**ACM PROJECT**

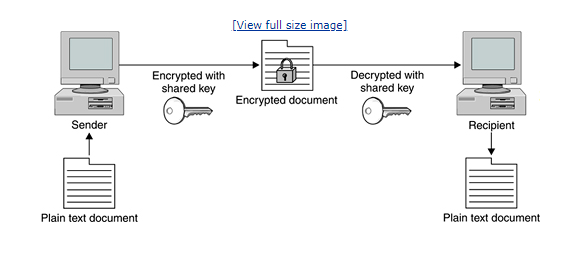
**CRYPTOGRAPHY TECHNIQUE IMPLEMENTATIONS**

**Cryptography** is a method of protecting information and communications through the use of codes, so that only those for whom the information is intended can read and process it. The prefix **"crypt-"** means **"hidden"** or **"vault"** -- and the suffix **"- graphy "** stands for **"writing."**

In computer science, cryptography refers to secure information and communication techniques derived from mathematical concepts and a set of rule-based calculations called algorithms, to transform messages in ways that are hard to decipher. These deterministic algorithms are used for cryptographic key generation, digital signing, verification to protect data privacy, web browsing on the internet, and confidential communications such as credit card transactions and email.

**Modern cryptography concerns itself with the following four objectives:**

1. **Confidentiality**: the information cannot be understood by anyone for whom it was unintended
2. **Integrity:**the information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected
3. **Non-repudiation**: the creator/sender of the information cannot deny at a later stage his or her intentions in the creation or transmission of the information
4. **Authentication**: the sender and receiver can confirm each other's identity and the origin/destination of the information



**History of cryptography**

The word "cryptography" is derived from the Greek *kryptos*, meaning hidden. The origin of cryptography is usually dated from about 2000 B.C., with the Egyptian practice of hieroglyphics. These consisted of complex pictograms, the full meaning of which was only known to an elite few. The first known use of a modern[**cipher**](https://searchsecurity.techtarget.com/definition/cipher) was by Julius Caesar (100 B.C. to 44 B.C.), who did not trust his messengers when communicating with his governors and officers. For this reason, he created a system in which each character in his messages was replaced by a character three positions ahead of it in the Roman alphabet.

In recent times, cryptography has turned into a battleground of some of the world's best mathematicians and computer scientists. The ability to securely store and transfer sensitive information has proved a critical factor in success in war and business.

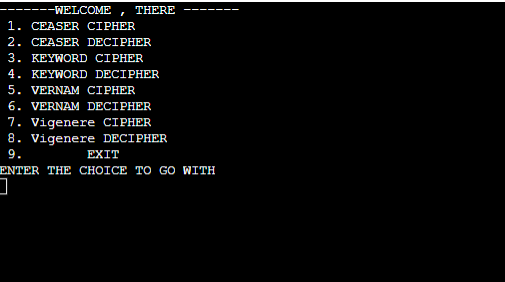
Because governments do not wish certain entities in and out of their countries to have access to ways to receive and send hidden information that may be a threat to national interests, cryptography has been subject to various restrictions in many countries, ranging from limitations of the usage and export of software to the public dissemination of mathematical concepts that could be used to develop cryptosystems. However, the internet has allowed the spread of powerful programs and, more importantly, the underlying techniques of cryptography, so that today many of the most advanced cryptosystems and ideas are now in the public domain.

## How Does Encryption Work?

Now that we are clear on the concept of encryption, let’s have a look at how exactly it works. In simpler words, encryption uses algorithms to jumble up whatever data you want to encrypt. You need to have a randomly generated key before sending the message or data to the person at the receiving end, through which they can decrypt it. Imagine you have put a lock on the box containing important documents with the help of a key. You send that box to your friend. She has the same key as yours through which she is able to unlock it and get access to those important documents. But in the digital world, all this is done electronically!

So, there are **three encryption levels** that are at work:

1. **Plain text**
2. **Encrypted text (ciphertext)**
3. **Decrypted text (same as the initial plain text).**



CEASER ENCRYPTION :

The Caesar Cipher technique is one of the earliest and simplest method of encryption technique. It’s simply a type of substitution cipher, i.e., each letter of a given text is replaced by a letter some fixed number of positions down the alphabet. For example with a shift of 1, A would be replaced by B, B would become C, and so on. The method is apparently named after Julius Caesar, who apparently used it to communicate with his officials.   
Thus to cipher a given text we need an integer value, known as shift which indicates the number of position each letter of the text has been moved down.   
The encryption can be represented using modular arithmetic by first transforming the letters into numbers, according to the scheme, A = 0, B = 1,…, Z = 25. Encryption of a letter by a shift n can be described mathematically as. 

(Encryption Phase with shift n)

(Decryption Phase with shift n)



**Examples :** 

**Text** : ABCDEFGHIJKLMNOPQRSTUVWXYZ

**Shift**: 23

**Cipher**: XYZABCDEFGHIJKLMNOPQRSTUVW

**Text** : ATTACKATONCE

**Shift**: 4

**Cipher**: EXXEGOEXSRGI

**Algorithm for Caesar Cipher:**   
**Input:** 

1. A String of lower case letters, called Text.
2. An Integer between 0-25 denoting the required shift.

**Procedure:** 

* Traverse the given text one character at a time .
* For each character, transform the given character as per the rule, depending on whether we’re encrypting or decrypting the text.
* Return the new string generated.

Program that receives a Text (string) and Shift value( integer) and returns the encrypted text.

