

Roll Number:- 2105048

Name:-Manav Jain

Date:- 26/07/2023

Lab Assignment No:-2

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

Lab Outcome Attained :- LO1

Theory:-

How vigenere cipher works?(with eg)

A technique for encrypting and decrypting messages is the Vigenere Cipher. It is a polyalphabetic substitution cipher, which implies that it encrypts the plaintext using a variety of cipher alphabets.

A keyword, generally a word or phrase, serves as the foundation for encryption in the Vigenere Cipher. To match the length of the plaintext message, the keyword is repeated. The shift value for each letter in the keyword is then calculated for each corresponding letter in the plaintext.

To encrypt a message, each letter of the plaintext is shifted by the corresponding letter in the keyword. Here the plaintext is divided into group of n characters each where n is length of key used for encryption . For Eg:-

Plaintext :- hello world

Key:- vig

Plain text will be divided as follows and mapped with key given accordingly :- (in group of 3)

Hel low orl d

Vig vig vig v

Then $(p+c)\%26$ formula is applied and letter corresponding to it is encoded character

Where , **p:- number corresponding to character in plain text starting from zero** , **c:-number corresponding to character present in key starting from zero**

So applying above text we get **cipher text** as:- **cmrgwcjzry**

Explain in brief how Kasiki test is used to break vigenere cipher?

A cryptanalysis technique for cracking the Vigenere cipher is the Kasiski test. It operates by scanning the ciphertext for repeating character patterns. If a character sequence is found to be repeated, the interval between the sequence's occurrences is most likely to be a multiple of the keyword's length.

Consider the case where the ciphertext comprises the letters "ABCABC". The interval between each occurrence of the sequence will be 3, 6, 9, 12, etc. if the keyword is 3 characters long. The gap between each occurrence of the sequence will be 4, 8, 12, 16, etc.

By finding the distances between repeated sequences in the ciphertext, the cryptanalyst can narrow down the possible values of the keyword length. Once the keyword length is known, the cryptanalyst can then use other methods to break the cipher.

Here is an example of how the Kasiski test can be used to break a Vigenere cipher:

Ciphertext:

ABCDEFGH

HIJKLMN OPQRSTUVWXYZ

The ciphertext's repetitive sequence is the first thing the cryptanalyst discovers. The letters "ABC" are repeated twice in this instance. The sequence's occurrences are separated by 12 steps.

The cryptanalyst can determine that the keyword length is three because the spacing between the sequence's repetitions is a multiple of three. The cryptanalyst can then employ additional techniques, like frequency analysis, to decipher the message.

The Kasiski test is a simple but effective method for breaking the Vigenère cipher. It is not foolproof, but it can be used to break ciphers that have been encrypted with short keywords.

How Playfair Cipher works ? (with eg)

The Playfair cipher is a symmetric encryption method that encrypts and decrypts communications using a 5x5 square letter-keyed matrix. Charles Wheatstone created it in 1854, and Lord Playfair later made it well-known. The primary goal of the Playfair cipher is to convert digraphs (pairs of letters) from plaintext into ciphertext using the encryption methods described below:

1)Before encrypting plain text if two consecutive letters in plaintext are same then insert bogus character 'x' in between them

2)If both characters in pair are in same row replace them by immediate right character from same row

3)If two characters in pair appear in same column replace them with immediate bottom character

4)If above two cases are not satisfied replace them by character in same row but in column of other character

Eg:-

Suppose we want to encrypt the message "HELLO" using the keyword "KEYWORD" (without repeating letters, and 'J' is combined with 'I').

Keyed Matrix Setup:

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

The plaintext "HELLO" is divided into digraphs: "HE" and "LLO".

Encryption Rules:

"HE": H and E are in the same row, so we replace H with the letter to its right (E) and E with the letter to its right (F).

"LLO": L and O form a rectangle, so we replace L with the letter at the opposite corner of the rectangle (M) and O with the letter at the opposite corner of the rectangle (N).

Ciphertext:

The encrypted message is "FE MN NM."

To decrypt the ciphertext, the recipient would use the same keyed matrix and apply the decryption rules in reverse.

How cryptanalysis on playfair cipher can be done ?

Cryptanalysis on the Playfair cipher involves attempting to break the encryption without knowing the key or the plaintext-ciphertext pair. Most common way is using **frequency analysis**

Cryptanalysts can perform frequency analysis on the ciphertext to identify patterns in the letter distribution. In English text, certain letters appear more frequently than others (e.g., 'E' is the most common letter). By analyzing the frequency of letters in the ciphertext, they can make

educated guesses about which letters might correspond to common letters in the English language.

