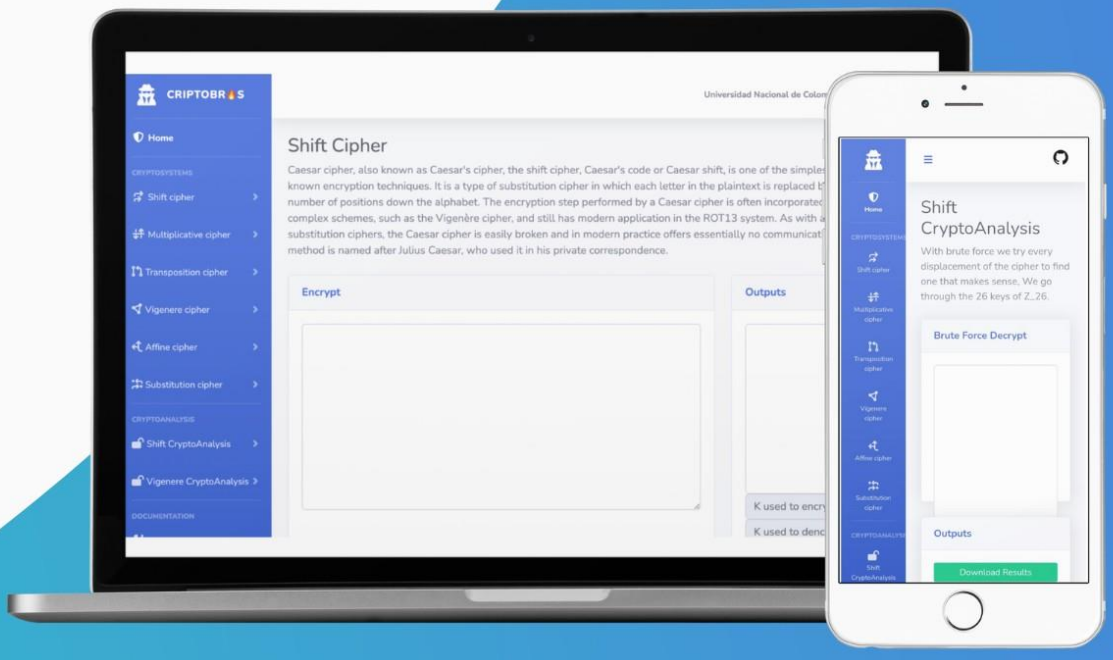
CRIPTOBROS

CRIPTOBROS
USER MANUAL

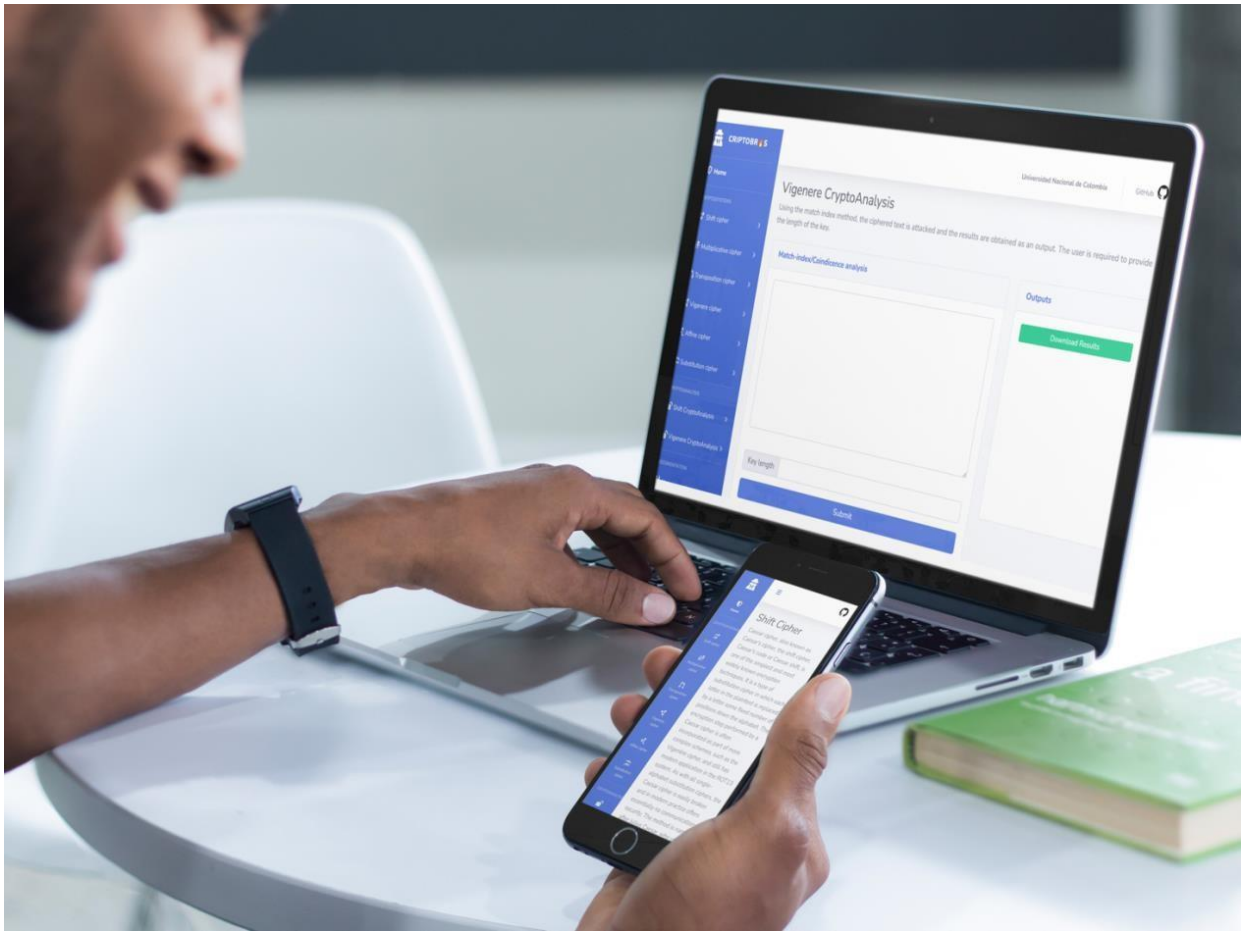


Content

1. Introduction:

Modern cryptography is heavily based on mathematical theory and computer science practice; cryptographic algorithms are designed around computational hardness assumptions, making such algorithms hard to break in actual practice by any adversary. While it is theoretically possible to break into a well-designed system, it is infeasible in actual practice to do so.

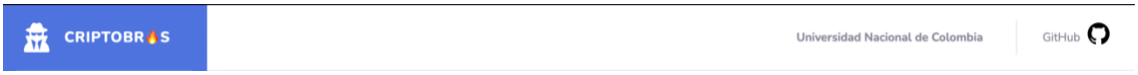
CriptoBros allows you to easily encrypt and decrypt plain text using an online application. The product includes everything necessary to have a complete presence on the Internet:
- the online encryption and decryption creation tool (the operation of which is explained in detail in this manual).
The application is intuitive and easy to use: you do not need to know cryptography,just have the texts that you want to encrypt or analyze. They adapt to any device (PCs, Tablets, and Smartphones) without the need for any extra steps.



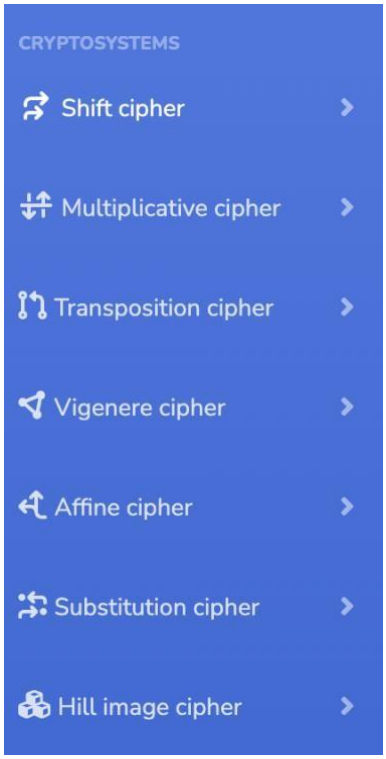
2. CriptoBros Online App Overview:

The panel of CriptoBros is divided into 4 areas:

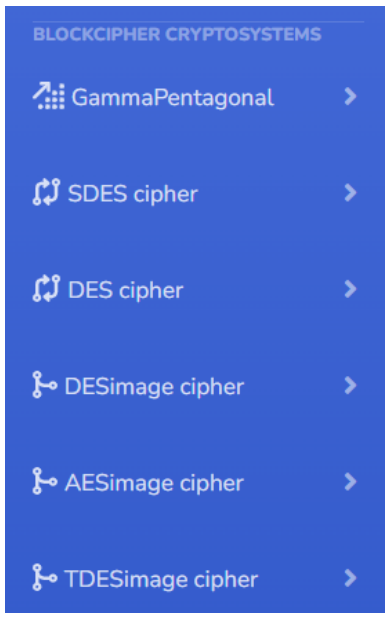
1. **Home**: We can see the name of the page **CriptoBros,** and some other features like the name of the University, Universidad Nacional de Colombia, that will carry you to the principal page of the university with just one click away, right next to it, will be found a logo of GitHub where you will be founding all the frontend code and backend code of the page.



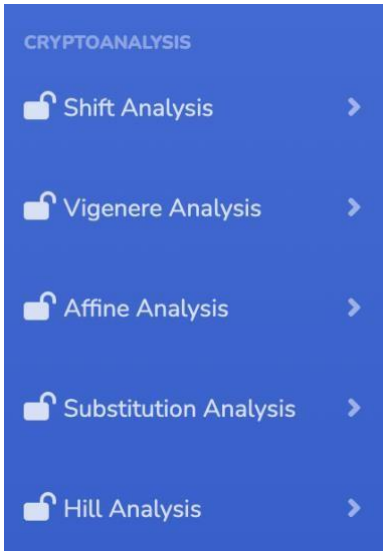
2. **Cryptosystems**: Suite of cryptographic algorithms needed to implement a particular security service, such as confidentiality. for example, we have: Shift cipher, Multiplicative cipher, Transposition cipher, Vigenère cipher, Affine cipher, and Substitution cipher.



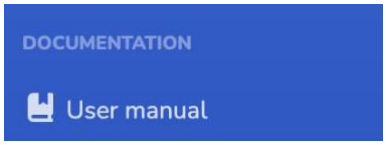
3. **Block cipher Cryptosystems:** A block cipher by itself allows encryption only of a single data block of the cipher's block length. For a variable-length message, the data must first be partitioned into separate cipher blocks. In the simplest case, known as electronic codebook (ECB) mode, a message is first to split into separate blocks of the cipher's block size (possibly extending the last block with padding bits), and then each block is encrypted and decrypted independently.



