

INS Practical 3

Date: **27-02-2023**

Roll no.: **20BCE119**

Name: **Kartavya Patel**

Course Code and Name: **2CSDE54 Information and Network Security**

Task

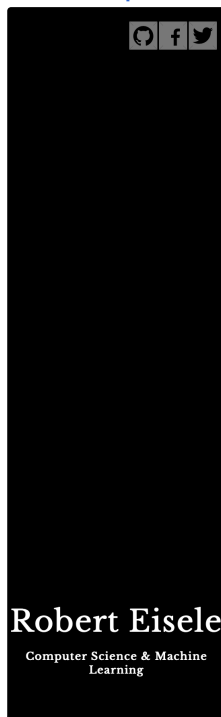
- Exploration of various tools to perform encryption and decryption

Caesar cipher tools

Link: <https://www.boxentriq.com/code-breaking/caesar-cipher>

The screenshot shows the Boxentriq website's interface for the Caesar Cipher tool. At the top, there's a navigation bar with 'BOXENTRIQ' and links for 'TOOLS', 'PUZZLE', and 'ABOUT'. Below this is a dark green header with the text 'Caesar Cipher Decoder, Solver and Encoder'. A search bar with the placeholder 'Find Tools...' is visible. A large banner for 'PLAYGROUND 2' is displayed, featuring the text 'EXCLUSIVE EPISODES EVERYDAY', 'NEW SEASON', and 'amazon miniTV WATCH FREE'. The main content area contains a paragraph explaining that the tool is a complete guide to the Caesar cipher and the tools needed to decode it. It lists several links: 'Caesar Cipher Tool (supporting English, French, German, Italian, Portugese, Spanish, Swedish)', 'Cipher Description and Cryptanalysis', 'History', 'Usage', and 'Trivia'. Below this, a paragraph states that the Caesar cipher, also known as a shift cipher, Caesar's code, or Caesar shift, is one of the oldest and most famous ciphers in history. It mentions that while being deceptively simple, it has been used historically for important secrets and is still popular among puzzlers. Another paragraph asks if the user is unsure if their cipher is a Caesar cipher and suggests using the 'Cipher Identifier' to find the right tool. At the bottom, there's a section titled 'Caesar Cipher Tool' with a text input field containing the word 'Hello'. Below the input field are buttons for 'Copy', 'Paste', and 'Text Opti...'. A 'Close X' button is also visible in the top right corner of the tool interface.

Link: <https://www.xarg.org/tools/caesar-cipher/>



[HOME](#) [ABOUT](#) [ARCHIVE](#) [PROJECTS](#)

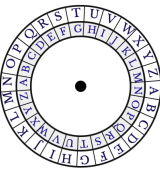
Caesar cipher decryption tool

The following tool allows you to encrypt a text with a simple offset algorithm - also known as Caesar cipher. If you are using 13 as the key, the result is similar to an **rot13 encryption**. If you use "guess" as the key, the algorithm tries to find the right key and decrypts the string by guessing. I also wrote a small article (with source) on **how to crack caesar-cipher** in an unknown context of an encrypted text.

If you want some in-depth knowledge, I highly recommend to read this **book**.

Genius without education is like silver in the mine

Use key: 13




Encrypt / Decrypt


Output:

Travhfjvgubhg rghpngvba vf yvxr fvyire va gur zvar.

© 2008 - 2023 Robert Eisele All rights reserved • [Privacy Policy](#), [Contact](#)

Link: <https://cryptii.com/pipes/caesar-cipher>

 Try out the new experience

 Students and Teachers, save up to 60% on Adobe Creative Cloud.
ads via Carbon

VIEW

Plaintext

If he had anything confidential to say, he wrote it in cipher, that is, by so changing the order of the letters of the alphabet, that not a word could be made out.

ENCODE DECODE

Caesar cipher

SHIFT

- 7 a→h +

ALPHABET

abcdefghijklmnopqrstuvwxyz

CASE STRATEGY

Maintain case

FOREIGN CHARS

Include Ignore

→ Encoded 163 chars

VIEW

Ciphertext

Pm ol ohk hufaopun jvumpkluaaphs av zhf, ol dyval pa pu jpwoly, aoha pz, if zv johunpun aol vykly vm aol slaalyz vm aol hswohila, aoha uva h dvyk jvbsk il thkl vba.

Caesar cipher: Encode and decode online

Method in which each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet. The method is named after Julius Caesar, who used it in his private correspondence.

[Decimal to text](#) [URL encode](#) [Enigma decoder](#) [Text to binary](#) [Commercial Enigma](#)

 Open in ciphereditor

Link: <https://md5decrypt.net/en/Caesar/>

[Home](#) [Encrypt / Decrypt](#) [Conversion tools](#) [Ciphers](#) [API](#) [Contact](#) [FR](#) [EN](#)

Caesar Cipher Decoder & Encoder

Shift :

[Encrypt](#) [Decrypt](#) [Bruteforce](#)

About Caesar cipher Decoder Online :

Caesar cipher is a basic letters substitution algorithm. It takes as input a message, and apply to every letter a particular shift. This shift used to be 3 (Caesar shift), according to history, when it was used by Caesar to encrypt war messages (so for example a would become d, b will be e, and so on and so forth). Of course you can choose any shift you want. This is basically a modulo 26 addition; Caesar cipher, as [Polybius Square cipher](#), is a monoalphabetical cipher. Like the others of this kind, the problem of this cipher is its really poor security. To break it, you can, like I do here, apply every shift to the Caesar cipher, and see if there's one that makes sense.