Output Screenshot:-

1)Vigenere cipher - encode plain text

The screenshot displays the dCode Vigenere Cipher tool interface. On the left, a sidebar contains a search bar, a list of results for 'Vigenere' (including 'CNSLAB' and 'Amphenol'), and social media sharing options. The main content area is titled 'VIGENERE CIPHER' and includes a breadcrumb trail: 'Cryptography > Poly-Alphabetic Cipher > Vigenere Cipher'. It features two primary sections: 'VIGENERE DECODER' and 'VIGENERE ENCODER'. The 'VIGENERE DECODER' section has a text input field containing 'nGmni akr bogpitr Fmeorcbi usxfyfr uik!', a 'PARAMETERS' section with 'PLAINTEXT LANGUAGE' set to 'English' and 'ALPHABET' set to 'ABCDEFGHIJKLMNOPQRSTUVWXYZ', and a 'DECRYPTION METHOD' section with 'KNOWING THE KEY/PASSWORD: CNSLAB' selected. The 'VIGENERE ENCODER' section has a text input field containing 'hello this is cns assignmet 2' and 'CIPHER KEY' set to 'CNSLAB'. A right sidebar titled 'Summary' lists various Vigenere cipher-related topics. At the bottom, there is a 'Similar pages' section with links to 'Beaufort Cipher', 'Caesar Cipher', 'Autoclave Cipher', and 'Vigenere Multiplicative'.

VIGENERE CIPHER
Cryptography > Poly-Alphabetic Cipher > Vigenere Cipher

VIGENERE DECODER

★ VIGENERE CIPHERTEXT (?)
nGmni akr bogpitr Fmeorcbi usxfyfr uik!

PARAMETERS

★ PLAINTEXT LANGUAGE English
★ ALPHABET ABCDEFGHIJKLMNOPQRSTUVWXYZ

► AUTOMATIC DECRYPTION

DECRYPTION METHOD

☒ KNOWING THE KEY/PASSWORD: CNSLAB
☐ 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 (?)
hello this is cns assignmet 2

★ CIPHER KEY CNSLAB
★ ALPHABET ABCDEFGHIJKLMNOPQRSTUVWXYZ


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

2)Vigenere cipher - decode cipher text



Search for a tool

★ SEARCH A TOOL ON dCODE BY KEYWORDS:

★ BROWSE THE FULL dCODE TOOLS' LIST


Results


Vigenere

CNSLAB

(Alphabet (26) ABCDEFGHIJKLMNOPQRSTUVWXYZ)

hello this is cns assignmnet 2





FLAT 20% OFF
SITEWIDE SALE


USE CODE: **RUSH20**

TEGO

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 (?)

jr dwo u jvk ts dpf sdsjiaeyeu 2

PARAMETERS

★ PLAINTEXT LANGUAGE

★ ALPHABET

► AUTOMATIC DECRYPTION

DECRYPTION METHOD

☒ KNOWING THE KEY/PASSWORD:

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

☐ 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 (?)

