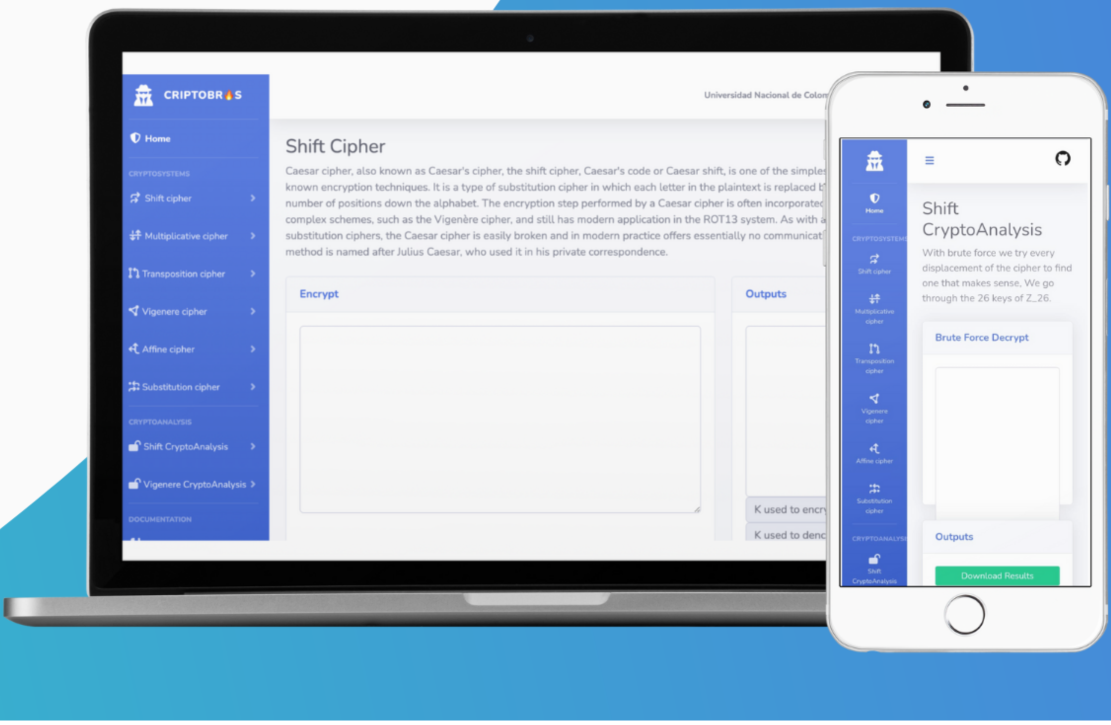
CRIPTOBROS

CRIPTOBROS

USER MANUAL



Shift Cipher

Caesar cipher, also known as Caesar's cipher, the shift cipher, Caesar's code or Caesar shift, is one of the simples known encryption techniques. It is a type of substitution cipher in which each letter in the plaintext is replaced b number of positions down the alphabet. The encryption step performed by a Caesar cipher is often incorporated complex schemes, such as the Vigenère cipher, and still has modern application in the ROT13 system. As with a substitution ciphers, the Caesar cipher is easily broken and in modern practice offers essentially no communicat method is named after Julius Caesar, who used it in his private correspondence.