Link: <https://www.thewordfinder.com/caesar-cipher-solver/>

CAESAR CIPHER DECODER

Enter your text below to decrypt or encrypt!

SOLVE / DECODE TEXT

Enter your text here

Shift

Custom Alphabet (max 40 letters)
ABCDEFGHIJKLMNOPQRSTUVWXYZ

☐ Use bruteforce to decrypt

DECODE TEXT

ENCRYPT / ENCODE TEXT

Enter your text here

Shift

Custom Alphabet (max 40 letters)
ABCDEFGHIJKLMNOPQRSTUVWXYZ

ENCODE TEXT

Cipher lookup table based upon +3 shift.

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

This is where you can put some information about how the cipher / tool works.

Plain Text: I was busy reading the dictionary when you called

Cipher Text: L xdu gubv xubduel wlv slludvduv sllubv xubduv

Transposition cipher tools

Link: <https://www.boxentriq.com/code-breaking/columnar-transposition-cipher>

BOXENTRIQ

TOOLS PUZZLE ABOUT

Columnar Transposition Cipher Decoder and Encoder

Find Tools...

In a columnar transposition cipher, the message is written in a grid of equal length rows, and then read out column by column. The columns are chosen in a scrambled order, decided by the encryption key. Since transposition ciphers doesn't affect the letter frequencies, it can be detected through [frequency analysis](#). Like other transposition ciphers, it can be attacked by moving letters around and anagramming. Also it can be attacked using brute-force methods if the key isn't long enough.


Columnar Transposition Cipher Tool


Enter message here...

Copy

Paste

Text Options...

 Type key here...

 English

Decode

Encode

Auto Solve (without key)

Instructions

Show grid

Auto Solve Options

Min Key Length

Max Key Length

Max Repeats

Shifting Mode

Link: <https://tholman.com/other/transposition/>

Transposition Cipher Solver

This is a little tool to help decrypt transposition ciphers in the horizontal column switching format. Obviously this tool wont just solve your cipher for you, you will have to work for it. Luckily for you though, its very simple. Firstly, Enter your cipher text in the textarea below, pick a period (any number) and press (re) load table.

Enter the encrypted text here

Proposed Key length: (re)load table

Transposition Cipher Solver v0.8 | [Tim Holman](#) | [Using Dragtable](#)

Link: <https://www.cryptool.org/en/cto/transposition>

The screenshot shows the CryptTool-Online website interface. At the top, there's a green header with the logo and navigation links for CryptTool Portal, CryptTool 1, CryptTool 2, and JCrypTool. Below this is a green navigation bar with links: CTO Overview, What is CryptTool-Online?, Source Code, and Links. The main content area is titled "Simple Column Transposition" with a subtitle "Cipher that interchanges lines of the plaintext". It features a table with columns: Cipher, Description, and Internal working. Below the table, there's an input section with a text area for "Input" (containing "Hello this is a test. Please enter your text here"), a "Keyword" field (containing "[according permutation: 1,4,5,3,2,6]"), and a "Cipher" field. There are also "Encipher" and "Decipher" buttons. At the bottom, there's a "Options" section with "Alphabet" and "Show grid" checkboxes. A cookie notice is visible at the very bottom.

Link: <https://asecuritysite.com/encryption/col>

The screenshot shows the Asecuritysite.com website interface. At the top, there's a header with the logo and navigation links: HOME, CIPHER, IP, IDS, MAGIC, NET, CISCO, CYBER, ENCRYPT, TEST, FUN, SUBJ, ABOUT. The main content area is titled "Columnar Transposition Cipher". Below this, there's a section for "[Encryption Home][Home]". The interface includes a "Parameters" section with a "Message" field (containing "DYNAMITWINTERPALACE"), a "Key" field (containing "ZEBRAS"), and a "Mode" dropdown (set to "Encrypt"). There's a "Determine" button. Below the parameters, there's a "Try an example:" section with two bullet points: "peterpiperpickedapickedpepper" and key of "GERMAN", and "defendtheeastwallofthecastle" and key of "GERMAN". To the right of the parameters, there's a large black area for the result, with the text "MNLNWPYEREIAITADTEC" visible at the top.

Link: <https://crypto.interactive-maths.com/columnar-transposition-cipher.html>

Columnar Transposition Cipher

Cipher Activity

Introduction

Encryption

Decryption

Discussion

Exercise

Alphabet:	
<input type="text" value="Standard"/>	
<input type="text" value="abcdefghijklmnopqrstuvwxyz"/>	
Key:	
<input type="text" value="Random Key"/> Random Key Length: <input type="text" value="5"/>	
Plaintext:	
<input type="text"/>	<input type="button" value="Encrypt"/>
<input type="button" value="Slow Encrypt"/>	
Ciphertext:	
<input type="text"/>	<input type="button" value="Decrypt"/>
<input type="button" value="Slow Decrypt"/>	

