

LAB ASSIGNMENT NO. 2

AIM: Cryptanalysis or decoding of polyalphabetic ciphers: Playfair, Vigenere cipher.

LAB OUTCOME ATTAINED:

LO1: Illustrate symmetric cryptography by implementing classical ciphers.

THEORY:

VIGENERE CIPHER

The Vigenère cipher is a method of encrypting alphabetic text by using a simple form of polyalphabetic substitution. It uses a keyword (or keyphrase) to determine the shift value for each letter in the plaintext. The keyword is repeated as necessary to match the length of the plaintext. In the Vigenère cipher, you use a keyword (or keyphrase) to determine the shift value for each letter in your plaintext. First, choose a keyword that you'll repeat to match the length of your plaintext.

For example, let's say your keyword is "KEY" and your plaintext is "HELLO" (all in uppercase).

Keyword: "KEYKEY" (repeating the keyword to match the length of the plaintext).

Plaintext: "HELLO."

Next, refer to the Vigenère Table (or Vigenère Square).

Encrypt your plaintext:

- Match each letter of your plaintext with the corresponding letter of your keyword (H -> K, E -> E, L -> Y, L -> K, O -> E).
- Find the corresponding letter in the Vigenère table at the intersection of the row and column of the matching letters.
- Your encrypted ciphertext is "KYKYE."

USE OF KASISKI TEST

The Kasiski test is a clever method to break the Vigenère cipher by exploiting repeated patterns in the ciphertext. By detecting these repeating substrings and measuring the distances between them, the test can infer the probable length of the keyword used in the encryption. Finding common factors among these distances helps to narrow down the potential keyword lengths.

Once the likely keyword length is determined, the ciphertext is divided into groups based on this length. Each group is then analysed separately using frequency analysis, as if it were encrypted with a simple substitution cipher. Since each group corresponds to a different shift value in the Vigenère cipher, frequency analysis becomes more effective.

By calculating the shift values for each group, the test reconstructs parts of the keyword. By piecing together these parts, the complete keyword is obtained, allowing for the decryption of the entire ciphertext.

Although the Kasiski test can be quite effective, its success depends on the presence of repeating patterns in the ciphertext and the length of the keyword. For shorter ciphertext or longer keywords, the test's accuracy may decrease, and additional techniques might be required for decryption.

PLAYFAIR CIPHER

The Playfair cipher is a digraphic substitution cipher used to encrypt plaintext. It operates on pairs of letters (digraphs) instead of individual letters, making it more secure than simple substitution ciphers. The cipher uses a 5x5 matrix (Playfair square) of letters, typically excluding "J," to create the encryption key.

In the Playfair cipher example, the keyword "KEYWORD" is used to generate the Playfair square. The plaintext "HELLO WORLD" is preprocessed into digraphs ("HE LX LO WO RL DX"). Applying encryption rules, the digraphs are encrypted: "HE" becomes "EK," "LX" becomes "RC," "LO" becomes "OD," and "WO" becomes "BM." The final ciphertext is "EKRCOMEDY." To decrypt, both sender and receiver must use the same Playfair square with the shared keyword to reverse the process and retrieve the original plaintext "HELLOWORLD." The cipher's digraphic approach enhances security compared to simple substitution ciphers, making it a valuable historical encryption technique.






CRYPTANALYSIS OF PLAYFAIR CIPHER


Cryptanalysis of the Playfair cipher aims to decrypt the ciphertext without knowing the keyword or Playfair square. Techniques like frequency analysis, pattern recognition, and the Kasiski examination are employed to identify repeating patterns and deduce likely digraphs. Brute force attacks involve trying all possible keyword and square combinations. Known and chosen plaintext attacks use partial knowledge of the plaintext-ciphertext pairs to infer the key. The Playfair cipher's security depends on the keyword's complexity and the ciphertext length. While it offers better security than simple substitution ciphers, cryptanalysis methods can still be effective with sufficient ciphertext data and clever analysis.

OUTPUT:

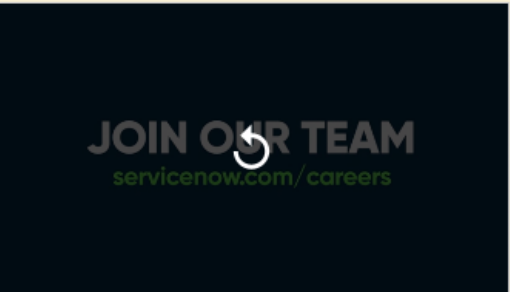
VIGENERE CIPHER

Results



Vigenere  TSEC
(Alphabet (26) ABCDEFGHIJKLMNOPQRSTUVWXYZ)

1zvgrsocfsxj




[Learn more](#)

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 CIPHERTEXT ?

1zvgrsocfsxj

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 ?

shreyakamath

★ CIPHER KEY TSEC

★ ALPHABET ABCDEFGHIJKLMNOPQRSTUVWXYZ

★ PRESERVE PUNCTUATION ☒

[▶ ENCRYPT](#)

Results

Vigenere

TSEC

(Alphabet (26) ABCDEFGHIJKLMNOPQRSTUVWXYZ)

shreyakamath

JOIN OUR TEAM

servicenow.com/careers

Learn more

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 CIPHERTEXT

1zvgrsocfsxj

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

shreyakamath

CIPHER KEY

TSEC

ALPHABET

ABCDEFGHIJKLMNOPQRSTUVWXYZ

PRESERVE PUNCTUATION

ENCRYPT

Results

Vigenere ?
Kasiski + IC test
(Alphabet (26) ABCDEFGHIJKLMNOPQRSTUVWXYZ)

	↑↓	↑↓
4 lett.		■
5 lett.		■
6 lett.		■
3 lett.		■
1 lett.		
2 lett.		
7 lett.		
8 lett.		
9 lett.		
10 lett.		
11 lett.		
12 lett.		
13 lett.		
14 lett.		
15 lett.		
16 lett.		
17 lett.		
18 lett.		
19 lett.		
20 lett.		
21 lett.		
22 lett.		
23 lett.		
24 lett.		