**How to decrypt?**   
We can either write another function decrypt similar to encrypt, that’ll apply the given shift in the opposite direction to decrypt the original text. However we can use the cyclic property of the cipher under modulo , hence we can simply observe   
 Hence, we can use the same function to decrypt, instead we’ll modify the shift value such that shift = 26-shift

# Keyword Cipher

A keyword cipher is a form of [monoalphabetic substitution](https://en.wikipedia.org/wiki/Monoalphabetic_substitution" \t "_blank). A keyword is used as the key, and it determines the letter matchings of the cipher alphabet to the plain alphabet. Repeats of letters in the word are removed, then the cipher alphabet is generated with the keyword matching to A, B, C etc. until the keyword is used up, whereupon the rest of the ciphertext letters are used in alphabetical order, excluding those already used in the key. 

**Encryption**

First line of input contains keyword which you wish to enter. Second line of input contains the string which you have to encrypt.   
**Plaintext :** 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   
**Encrypted :** K R Y P T O S A B C D E F G H I J L M N Q U V W X Z  
With KRYPTOS as the keyword, all As become Ks, all Bs become Rs and so on. Encrypting the message “knowledge is power” using the keyword “kryptos”:   
Encrypting the message: Knowledge is Power   
Encoded message: IlmWjbaEb gq NmWbp  
**Examples:** 

**Input :**

Keyword : secret

Message : zombieHere

**Output :**

Ciphered String : zljeftdtot

Take the first example, we used "secret" keyword there.

**Plain Text : 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**

When "secret" keyword is used, the new encypting text becomes :

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

This means 'A' means 'S', 'B' means 'E' and 'C' means 'C' and so on.

Lets encode the given message "Zombie Here"

ZOMBIE HERE becomes zljeftdtot

**Decryption**

To decode the message you check the position of given message in encrypting text with the plain text.

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

Message : PTYBIATLEP   
Deciphered Text : DECIPHERED

Now, how we generate the deciphered string?   
We search for ‘P’ in Encrypted Text and compare its position with plain text letter and generate that letter. So ‘P’ becomes ‘D’, ‘T’ becomes ‘E’, ‘Y’ becomes ‘C’ and so on.

# Vernam Cipher

The Vernam Cipher is an algorithm invented in 1917 to encrypt teletype (TTY) messages.

So named for Gilbert Sandford Vernam, it is a symmetric cipher patented July 22, 1919. The Vernam Cipher combines plaintext (the original message) with pseudo-random series of polyalphabetic characters to form the ciphertext using an “exclusive or” (XOR) function. US Army Captain Joseph Mauborgne soon discovered that the cipher could be made much stronger by using truly random numbers printed on pads of paper. Streams of paper with the random numbers in that fashion became a process known as “one-time pad”. The Vernam using one-time pad is regarded as unbreakable.

On background, a teletype is a character printer connected to a telegraph that provides a user interface for people to communicate over various communications protocols such as dedicated or public wires, radio, or microwave.

**Method to take key:**   
In Vernam cipher algorithm, we take a key to encrypt the plain text which length should be equal to the length of the plain text.

**Encryption Algorithm:** 

1. Assign a number to each character of the plain-text and the key according to alphabetical order.
2. Add both the number (Corresponding plain-text character number and Key character number).
3. Subtract the number from 26 if the added number is greater than 26, if it isn’t then leave it.

**Plain-Text:** RAMSWARUPK

**Key:** RANCHOBABA

**PT:** r a m s w a r u p k

**NO:** 17 0 12 18 22 0 17 20 15 10

**KEY:** r a n c h o b a b a

**NO:** 17 0 13 2 7 14 1 0 1 0

**CIPHER-TEXT:** i a z u d o s u q k

Now add the number of Plain-Text and Key and after doing the addition and subtraction operation (if required), we will get the corresponding Cipher-Text character number. 

# Vigenère Cipher

Vigenere Cipher is a method of encrypting alphabetic text. It uses a simple form of [polyalphabetic substitution](https://en.wikipedia.org/wiki/Polyalphabetic_cipher" \t "_blank). A polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets .The encryption of the original text is done using the *[Vigenère square or Vigenère table](https://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher" \l "/media/File:Vigen%C3%A8re_square_shading.svg" \t "_blank)*.

* The table consists of the alphabets written out 26 times in different rows, each alphabet shifted cyclically to the left compared to the previous alphabet, corresponding to the 26 possible[Caesar Ciphers](https://www.geeksforgeeks.org/caesar-cipher/).
* At different points in the encryption process, the cipher uses a different alphabet from one of the rows.
* The alphabet used at each point depends on a repeating keyword.

**Example:** 

Input : Plaintext : GEEKSFORGEEKS

Keyword : AYUSH

Output : Ciphertext : GCYCZFMLYLEIM

For generating key, the given keyword is repeated

in a circular manner until it matches the length of

the plain text.

The keyword "AYUSH" generates the key "AYUSHAYUSHAYU"

The plain text is then encrypted using the process

explained below.

**Encryption**

The first letter of the plaintext, G is paired with A, the first letter of the key. So use row G and column A of the Vigenère square, namely G. Similarly, for the second letter of the plaintext, the second letter of the key is used, the letter at row E and column Y is C. The rest of the plaintext is enciphered in a similar fashion.

**Decryption**

Decryption is performed by going to the row in the table corresponding to the key, finding the position of the ciphertext letter in this row, and then using the column’s label as the plaintext. For example, in row A (from AYUSH), the ciphertext G appears in column G, which is the first plaintext letter. Next we go to row Y (from AYUSH), locate the ciphertext C which is found in column E, thus E is the second plaintext letter.  
A more **easy implementation** could be to visualize Vigenère algebraically by converting [A-Z] into numbers [0–25]. 

**Encryption**

The plaintext(P) and key(K) are added modulo 26.

Ei = (Pi + Ki) mod 26

**Decryption**

Di = (Ei - Ki + 26) mod 26