4. **Cryptoanalysis:** It is used to breach cryptographic security systems and gain access to the contents of encrypted messages, even if the cryptographic key is unknown. We can find some of them as Substitution cryptoanalysis, Shift cryptoanalysis, Vigenère cryptoanalysis, Affine cryptoanalysis, and Hill cryptoanalysis.



5. **Documentation:** This provides easily accessible information on this product and gives answers to important questions about product usage in general. aspects of functionality. The architecture of a technicalproduct.

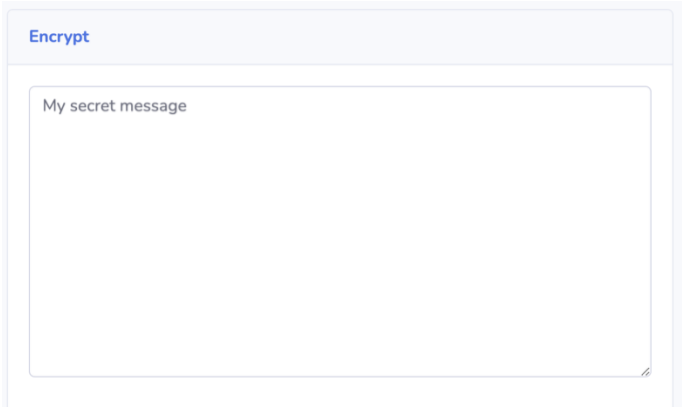


3. Crypto Systems:

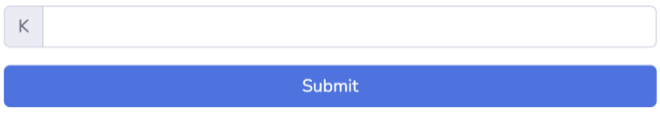
Let's take a view of each of the cryptosystems:

1. **Shift Cipher System**: The first to see it's a is a brief explanation of the type of system, like: "It is a type of substitution cipher in which each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet". Then you can find 3 boxes:

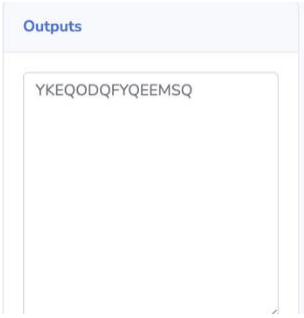
    - **Encrypt:** Where you put your top-secret message or just something you want to say in plain text.



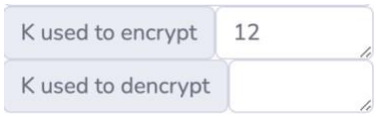
It is also needed a number key (K) between 1-26, in the box under the one you put the plain text so that it can encrypt the message, or if you don't want to give any key, it will be provided by a random one with just pressing submit.



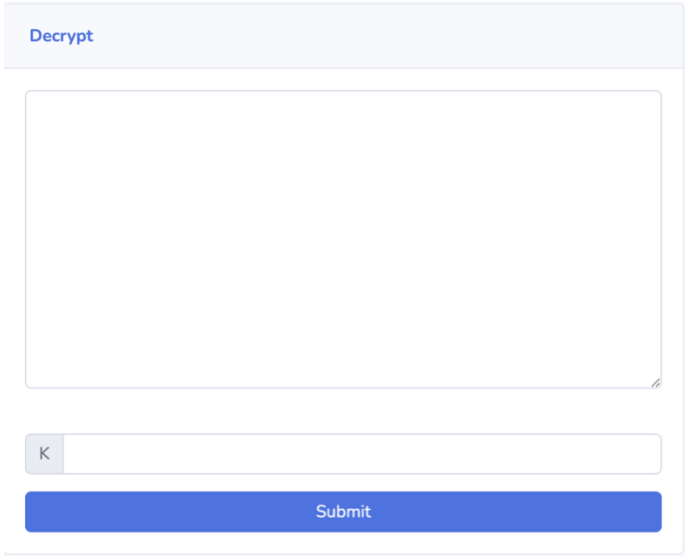
- **Outputs:** You will find the encrypted or the plain text. If you use the Encrypt box you will find the encrypted text, on the other hand, if you use the Decrypt box you will see the decrypted text, i.e., plain text.



Under that box it will be shown de key (K) used to encrypt and decrypt other it's encrypted or decrypted.

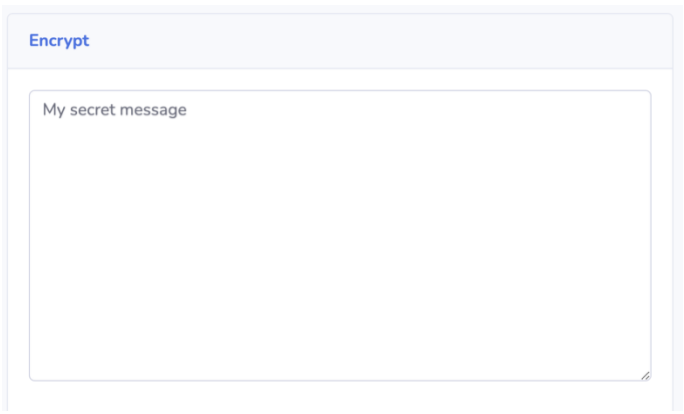


- **Decrypt**: If you have an encrypted text, use the decryption box to return to the plain text using the key (K) between 1-26 mentioned before.



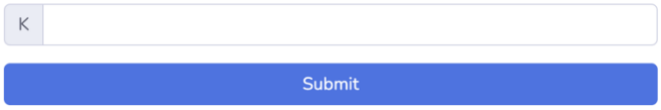
2. **Multiplicative Cipher System**: The first to see it is a brief explanation of the type of system, like: "Multiplicative Ciphers work by using the modulo operator to encrypt and decrypt messages." Then you can find 3 boxes:

- **Encrypt:** Where you put your top-secret message or just something you want to say in plain text.



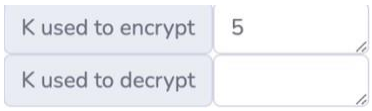
It is also needed a prime number key (K) module 26 in the box under the one you put

the plain text, so that it can encrypt the message, or if you don't want to give any key, it will be provided by a random prime number key (K) module 26 by just pressing submit.

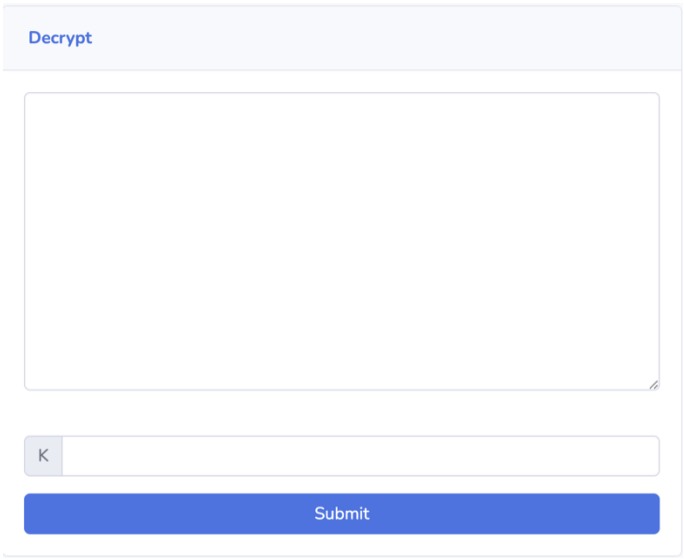


- **Outputs:** You will find the encrypted or the plain text. If you use the Encrypt box you will find the encrypted text, on the other hand, if you use the Decrypt box you will see the decrypted text, i.e., plain text.

Under that box it will be shown de key (K) used to encrypt and decrypt other it's encrypted or decrypted.

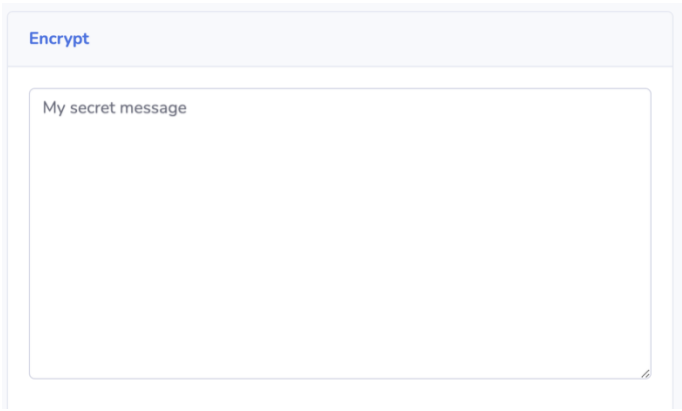


- **Decrypt**: If you have an encrypted text, use the decryption box to return to the plain text using the prime number key (K) module 26 mentioned before.

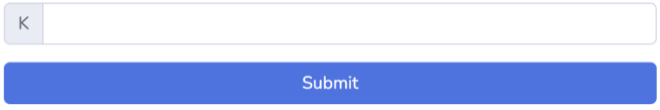


3. **Transposition Cipher System:** The first to see it's a is a brief explanation of the type of system, like: "Transposition cipher is the name given to any encryption that involves rearranging the plain text letters in a new order." Then you can find 3 boxes:

    - **Encrypt:** Where you put your top-secret message or just something you want to say in plain text.

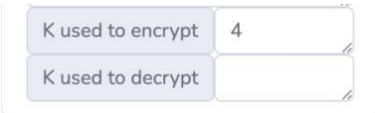


    It is also needed a number key (K) between 2 and the length of the plain text in the box under the one you put the plain text so that it can encrypt the message, or if you don't want to give any key, it will be provided by a random key (K) with just pressing submit.

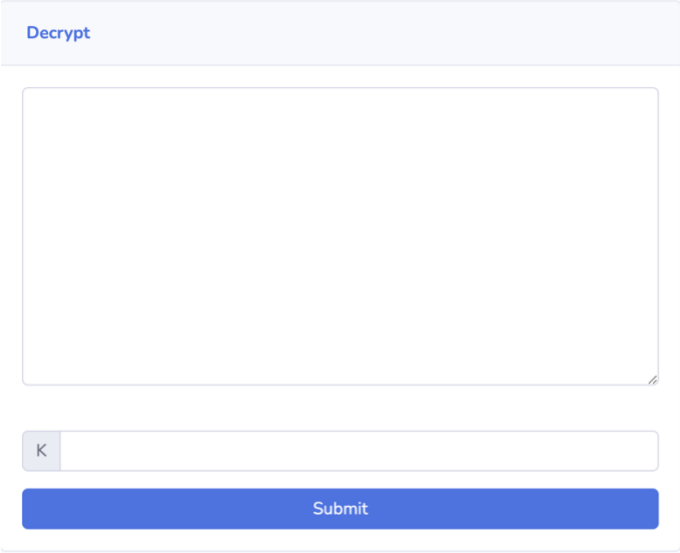


- **Outputs:** You will find the encrypted or the plain text. If you use the Encrypt box you will find the encrypted text, on the other hand, if you use the Decrypt box you will see the decrypted text, i.e., plain text.

