


127.0.0.1:5500/index.html

Apps Gmail YouTube Maps

Other bookmarks




Crypto Ciphers

Home Caesar Cipher Morse Code Cipher Running Key Cipher ASCII Cipher Atbash Cipher Vemam Cipher

Ciphers

Ciphers are considered to be the foundation of cryptography. In general, a cipher is nothing more than a collection of instructions (an algorithm) for conducting both encryption and decryption. Despite the fact that they appear to be a basic notion, ciphers play an important function in current technology. Ciphers are used in communication technologies such as the internet, mobile phones, digital television, and even ATMs to ensure security and privacy.

Although the majority of individuals claim they are unfamiliar with cryptography, they are often familiar with the notion of ciphers, whether or not they are aware of it. The Da Vinci Code and National Treasure: Book of Secrets are two recent films with narratives built on encryption and ciphers, presenting these subjects to a wider audience. Thus, in order to give a realistic solution, we have developed a javascript implementation for some ciphers that allows you to encrypt and decrypt arbitrary text (of your choice). A brief history of each cipher is also supplied, along with cryptanalysis tips.



The Cipher Disk

Leon Alberti was a renaissance man, literally. Some have compared him to Leonardo Di Vinci (Sorriso, "The Alberti Cipher"). Like Di Vinci, Alberti loved to invent and explore new boundaries of science and math. His most famous invention was by far, "The formula" or as it is known today, the cipher disk. The cipher disk is the first mechanical device invented to encrypt a language (Sarfinkel and Grunspan 26).

Modern Ciphers


Modern algorithms are those that are used in current technology e.g. block ciphers, public key cryptosystems etc. These algorithms are very secure (otherwise they would not be used), but in many cases we can practice on weakened versions of the algorithms. These algorithms are very secure (otherwise they would not be used), but we can practice on weakened versions of the algorithms in most cases.

Due to this never-ending battle of computing power, computers using the internet usually support a large list of ciphers at any given time. This list of ciphers is called a cipher suite and when two computers connect, they share the list of ciphers they both support and a common cipher is agreed upon in order to carry out encryption between them. This process exists to ensure the greatest interoperability between users and servers at any given time. Ciphers such as the Enigma and DES (Data Encryption Standard) have been broken and are no longer considered safe for cryptographic use. To date, RSA (Rivest, Shamir, Adleman) and AES (Advanced Encryption Standard) are considered safe, but as computing power increases, these will also fall one day and new ciphers will have to be developed to continue the use of cryptography on the web.

127.0.0.1:5500/HTML/caesar-cipher.html

Apps Gmail YouTube Maps

Other bookmarks



Crypto Ciphers

Home Caesar Cipher Morse Code Cipher Running Key Cipher ASCII Cipher Atbash Cipher Vemam Cipher

Caesar Cipher

The Caesar cipher (or Caesar code) is a monoalphabetic substitution cipher, where each letter is replaced by another letter located a little further in the alphabet (therefore shifted but always the same for given cipher message). The shift distance is chosen by a number called the offset, which can be right (A to B) or left (B to A).

Encryption:

Encryption with Caesar code is based on an alphabet shift. The most commonly used shift/offset is by 3 letters.

Plain Alphabet ABCDEFGHIJKLMNOPQRSTUVWXYZ

Caesar Alphabet (←3) DEF GHIJ KLMNOPQRSTU VWXYZABC

Example: Encrypt DCODEX with a shift of 3. To encrypt D, take the alphabet and look 3 letters after. G. So D is encrypted with G. To encrypt X, loop the alphabet after X: Y, after Y: Z, after Z: A. So X is coded A. DCODEX is coded GFRGHA.

Decryption:

Caesar code decryption replaces a letter another with an inverse alphabet shift: a previous letter in the alphabet.

Example: Decrypt GFRGHA with a shift of 3.

To decrypt G, take the alphabet and look 3 letters before: D. So G is decrypted with D.

To decrypt X, loop the alphabet, before A: Z, before Z: Y, before Y: X. So A is decrypted X.

GFRGHA is decrypted DCODEX.

Another way to decrypt, more mathematical, note A=0, B=1, ..., Z=25, subtracts a constant (the shift), then the result modulo 26 (alphabet length) is the plain text.

Example: Take G=6, subtract the shift 6-3=3 and 3=D, so G is decrypted with D. Take A=0, 0-3=-3 and -3 mod 26 = 23=X, so A is decrypted with X, etc. GFRGHA is decrypted DCODEX.

Another way to decrypt, more mathematical, note A=0, B=1, ..., Z=25, subtracts a constant (the shift), then the result modulo 26 (alphabet length) is the plain text.
Example: Take G=6, subtract the shift 6 $6-3=3$ and $3-D$, so G is decrypted with D. Take A=0, $0-3=-3$ and $-3 \bmod 26 = 23$, $23=X$, so A is decrypted with X, etc. GFRGHA is decrypted DCODEX

Caesar Cipher Implementation

Input Data:

Key:

Output Data:

Instructions:

1. Enter the text to encrypt
2. Enter any number as key.
3. Click on encrypt button to encrypt the text.
4. Follow the same instructions to decrypt.

Encrypt

Decrypt

Clear

Another way to decrypt, more mathematical, note A=0, B=1, ..., Z=25, subtracts a constant (the shift), then the result modulo 26 (alphabet length) is the plain text.
Example: Take G=6, subtract the shift 6 $6-3=3$ and $3-D$, so G is decrypted with D. Take A=0, $0-3=-3$ and $-3 \bmod 26 = 23$, $23=X$, so A is decrypted with X, etc. GFRGHA is decrypted DCODEX

Caesar Cipher Implementation

Input Data:

Key:

Output Data:

Instructions:

1. Enter the text to encrypt
2. Enter any number as key.
3. Click on encrypt button to encrypt the text.
4. Follow the same instructions to decrypt.

Encrypt

Decrypt

Clear