Shift CryptoAnalysis

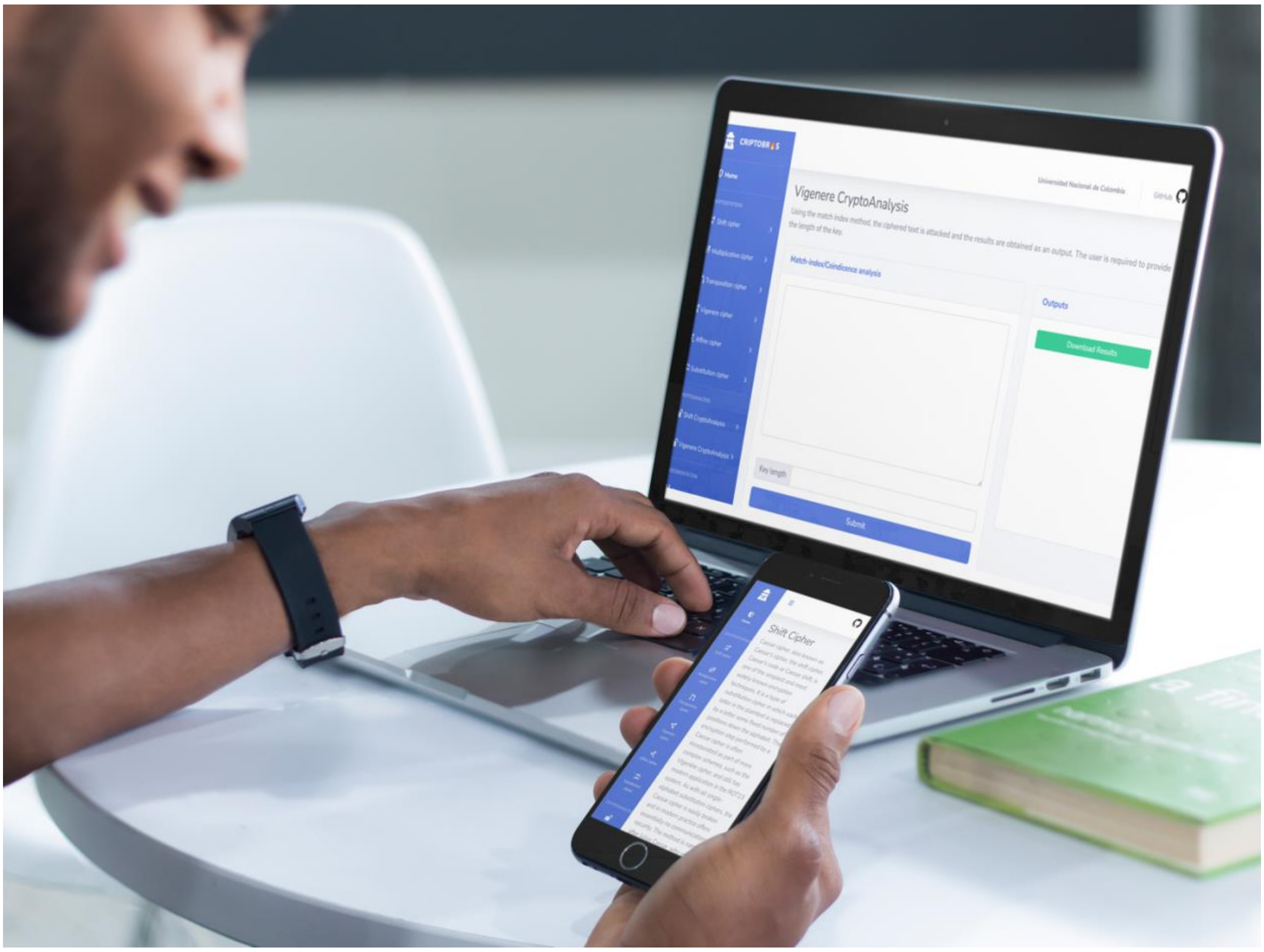
With brute force we try every displacement of the cipher to find one that makes sense, We go through the 26 keys of Z_26.

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 have knowledge of 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.

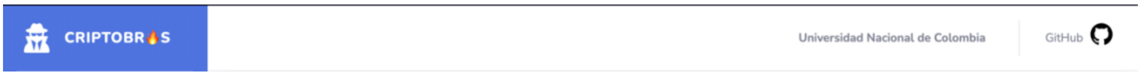


Using the match index method, the ciphered text is attacked and the results are obtained as an output. The user is required to provide the length of the key.

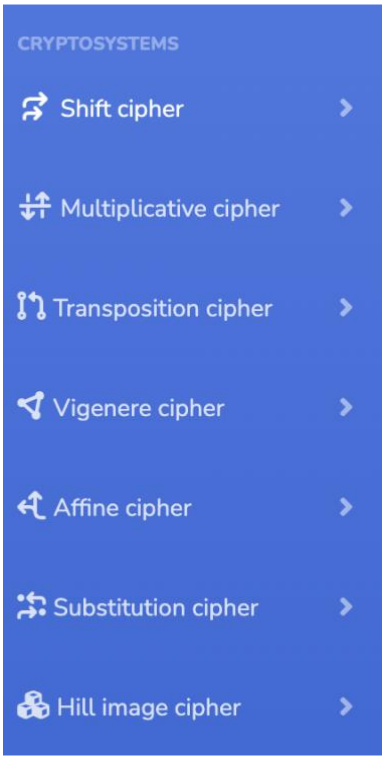
2. CriptoBros Online App Overview:

The panel of CriptoBros is divided into 4 areas:

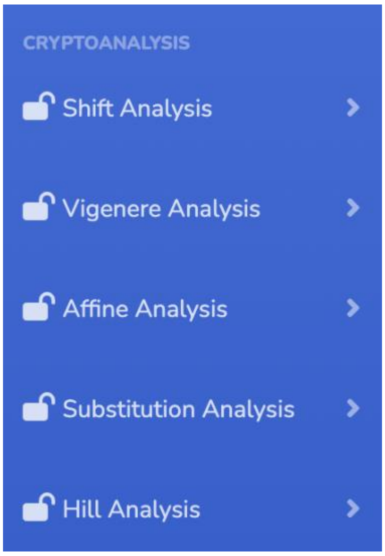
1. **Home**: We can see the name of the page **CriptoBros,** and some other features like the name of the University, Universidad Nacional de Colombia, that will carry you to the principal page of the university with just one click away, right next to it, will be found a logo of GitHub where you will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



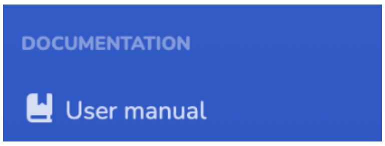
2. **Cryptosystems**: Suite of cryptographic algorithms needed to implement a particular security service, such as confidentiality. for example, we have: Shift cipher, Multiplicative cipher, Transposition cipher, Vigenère cipher, Affine cipher, Substitution cipher.



3. **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, Hill cryptoanalysis.



4. **Documentation:** Provides easily accessible information on this product and gives answers to important questions pertaining to: product usage in general. aspects of functionality. architecture of a technical product.

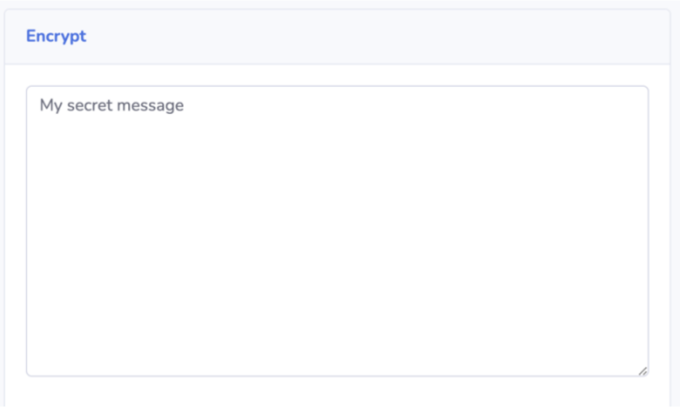


3. Crypto Systems:

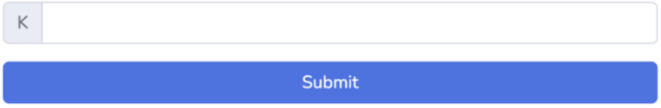
Let's take a view of each of the cryptosystem:

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:

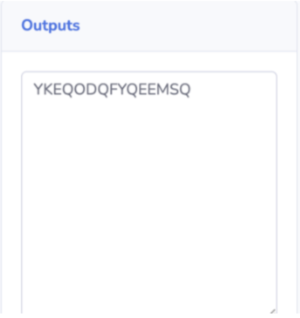
- **Encrypt:** Where you put your top-secret message or just something you want to say in a plain text.



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.

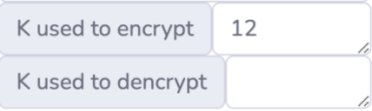


- **Outputs:** You will find the encrypted or the plaint text. If you use the Encrypt box you will be find the encrypted text, in the other hand, if you use the Decrypt box you will see the decrypted text, i.e., plain text.