Under that box it will be shown de key (K) used to encrypt and decrypt other it's encrypted or decrypted.



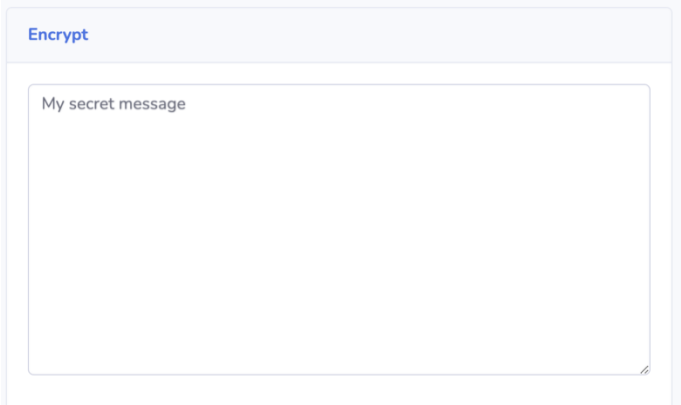
- **Decrypt**: If you have an encrypted text, use the decryption box to return to the plain text using a number key (K) between 2 and the length of the plain text mentioned before.



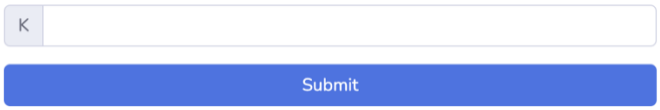
4. **Vigenère Cipher System:** The first to see it is a brief explanation of the type of system, like: "Vigenère Cipher is a method of encrypting alphabetic text. It uses a simple form of polyalphabetic substitution. A polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets." Then you can find 3 boxes:

- **Encrypt:** Where you put your top-secret message or just something you want to

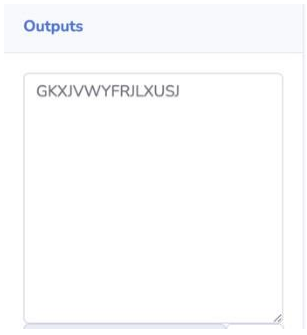
say in plain text.



It is also needed a string key (K), which can be a string with a length between 1 and the length of the plain text, in the box under the one you put the plain text, so that it can encrypt the message, or if you don't want to give any key, it will be provided by a random key (K) with the specifications mentioned before by just pressing submit.



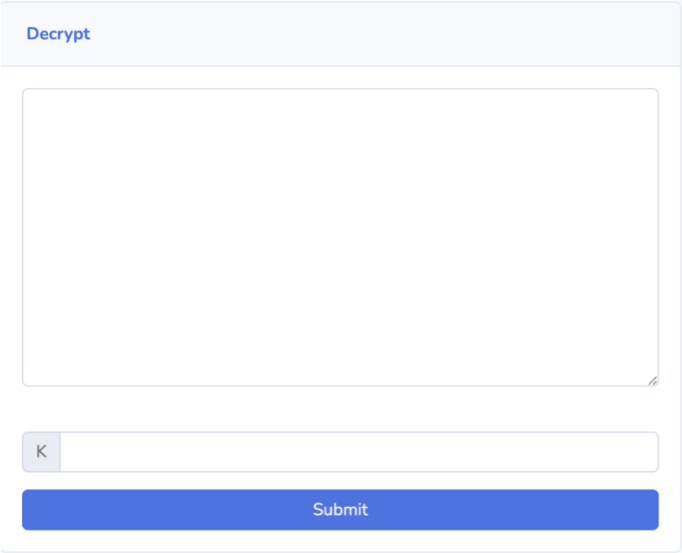
- **Outputs:** You will find the encrypted or the plain text. If you use the Encrypt box you will find the encrypted text, on the other hand, if you use the Decrypt box you will see the decrypted text, i.e., plain text.



Under that box it will be shown de key (K) used to encrypt and decrypt other it's encrypted or decrypted.

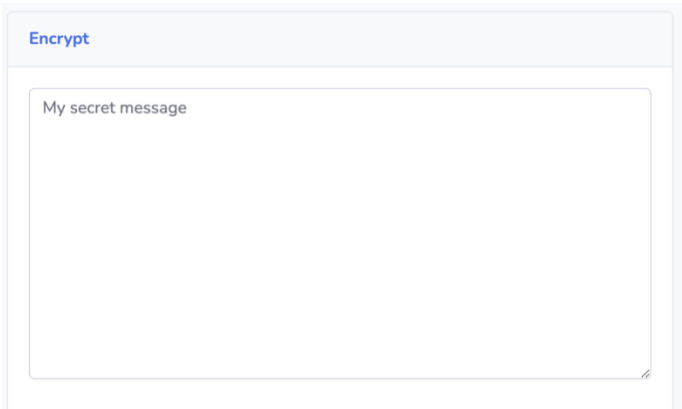
- **Decrypt**: If you have an encrypted text, use the decryption box to return to the

plain text the string key (K) mentioned before.

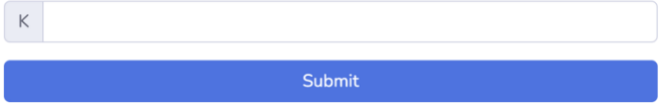


5. **Affine Cipher System:** The first to see it is a brief explanation of the type of system, like: "The affine cipher is a type of monoalphabetic substitution cipher, where each letter in an alphabet is mapped to its numeric equivalent, encrypted using a simple mathematical function, and converted back to a letter." Then you can find 3 boxes:

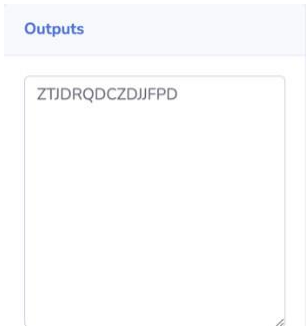
   - **Encrypt:** Where you put your top-secret message or just something you want to say in plain text.



It is also needed a key (K), which can be a tuple that is relative numbers mod 26, in thebox under the one you put the plain text, so that it can encrypt the message, or if you don't want to give any key, it will be provided by a random key (K) with the specifications mentioned before by just pressing submit.

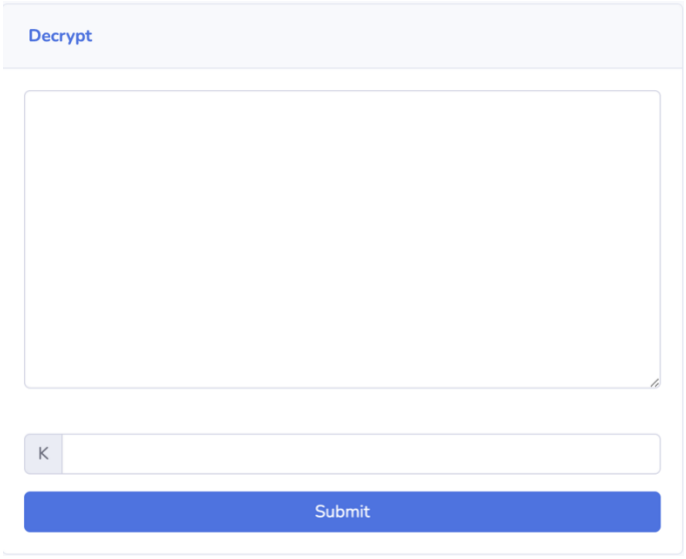


- **Outputs:** You will find the encrypted or the plain text. If you use the Encrypt box you will find the encrypted text, on the other hand, if you use the Decrypt box you will see the decrypted text, i.e., plain text.

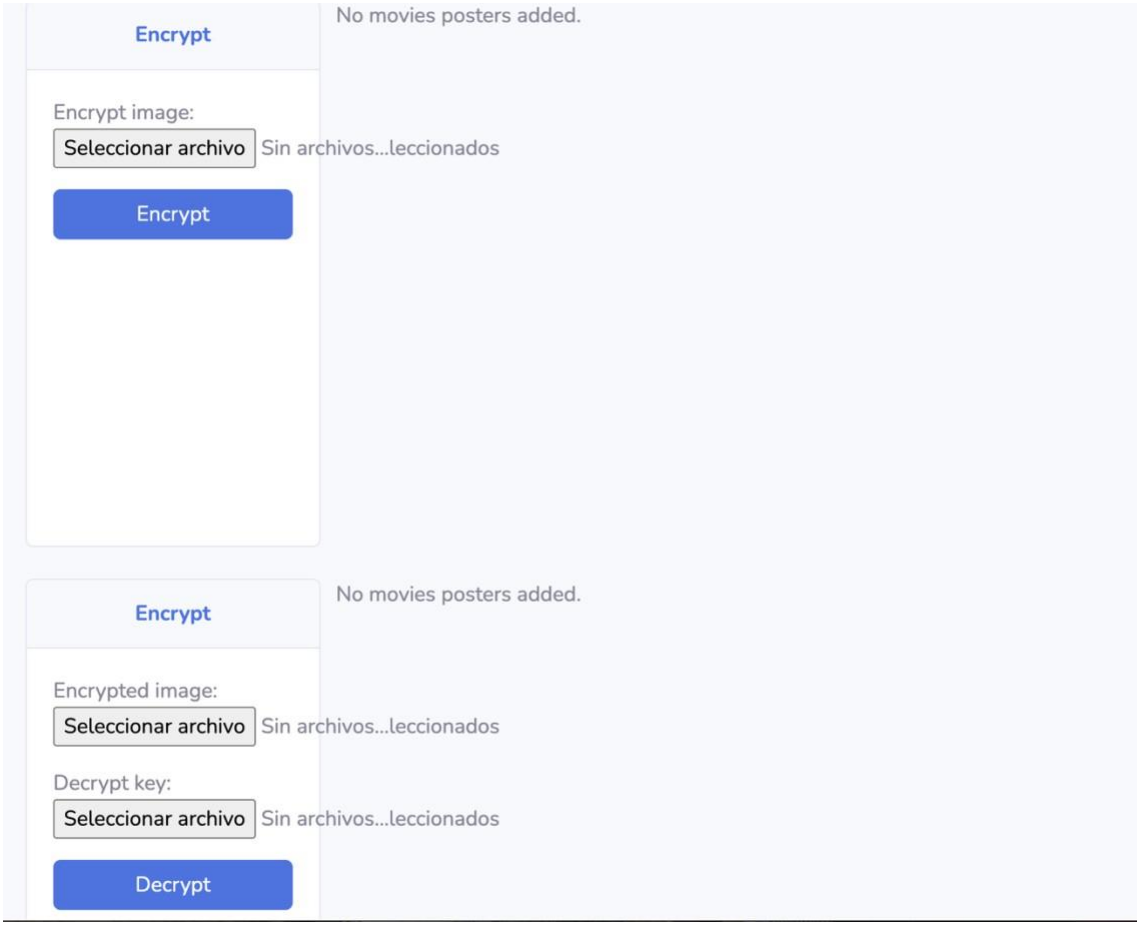


Under that box it will be shown de key (K) used to encrypt and decrypt other it's encrypted or decrypted.