VIGENERE DECODER

★ VIGENERE CIPHERTEXT ?
1zvgrsocfsxj

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 ?
shreyakamath

★ CIPHER KEY TSEC

★ ALPHABET ABCDEFGHIJKLMNOPQRSTUVWXYZ

★ PRESERVE PUNCTUATION ☒

▶ ENCRYPT

Results

Vigenere 4
(Alphabet (26) ABCDEFGHIJKLMNOPQRSTUVWXYZ)

	↑↓	↑↓
AOVV	11alrethfeco	
AOXY	1lyirerefeal	
DNGP	improfincfriu	
XOVV	olaluethieco	
NZGP	yapretinstru	
JSVV	chaliathwaco	
RZKV	uallatehotno	
YOXG	nlyaterwhead	
NZGY	yapietiestrl	
YSVV	nhaltathhaco	
RZKR	ualpatelotns	
DHGP	isprolinclru	
YOVJ	nlaxtettheca	
LOVV	alalgethueco	
KOXO	blysheroveav	
KOXY	blyihereveal	
YKVV	npaltithhico	
YKVJ	npaxtitthica	
XZKG	oalautewitnd	
JZKV	callitehwtno	
YOVO	nlastetohecv	
YAXB	nlyfterbheai	
RZKP	ualratenotnu	
DZGP	iaprotinctru	
YSVO	nhastatohacv	

VIGENERE DECODER

★ VIGENERE CIPHERTEXT ?
1zvgrsocfsxj

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 ?
shreyakamath

★ CIPHER KEY TSEC

★ ALPHABET ABCDEFGHIJKLMNOPQRSTUVWXYZ


★ PRESERVE PUNCTUATION ☒

▶ ENCRYPT

Results

Vigenere TS
 (Alphabet (26) ABCDEFGHIJKLMNOPQRSTUVWXYZ)

TS shcoyavkmaer



"I don't get that 3 o'clock low in the afternoon."

Shop now

Kaytee Boyd
 Integrative nutritionist and former professional athlete

Vigenere Cipher - dCode
 Tag(s) : Poly-Alphabetic Cipher

VIGENERE DECODER

★ VIGENERE CIPHERTEXT (?)
 1zvgrsocfsxj

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: TS
☐ KNOWING A PLAINTEXT WORD:
☐ VIGENERE CRYPTANALYSIS (KASISKI'S TEST)

► DECRYPT

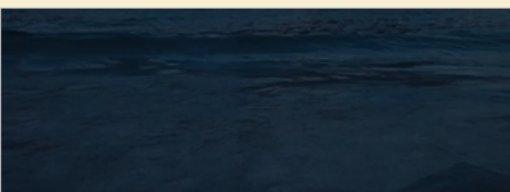
See also: Beaufort Cipher – Caesar Cipher

Results

Vigenere ?
 (Alphabet (26) ABCDEFGHIJKLMNOPQRSTUVWXYZ)

↑↓	↑↓
TSEC	shreyakamath
HLBUXA	eomushreya
WV00ZJ	pehssjshreya
XYHSZL	obooshreyayy
KEFOKB	bvqshreyaeni
OHOPNU	xshreyavrdkp
QCDZAO	vxshreyactxv
TSECTS	shreyavkbqer

#8



VIGENERE DECODER

★ VIGENERE CIPHERTEXT (?)
 1zvgrsocfsxj

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: SHREYA
☐ VIGENERE CRYPTANALYSIS (KASISKI'S TEST)

► DECRYPT

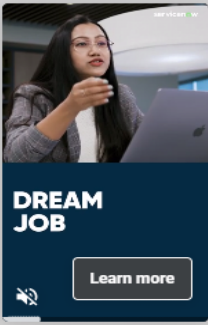
See also: Beaufort Cipher – Caesar Cipher

PLAYFAIR CIPHER

Results

MYNAMEISSHREYA

SETGSFMPPESLTF



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

Share

[+](#) [f](#) [t](#) [r](#) [e](#)

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 DECODER

★ PLAYFAIR CIPHERTEXT (?)

SETGSFMPPESLTF

★ PLAYFAIR GRID

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

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

WHOLEABCFGIZKMNPQRSTUVM

★ 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 (?)

mynameissshreya

★ PLAYFAIR GRID

W	H	O	L	E
A	B	C	D	F

W H O L E
A B C D F

Results

MYNAMEISSHREYA



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

Share

[+](#) [f](#) [t](#) [r](#) [e](#)

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 DECODER

★ PLAYFAIR CIPHERTEXT (?)

SETGSFMPPESLTF

★ PLAYFAIR GRID

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

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

WHOLEABCFGIZKMNPQRSTUVM

★ 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

Roll no. : 53
Name: Shreya Kamath
Date: 27th July, 2023.

CONCLUSION:

Hence, we have conducted Cryptanalysis or decoding of polyalphabetic ciphers such as the Playfair and Vigenere cipher. We also understood how the Kasiski Test is used to break the Vigenere cipher.