PLAINTEXT LANGUAGE: English

★ ALPHABET: ABCDEFGHIJKLMNOPQRSTUVWXYZ

▶ AUTOMATIC DECRYPTION

DECRYPTION METHOD

● KNOWING THE KEY/PASSWORD: TSEC
○ KNOWING THE KEY-LENGTH/SIZE, NUMBER OF LETTERS: 4
○ KNOWING ONLY A PARTIAL KEY:
○ KNOWING A PLAINTEXT WORD:
○ VIGENERE CRYPTANALYSIS (KASISKI'S TEST)

▶ DECRYPT

See also: Beaufort Cipher – Caesar Cipher

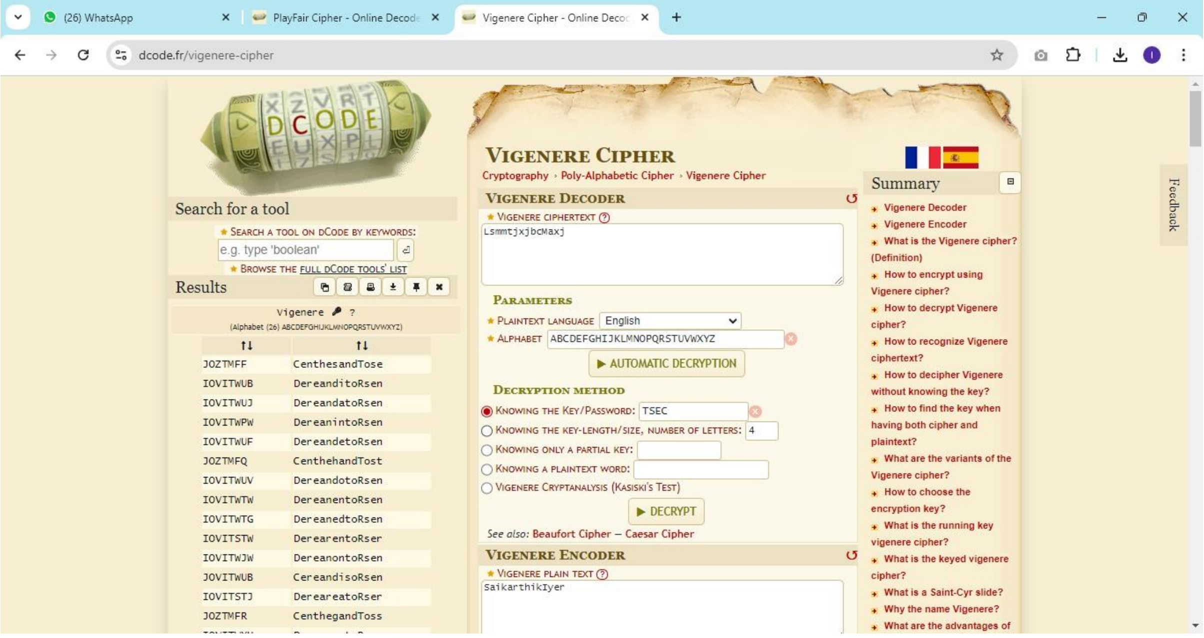
VIGENERE ENCODER

★ VIGENERE PLAIN TEXT ⓘ

```
SaikarthikIyer
```

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


(26) WhatsApp
PlayFair Cipher - Online Decode
Vigenere Cipher - Online Deco
dcode.fr/vigenere-cipher
Feedback

Search for a tool

★ SEARCH A TOOL ON DCODE BY KEYWORDS: e.g. type 'boolean'

★ BROWSE THE FULL DCODE TOOLS' LIST

Results

Vigenere 🔑 ?
(Alphabet (26) ABCDEFGHIJKLMNOPQRSTUVWXYZ)

↑↓	↑↓
JOZTMFF	CenthesandTose
IOVITWUB	DereanditoRsen
IOVITWUJ	DereandatoRsen
IOVITWPW	DereanintoRsen
IOVITWUF	DereandetoRsen
JOZTMFQ	CenthehandTost
IOVITWUV	DereandotoRsen
IOVITWTW	DereanentoRsen
IOVITWTG	DereanedtoRsen
IOVITSTW	DerearentoRser
IOVITWJW	DereanontoRsen
JOVITWUB	CereandisoRsen
IOVITSTJ	DereareatoRser
JOZTMFR	CenthegandToss

VIGENERE CIPHER

Cryptography › Poly-Alphabetic Cipher › Vigenere Cipher

VIGENERE DECODER

★ VIGENERE CIPHERTEXT ⓘ

```
LsmmtjxjbcMaxj
```

PARAMETERS

★ PLAINTEXT LANGUAGE: English

★ ALPHABET: ABCDEFGHIJKLMNOPQRSTUVWXYZ

▶ AUTOMATIC DECRYPTION

DECRYPTION METHOD

● KNOWING THE KEY/PASSWORD: TSEC
○ KNOWING THE KEY-LENGTH/SIZE, NUMBER OF LETTERS: 4
○ KNOWING ONLY A PARTIAL KEY:
○ KNOWING A PLAINTEXT WORD:
○ VIGENERE CRYPTANALYSIS (KASISKI'S TEST)

▶ DECRYPT

See also: Beaufort Cipher – Caesar Cipher

VIGENERE ENCODER

★ VIGENERE PLAIN TEXT ⓘ

```
SaikarthikIyer
```

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