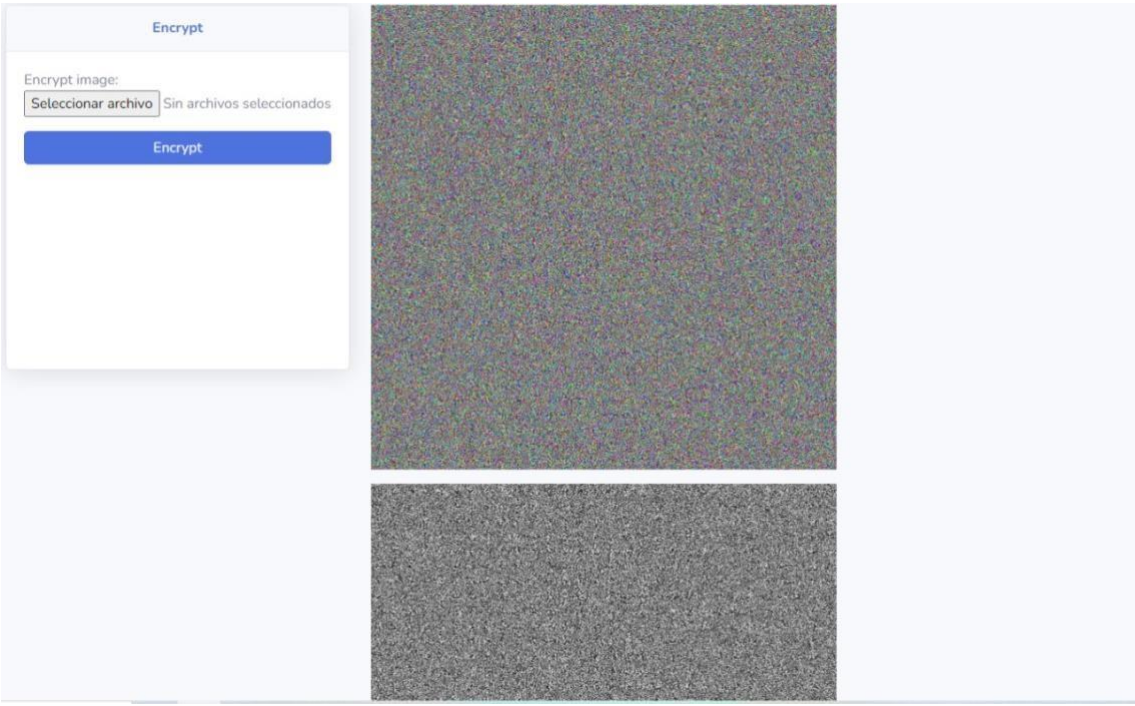
- **Decrypt**: If you have an encrypted text, use the decryption box to return to the plain text using the tuple that are relative numbers mod 26 key (K) mentioned before.



6. **Hill Image System:** The Hill cipher algorithm is a symmetric key algorithm with several advantages in data encryption. But, the inverse of the key matrix used for encrypting the plaintext does not always exist. Then if the key matrix is not invertible, encrypted text cannot be decrypted. In the Involutory matrix generation method, the key matrix used for the encryption is itself invertible.

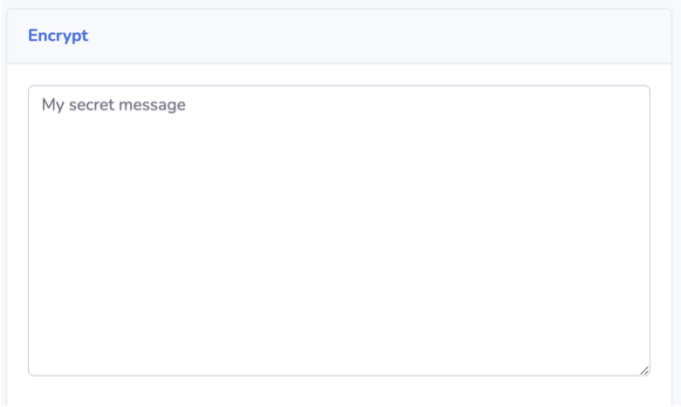


Implemented Hill Cipher technique one is a cover image which acts as a key image which is shared by both sender and receiver and other is Informative image. As the first step, we add a cover image and informative image to obtain the resultant image. Uploading an image

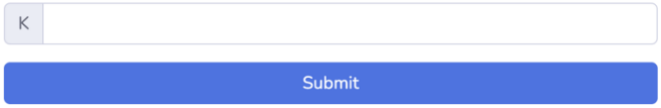


7. **Substitution Cipher System:** The first to see it is a brief explanation of the type of system, like: "Substitution cipher is a method of encrypting in which units of plaintext are replaced with the ciphertext, in a defined manner, with the help of a key; the "units" may be single letters (the most common), pairs of letters, triplets of letters, mixtures of the above, and so forth." Then you can find 3 boxes:

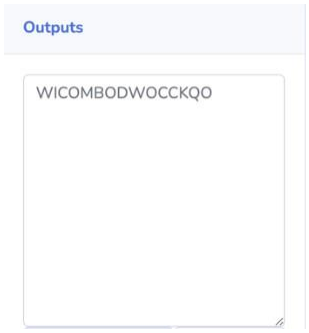
- **Encrypt:** Where you put your top-secret message or just something you want to say in plain text.



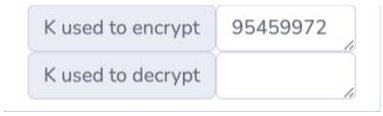
It is also needed a number key (K, so that it can encrypt the message, or if you don't want to give any key, it will be provided by a random key (K) just pressing submit.



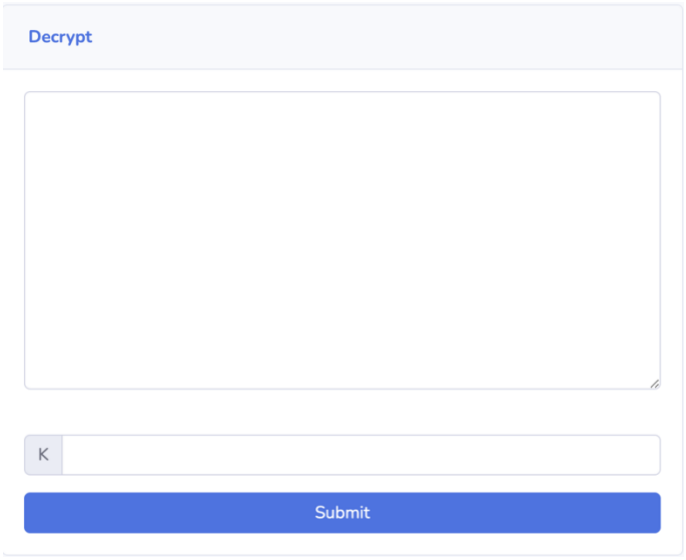
- **Outputs:** You will find the encrypted or the plain text. If you use the Encrypt box you will find the encrypted text, on the other hand, if you use the Decrypt box you will see the decrypted text, i.e., plain text.



Under that box it will be shown de key (K) used to encrypt and decrypt other it's encrypted or decrypted.



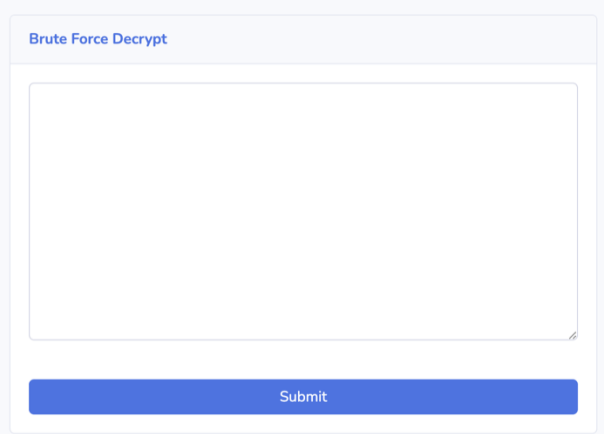
- **Decrypt**: If you have an encrypted text, use the decryption box to return to the plain text using a key (K) mentioned before.



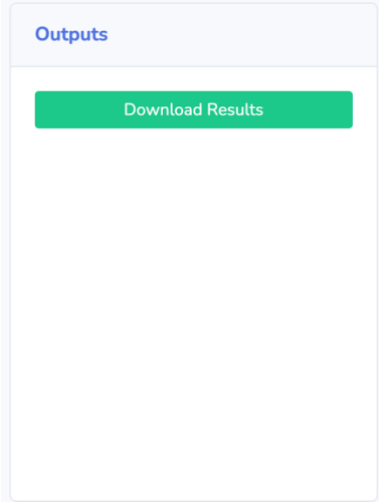
4. Crypto Analysis:

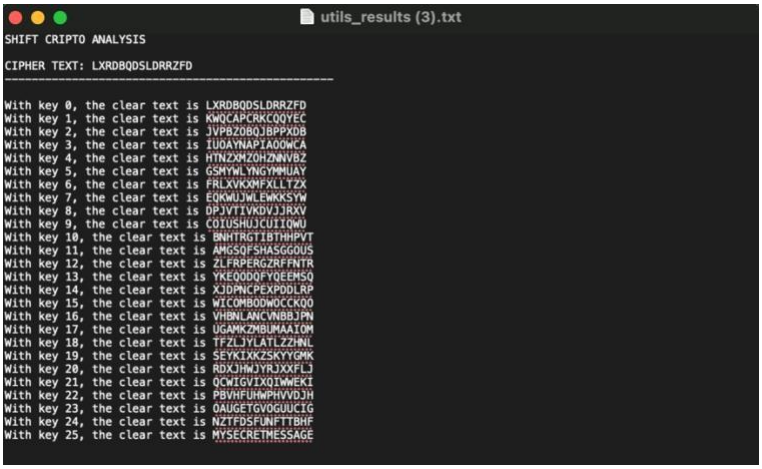
Cryptanalysis is the process of studying cryptographic systems to look for weaknesses or leaks of information. Let's see how we can break in.

1. **Shift Cryptanalysis:** With brute force, we try every displacement of the cipher to find onethat makes sense, we go through the 26 keys of Z_26.