hello this is cns assignmnet 2

★ CIPHER KEY

★ ALPHABET

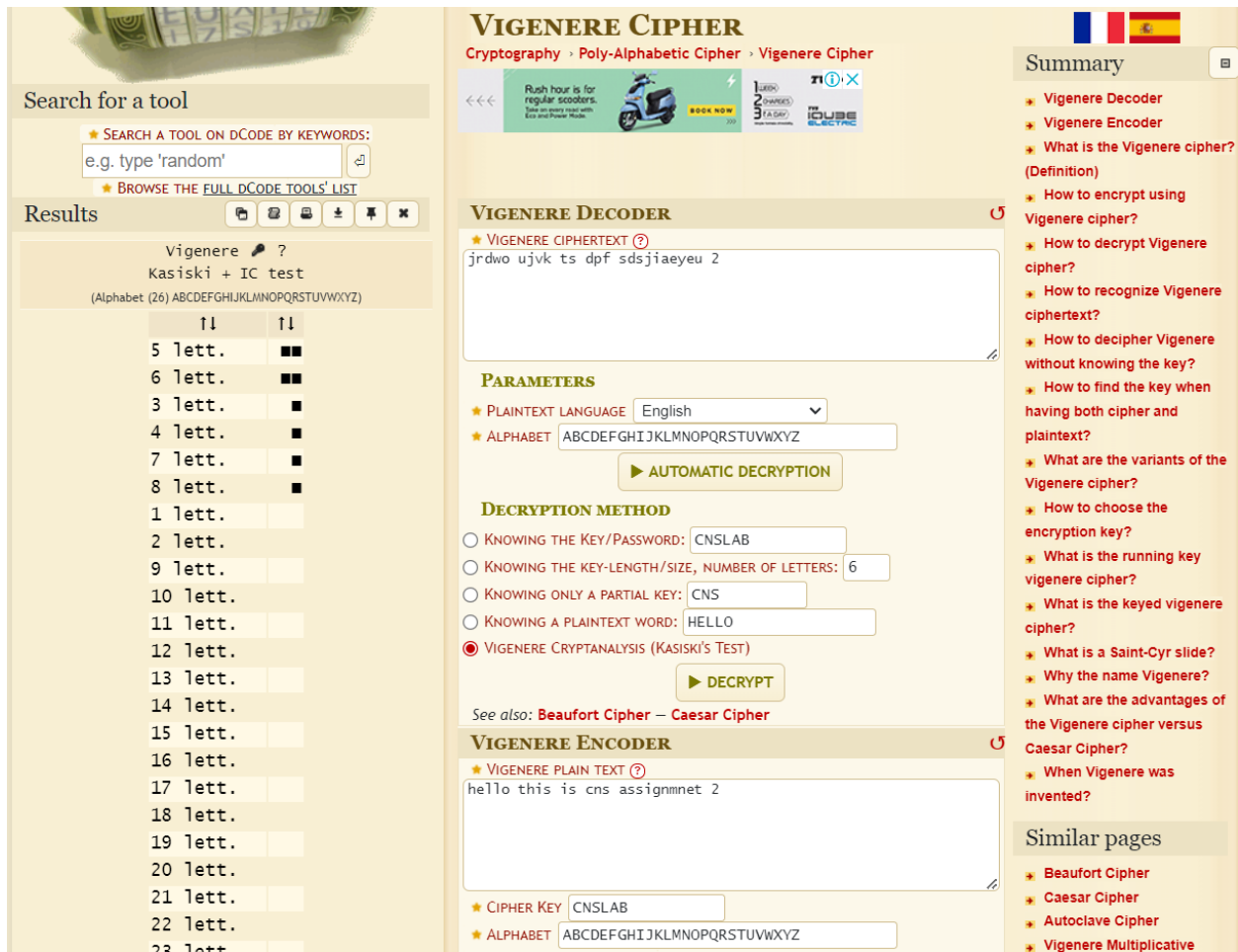
Summary

- 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

3)Vigenere Cipher - Kasiki test



The image shows a web-based Vigenere Cipher tool interface. It is divided into three main sections: a search/results area on the left, a central processing area, and a summary/similar pages area on the right.

Search for a tool: A search bar with the text "e.g. type 'random'" and a link to "BROWSE THE FULL DCODE TOOLS' LIST".

Results: A list of tools including "Vigenere", "Kasiski + IC test", and "Alphabet (26) ABCDEFGHIJKLMNOPQRSTUVWXYZ".

VIGENERE CIPHER: The main title of the tool, with sub-navigation for "Cryptography", "Poly-Alphabetic Cipher", and "Vigenere Cipher".


VIGENERE DECODER: A section for decoding ciphertext. It includes a text input field with the example "jrdwo ujkv ts dpf sdsjiaeyeu 2". Below this are "PARAMETERS" for "PLAINTEXT LANGUAGE" (English) and "ALPHABET" (ABCDEFGHIJKLMNOPQRSTUVWXYZ). A "DECIPHER METHOD" section offers options like "KNOWING THE KEY/PASSWORD", "KNOWING THE KEY-LENGTH/SIZE", "KNOWING ONLY A PARTIAL KEY", and "KNOWING A PLAINTEXT WORD". The "VIGENERE CRYPTANALYSIS (KASISKI'S TEST)" option is selected. A "DECRYPT" button is present.

VIGENERE ENCODER: A section for encoding plaintext. It includes a text input field with the example "hello this is cns assignmnet 2". Below this are "PARAMETERS" for "CIPHER KEY" (CNSLAB) and "ALPHABET" (ABCDEFGHIJKLMNOPQRSTUVWXYZ).

Summary: A list of related topics and questions, such as "Vigenere Decoder", "Vigenere Encoder", "What is the Vigenere cipher?", "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?", and "When Vigenere was invented?".

Similar pages: A list of related tools and concepts, including "Beaufort Cipher", "Caesar Cipher", "Autoclave Cipher", and "Vigenere Multiplicative".

4) Playfair cipher (key - networksecurity) - encode




Search for a tool

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

★ BROWSE THE [FULL DCODE TOOLS' LIST](#)

Results


MYNAMEISNIRANIAN



SAMSUNG

Ecobubble™
Top Load
7.0Kg

Starting ₹ 16316*



-24%

PLAYFAIR CIPHER

Cryptography > Polygrammic Cipher > PlayFair Cipher

PLAYFAIR DECODER

★ PLAYFAIR CIPHERTEXT ?
GDTIGOARRFSIRFIT

★ PLAYFAIR GRID

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

RESIZE: 5 x 5

NETWORKSCUIYABDFGHLMPQVXZ

ABCDEFGHIJKLMNPOQRSTUVWXYZ (-J)
ABCDEFGHIJKLMNPOQRSTUVWXYZ (-V)
ABCDEFGHIJKLMNPOQRSTUVWXYZ (-W)
ABCDEFGHIJKLMNPOQRSTUVWXYZ (-Q)
ABCDEFGHIJKLMNPOQRSTUVWXYZ (-Z)

★ 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

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

Conclusion:-

Successfully implemented cryptanalysis of vigenere cipher as well as playfair cipher and also encoded plain text , learnt in detail about cryptanalysis ,encoding in vigenere , playfair cipher