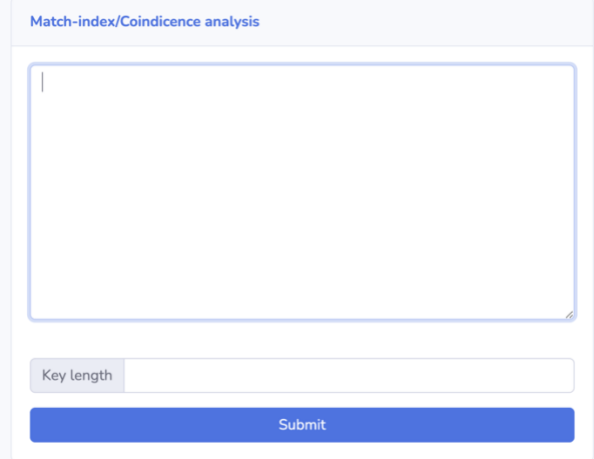
In the box shown above, we write de encrypted message we want to decrypt, then by pressing submit we get a result we will be downloading, giving us a .txt file with decrypted code.



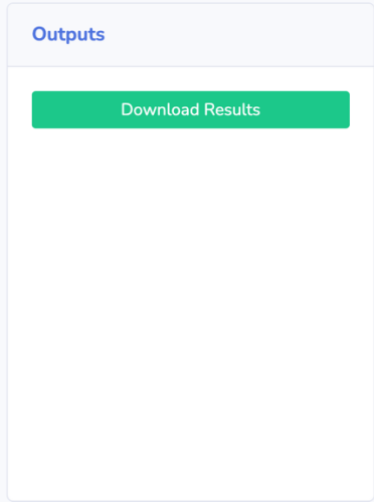


As you can see, the decrypted code was in key 25, as it says, my secret message.

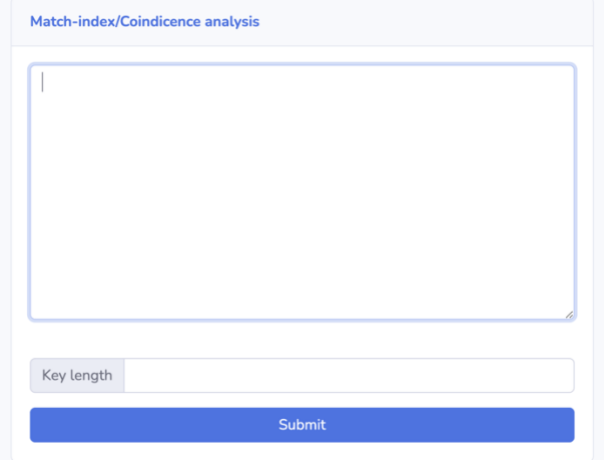
2. **Vigenère Cryptanalysis:** Using the match index method, the ciphered text is attacked and the results are obtained as an output. The user must provide the key's length and press Submit.



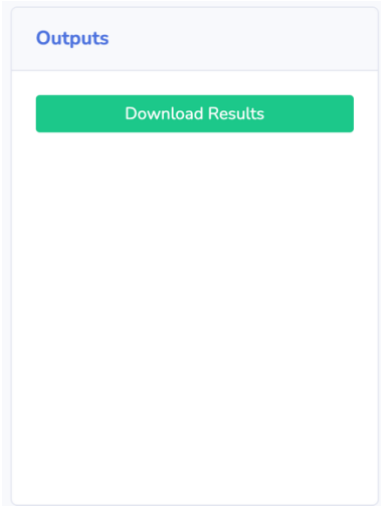
In the box shown above, we write de encrypted message we want to decrypt, by pressing submit we get a result we will be downloading, giving us a .txt file with the possible key and the decrypted code.



3. **Affine Cryptoanalysis:** With brute force, we try every possible combination of keys to findone that makes sense. We go through the 312 possible keys. And that is because there are finite combinations of a and b.



In the box shown above, we write de encrypted message we want to decrypt, by pressingsubmit we get the result, and will be downloaded, giving a .txt file

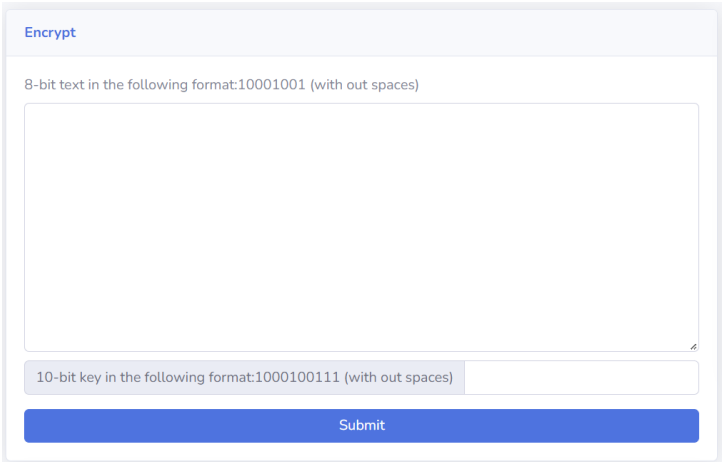



```
Assuming the keys are 17 and 0, the text is DPJVTIVKDVJJRXV
Assuming the keys are 17 and 1, the text is GSMYWLYNGYMMUAY
Assuming the keys are 17 and 2, the text is JVPBZOBQJBPPXDB
Assuming the keys are 17 and 3, the text is MYSECRETMESSAGE
Assuming the keys are 17 and 4, the text is PBVHFUHWPHVVDJH
Assuming the keys are 17 and 5, the text is SEYKIXKZSKYYGMK
Assuming the keys are 17 and 6, the text is VHBNLANCVNBBJPN
Assuming the keys are 17 and 7, the text is YKEQODQFYQEEMSQ
```

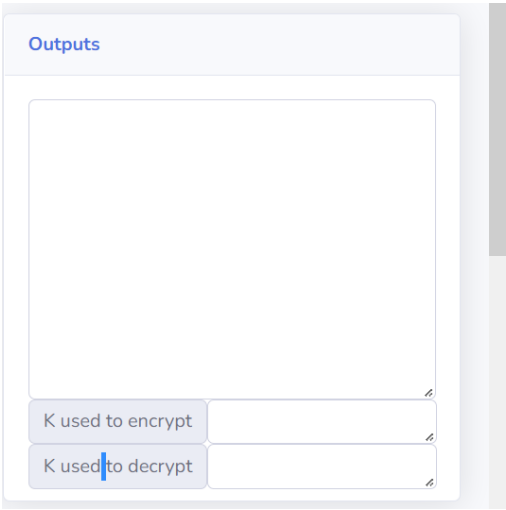
5. Block cipher Cryptosystems:

A block cipher uses a symmetric key and algorithm to encrypt and decrypt a block of data. A block cipher requires an initialization vector (IV) that is added to the input plaintext to increase the key space of the cipher and make it more difficult to use brute force to break the key.

1. **SDES Cipher**: It is a simple version of the DES Algorithm. It is similar to the DES algorithm but is a smaller algorithm and has fewer parameters than DES. It was made for educational purposes so that understanding DES would become simpler. It is a block cipher that takes a block of plain text and converts it into ciphertext. It takes a block of 8 bit:
    - **Encrypt:** Where you put your top-secret message or just something you want to say in plain text with a 10-bit key in the following format:1000100111 (without spaces)

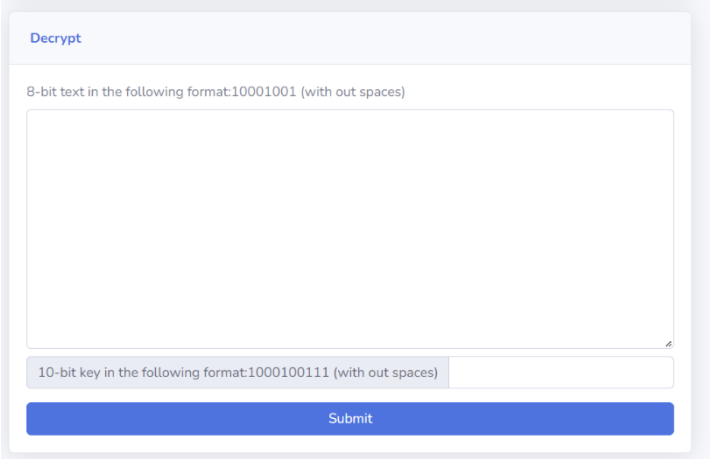


    - **Outputs:** You will find the encrypted or the plain text with 8-bit text in the following format:10001001. If you use the Encrypt box you will find the encrypted text, on the other hand, if you use the Decrypt box you will see the decrypted text, i.e., 8-bit text in the following format:10001001.



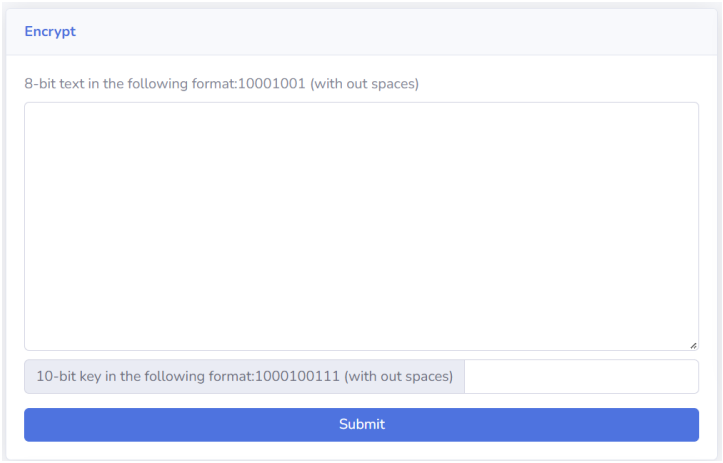
Under that box it will be shown de key (K) used to encrypt and decrypt other it's encrypted or decrypted.

- **Decrypt**: If you have an encrypted text, use the decryption box to return to the plain text using a key (K) mentioned before.

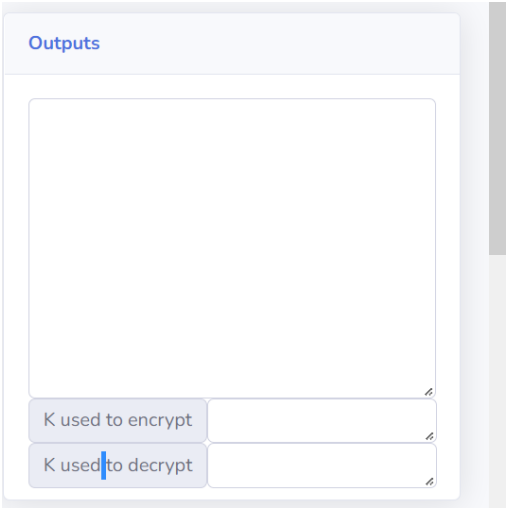


2. **DES Cipher:** It is a symmetric-key algorithm for the encryption of digital data. Although its short key length of 56 bits makes it too insecure for modern applications, it has been highly influential in the advancement of cryptography.

▪ **Encrypt:** Where you put your top-secret message or just something you want to say in plain text with a 10-bit key in the following format:1000100111 (without spaces)

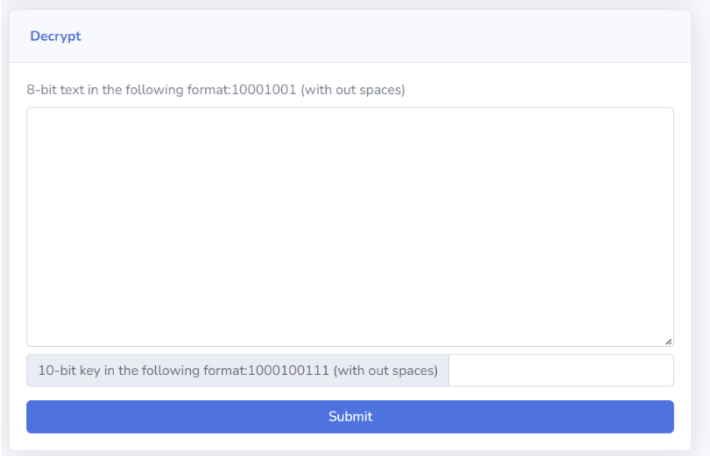


▪ **Outputs:** You will find the encrypted or the plain text with 8-bit text in the following format:10001001. If you use the Encrypt box you will find the encrypted text, on the other hand, if you use the Decrypt box you will see the decrypted text, i.e., 8-bit text in the following format:10001001.



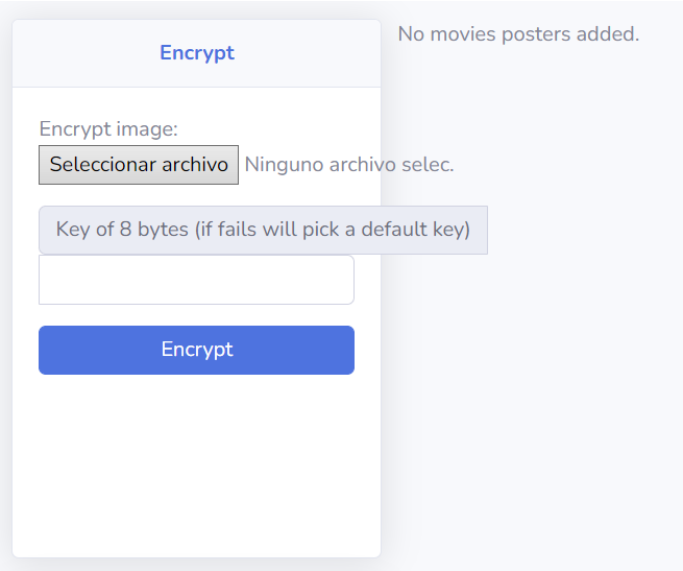
Under that box it will be shown de key (K) used to encrypt and decrypt other it's encrypted or decrypted.

- **Decrypt**: If you have an encrypted text, use the decryption box to return to the plain text using a key (K) mentioned before.

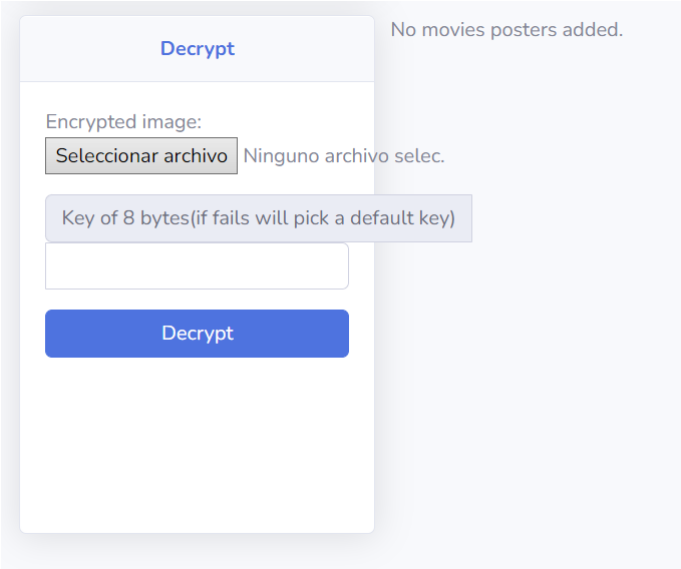


3. **DESimage Cipher:** DES is considered a symmetric key block cipher algorithm. The implementation structure of DES ithe s Fiestel cipher. InFiestel structure as 16 rounds of steps are used.64 bit block size is used for DES structure .It has 64 bit key length, but DES utilizes only 56 bit key. Remaining 8 bits is used later but not used for encryption.

- **Encrypt:** In the encryption method we considered two inputs, one is encryption secret key and another one is original color image. Image file can be reshaped or divided pixel block of original image and express DES encryption process and defining the key for encryption that is secret key. By using DES algorithm procedure finally original image is encrypted with security, this is encrypted image



- **Outputs:** An encrypted image and decrypted image.
- **Decrypt**: It is a reverse process of Image encryption. In this method encrypted image is considered as input for DES algorithm structure for decryption. Encrypted image is divided again into pixel blocks that are same as DES algorithm block length. Primarily function blocks of 64-bit size are entered. Then same secrecy key that is decryption key used for process of decryption which one is used for encryption. Here we follow a reverse ordered procedure of encryption.



4. **AESimage Cipher:** The Advanced Encryption Standard (AES) is a symmetric block cipher chosen by the U.S. government to protect classified information. AES is implemented in software and hardware throughout the world to encrypt sensitive data.

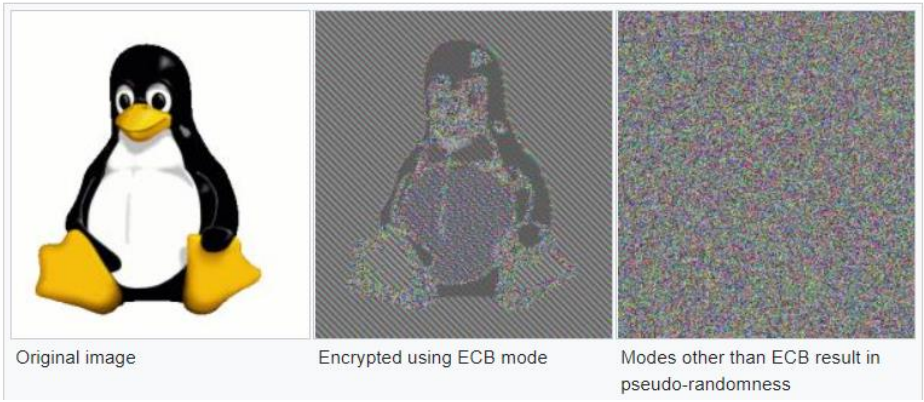
   Different cipher modes mask patterns by cascading outputs from the cipher block or other globally deterministic variables into the subsequent cipher block. The inputs of the listed modes are summarized in the following table:

   We are going to use just five of them: **ECB ,CBC, CFB, OFB, CTR.**

Summary of modes

Mode		Formulas	Ciphertext
Electronic codebook	(ECB)	$Y_i = F(PlainText_i, Key)$	Y_i
Cipher block chaining	(CBC)	$Y_i = PlainText_i$ XOR $Ciphertext_{i-1}$	$F(Y, Key)$; $Ciphertext_0 = IV$
Propagating CBC	(PCBC)	$Y_i = PlainText_i$ XOR ($Ciphertext_{i-1}$ XOR $PlainText_{i-1}$)	$F(Y, Key)$; $Ciphertext_0 = IV$
Cipher feedback	(CFB)	$Y_i = Ciphertext_{i-1}$	Plaintext XOR $F(Y, Key)$; $Ciphertext_0 = IV$
Output feedback	(OFB)	$Y_i = F(Y_{i-1}, Key)$; $Y_0 = F(IV, Key)$	Plaintext XOR Y_i
Counter	(CTR)	$Y_i = F(IV + g(i), Key)$; IV = token()	Plaintext XOR Y_i

- **Electronic codebook (ECB):** The disadvantage of this method is a lack of diffusion. Because ECB encrypts identical plaintext blocks into identical ciphertext blocks, it does not hide data patterns well. ECB is not recommended for use in cryptographic protocols.

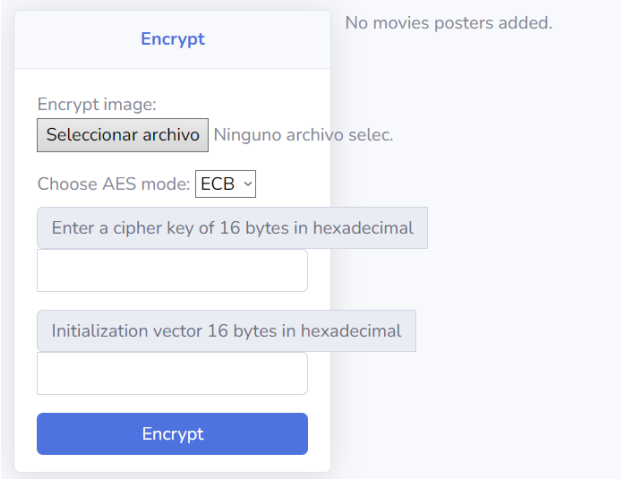


Original image | Encrypted using ECB mode | Modes other than ECB result in pseudo-randomness

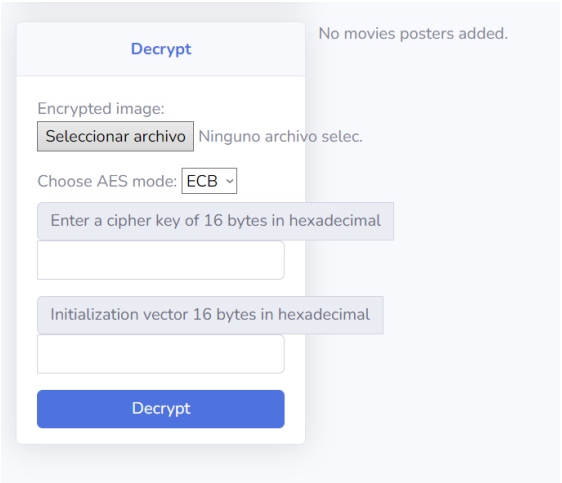
- **Cipher block chaining (CBC):** cipher block chaining (CBC) mode of operation in 1976. In CBC mode, each block of plaintext is XORed with the previous ciphertext block before being encrypted. This way, each ciphertext block depends on all plaintext blocks processed up to that point. To make each message unique, an initialization vector must be used in the first block.
- **Cipher Feedback (CFB):** The cipher feedback (CFB) mode, in its simplest form uses the entire output of the block cipher. In this variation, it is very similar to CBC, makes a block cipher into a self-synchronizing stream cipher. CFB decryption in this variation is almost identical to CBC encryption performed in reverse.
- **Output feedback (OFB):** The output feedback (OFB) mode makes a block cipher into a synchronous stream cipher. It generates keystream blocks, which are then XORed with the plaintext blocks to get the ciphertext. Just as with

other stream ciphers, flipping a bit in the ciphertext produces a flipped bit in the plaintext at the same location. This property allows many error-correcting codes to function normally even when applied before encryption.

- **Counter (CTR):** CTR mode has similar characteristics to OFB, but also allows a random-access property during decryption. CTR mode is well suited to operate on a multi-processor machine, where blocks can be encrypted in parallel. Furthermore, it does not suffer from the short-cycle problem that can affect OFB.
- **Encrypt:** In the encryption method we considered two inputs, one is encryption secret key and another one is original color image. Image file can be reshaped or divided pixel block of original image and express AES encryption process and defining the key for encryption that is secret key. By using AES algorithm and a mode procedure finally original image is encrypted with security.

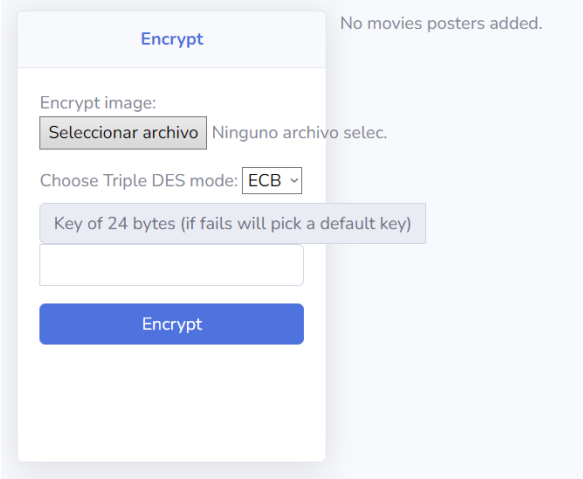


- **Decrypt:** It is a reverse process of Image encryption. In this method encrypted image is considered as input for AES algorithm structure for decryption. Encrypted image is divided again into pixel blocks that are same as AES algorithm block length. Then same secrecy key that is decryption key used for process of decryption which one is used for encryption. Here we follow a reverse ordered procedure of encryption.

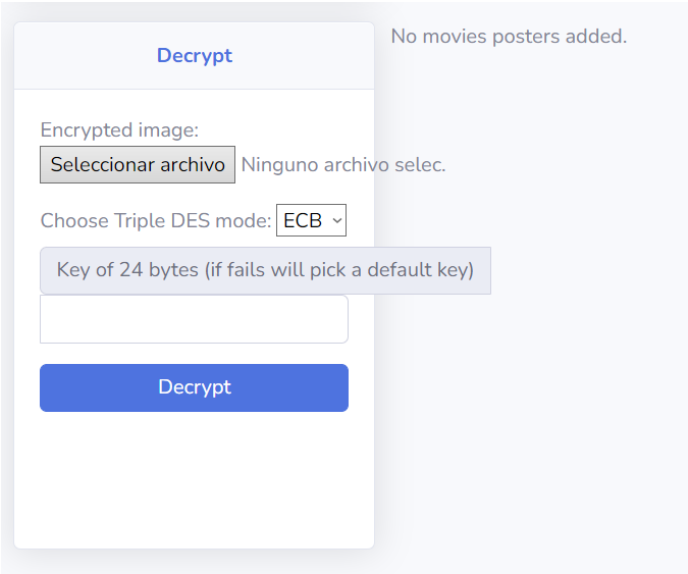


5. **TDESimage cipher:** It is a symmetric-key block cipher, which applies the DES cipher algorithm three times to each data block. The Data Encryption Standard's (DES) 56-bit key is no longer considered adequate in the face of modern cryptanalytic techniques and supercomputing power. A CVE released in 2016, CVE-2016-2183 disclosed a major security vulnerability in DES and 3DES encryption algorithms. As AESimgae cipher we'll be using the same modes.

   - **Encrypt**: Triple-DES encryption uses a triple-length DATA key comprised of three 8-byte DES keys to encipher 8 bytes of data using this method: Encipher the data using the first key Decipher the result using the second key Encipher the second result using the third key The procedure is reversed to decipher data that has been triple-DES enciphered: Decipher the data using the third key Encipher the result using the second key Decipher the second result using the first key.



   - **Decrypt:** It is a reverse process of Image encryption. In this method encrypted image is considered as input for 3DES algorithm structure for decryption. Encrypted image is divided again into pixel blocks that are same as 3DES algorithm block length. Then same secrecy key that is decryption key used for process of decryption which one is used for encryption. Here we follow a reverse ordered procedure of encryption.



For a given cryptographic system, the minimum length of a ciphertext to be able to be cryptanalyzed can be found using $\frac{log_2|K|}{log_2|P|-H_L}$, where $|K|$ the size of our key space, $|P|$ the size of our alphabet, and H_L the entropy of a given language. In this case, we want to do the analysis for the Vigenère cipher, for the English language, so our $|P| = 26$, $H_L \approx 1.5$ and our $|K| = 26^n$, for a given key length n.
Then:

$$\begin{aligned}\frac{log_2|K|}{log_2|P| - H_L} &= \frac{log_2 26^n}{log_2 26 - 1{,}5} \\ &= \frac{n log_2 26}{log_2 26 - 1{,}5} \\ &= \frac{n * 4{,}7}{4{,}7 - 1{,}5} \\ &= \frac{n * 4{,}7}{3{,}2} \\ &= \frac{n * 4{,}7}{3{,}2} \\ &\approx n * 1{,}47\end{aligned}$$

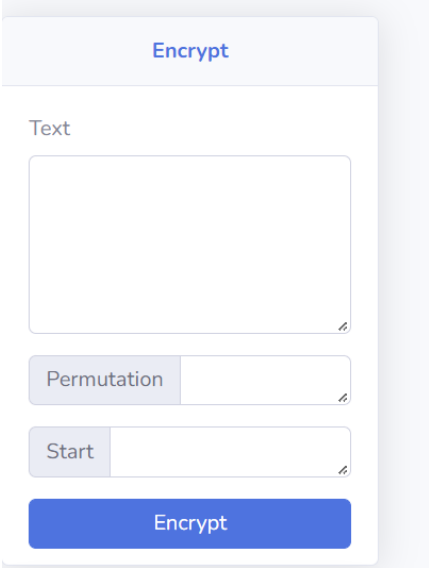
Therefore, for a key of length n, we need a ciphertext $1.47 * n \approx 1.5 * n$. For example, for a key of length $n = 3$, a ciphertext of minimum length $n = 1.5 * 3 = 4.5 \approx 5$ would be needed, or for a key of length $n = 6$, then length 9. However, this is just a theoretical limit, for an opponent with unlimitedresources. In general, and as could be seen with our tests, a larger key is required to properly perform cryptanalysis.

6. **Gamma-Pentagonal Cipher:** The Gamma-Pentagonal cryptographic system has the property of probabilistic security since it is associated with a difficult problem of number theory. More precisely, the problem we are dealing with consists in determining the number of ways in which an integer can be written as the sum of three polygonal numbers. It is recalled that polygonal numbers are those that can be described as a polygonal arrangement of points, for example, triangular numbers, squares, pentagonal, etc.
    - **Encrypt**: The difficult problem is to determine in how many ways a positive integer can be written as a sum of at least three square numbers. The above problem can be seen as finding how many admissible trajectories such as the ones we will illustrate later, connect the origin with a point in the usual plane. Then the point is related to a letter. The set-up process is as follows:

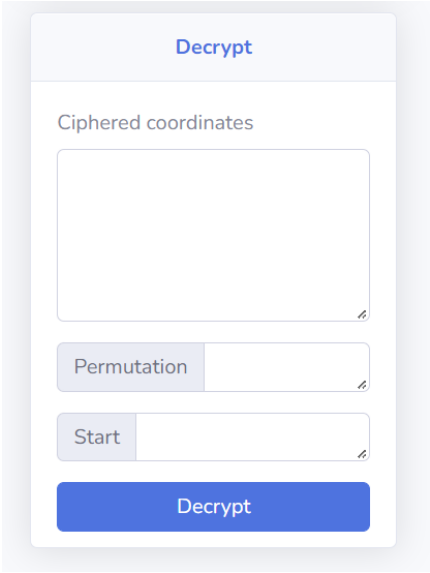
      - The user must provide the `origin` coordinates, a `permutation` and the `clear text`. The origin and the permutation must remain secret.
      - A matrix of 10 columns is created, each of which contains the complete alphabet (26 letters). Then the order of each column is shifted, the magnitude of the displacement is determined by the respective number in the initial permutation.
      - At the same time, the following equivalence classes are created:

        $$\bar{x} := [(a, b) : a + b = x]$$

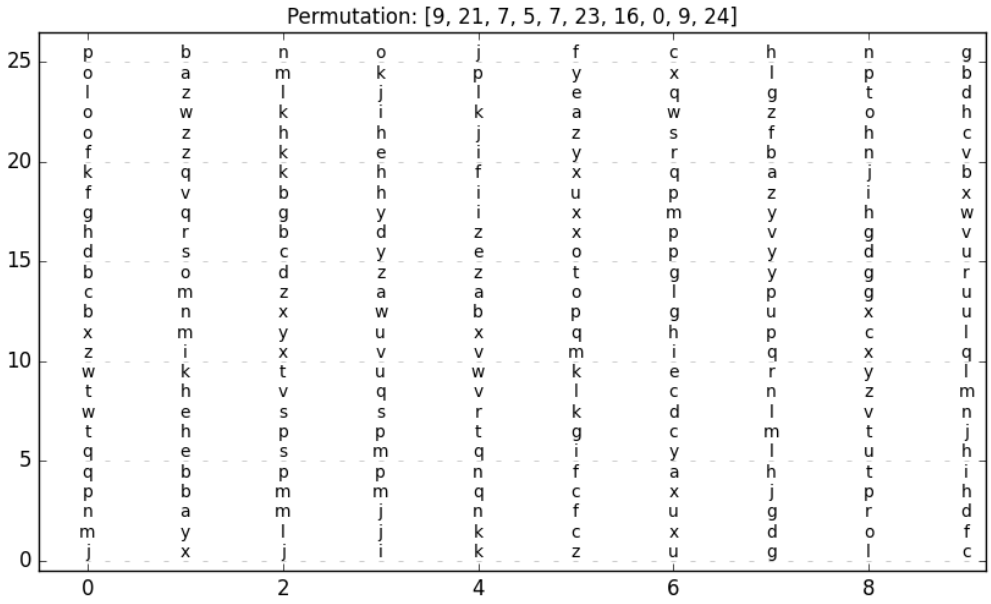
        Then, $d(\bar{x})$ is defined as the sum of the incoming arrows for each point in the class.
      - Finally, the value of each $a_{i,j}$ in the matrix is shifted by $d(\overline{(i, j)})$ units.



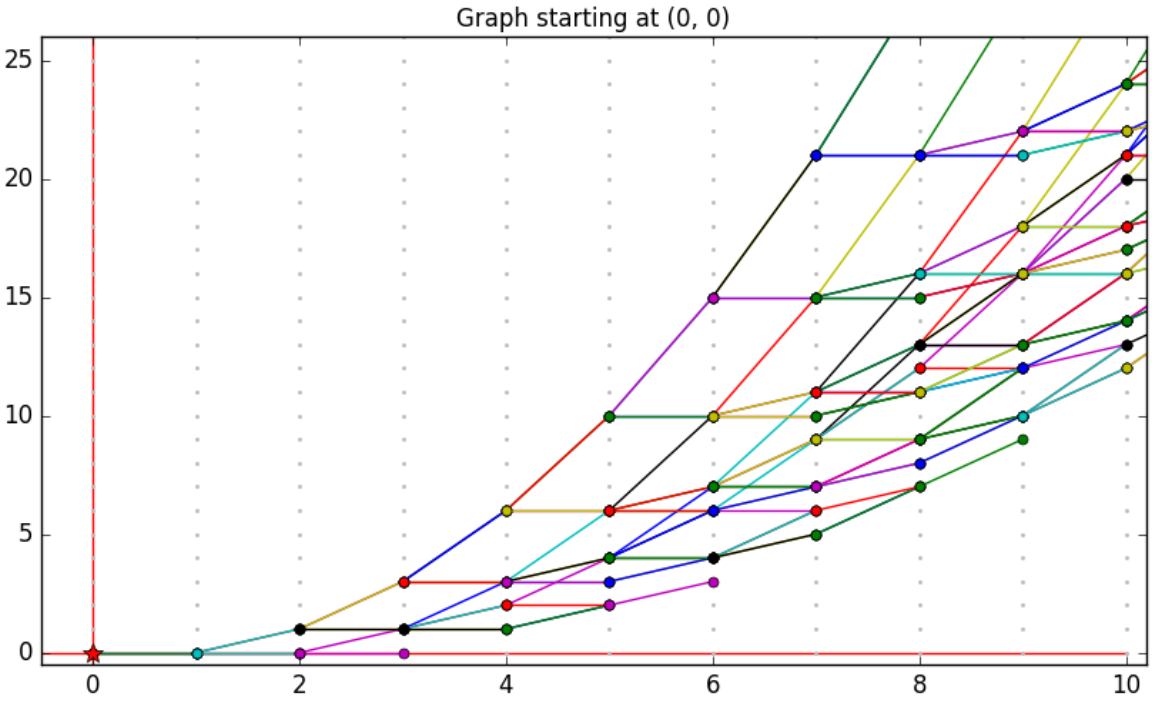
- **Decrypt:** The user must provide the origin coordenates, the permutation and the ciphered coordenates. After doing the set-up, the coordinates are translated into letters, returning the original clear text. Since the keys in each alphabet can be used with the same probability when constructing ciphertexts then we can infer that the gamma-pentagonal system is unbreakable.



As an example:

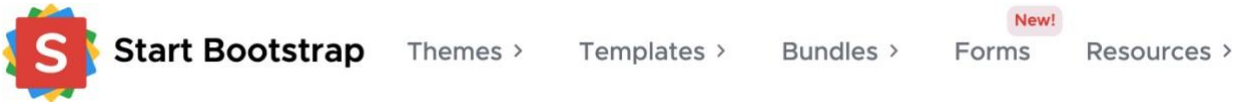


A graph generated with (0,0) as the origin point is shown bellow:



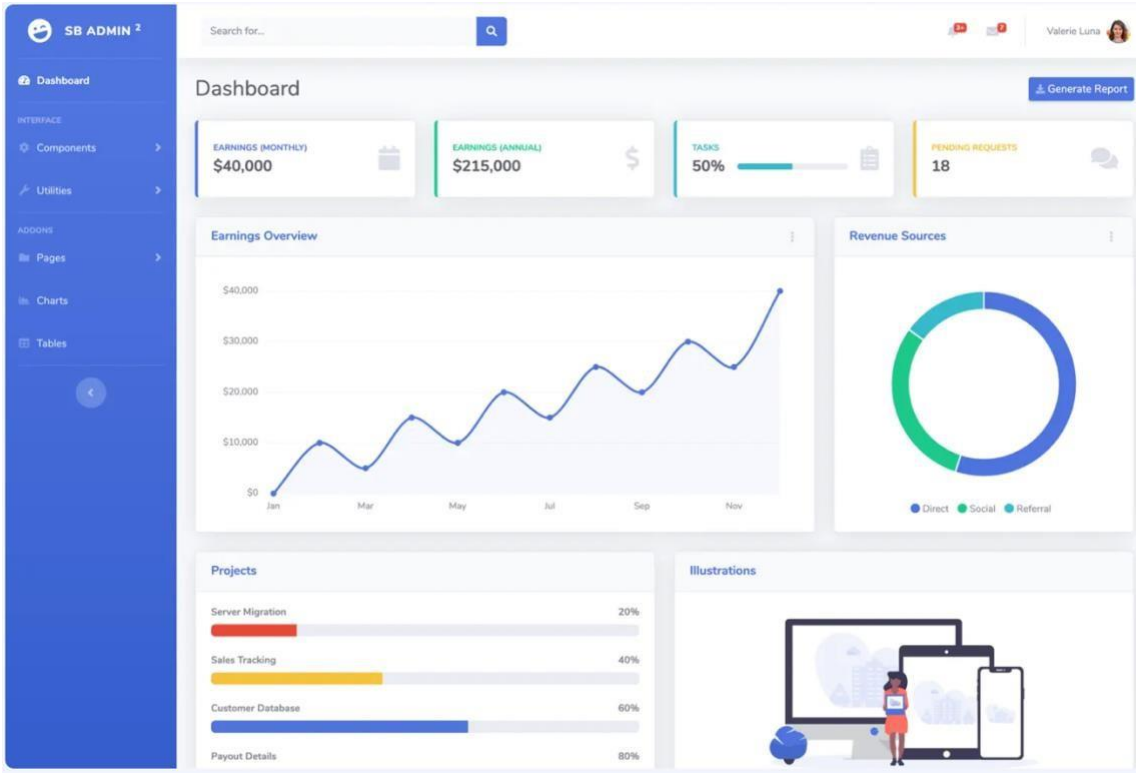
6. Page Design:

The page Design was inspired by a free open-source start Bootstrap theme.

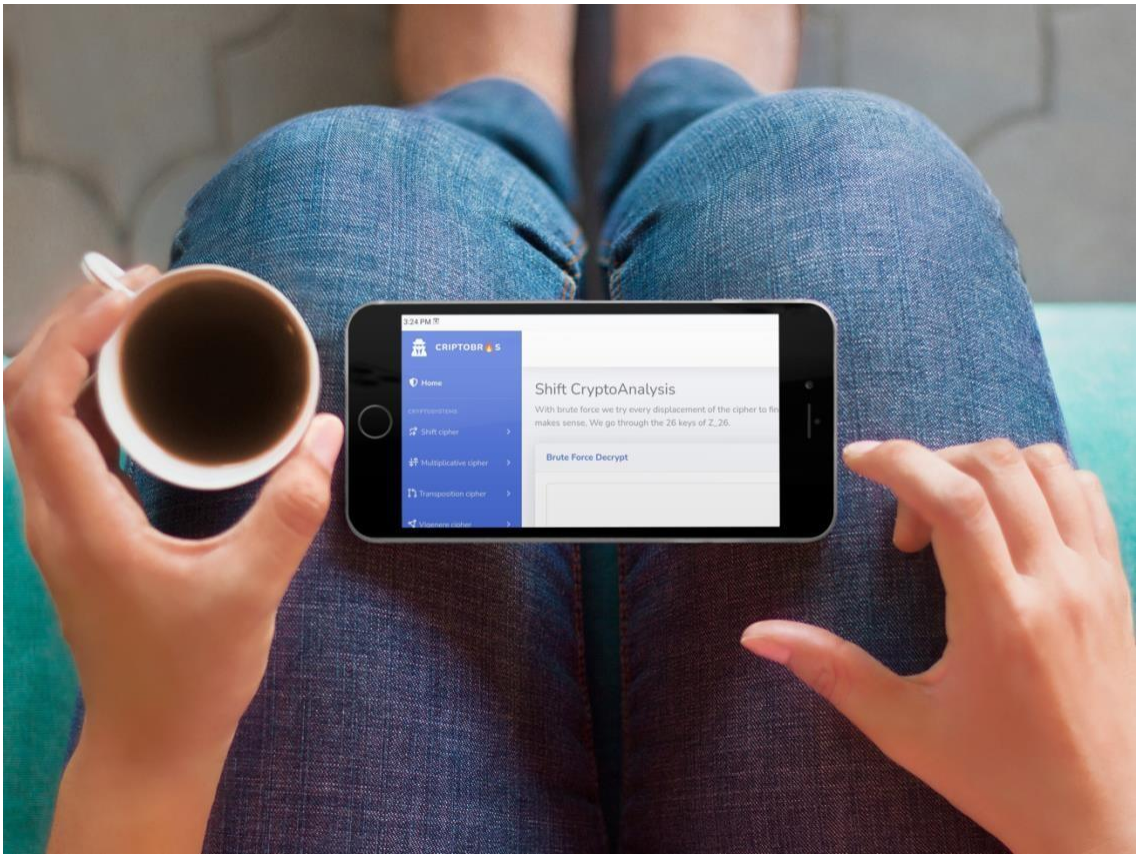


- Templatete:

We used a template called SB Admin 2 is a free, open-source, Bootstrap 4-based admin theme perfect for quickly creating dashboards and web applications. Its modern design style with subtle shadows and a card-based layout could be described as flat material and is inspired by the principles of material design along with a simple, attractive color system.



We got some features like Features: A modern, material design-inspired layout, a focus on utility, classes to minimize CSS bloat, custom card, and button components, and custom utility classes forextended functionality.



- Color:

There are many ways to create a website that stands out on the Internet, and one of them is to choose a unique color scheme. Whether you're designing a blog, an online store, or a personal page, the color selection for a website is one of the first things visitors will notice, and you're sure to make a lasting impression. We used kind a color bust:

Using a gradient background on your web page can set the tone for a wide-gamut color palette. In the case of Foodie Marketing, a pop of pink and orange hues inspires a cool contrast of teal, blue, and lime green. The white logo, text, and buttons add a professional touch to the page'svibrant vibe.