YKEQODQFYQEEMSQ

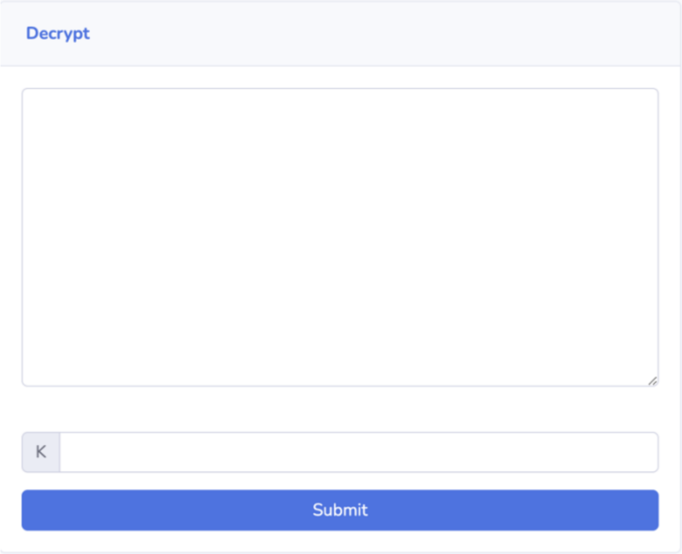
Under that box it will be shown de key (K) used to encrypt and decrypt ither it's encrypted or decrypted.



K used to encrypt: 12

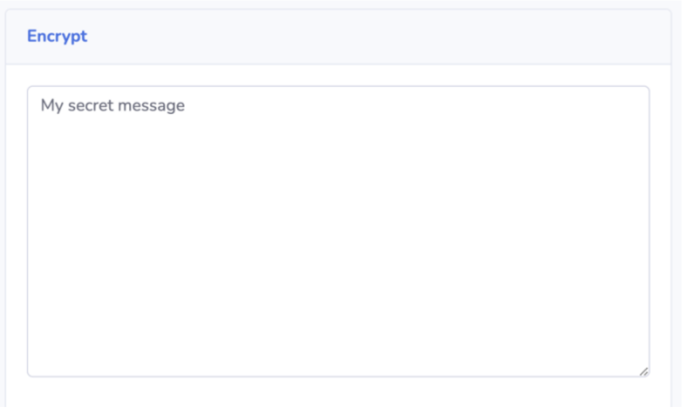
K used to dencrypt:

- **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.

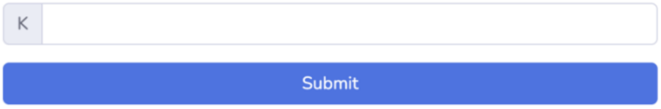


2. **Multiplicative Cipher System**: The first to see it's a is a brief explanation of the type of system, like: "Multiplicative Ciphers work by using the modulo operator to encrypt and decrypt messages." Then you can find 3 boxes:

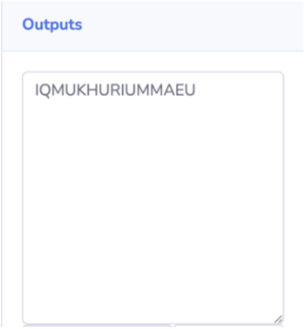
- **Encrypt:** Where you put your top-secret message or just something you want to say in a plain text.



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 with just pressing submit.

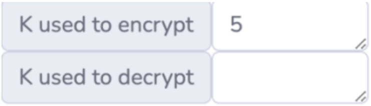


- **Outputs:** You will find the encrypted or the plaint text. If you use the Encrypt box you will be find the encrypted text, in the other hand, if you use the Decrypt box you will see the decrypted text, i.e., plain text.



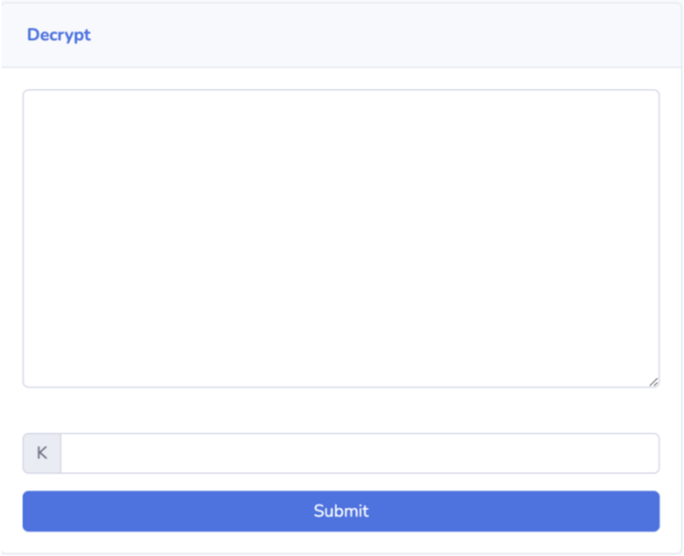
IQMUKHURIUMMAEU

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



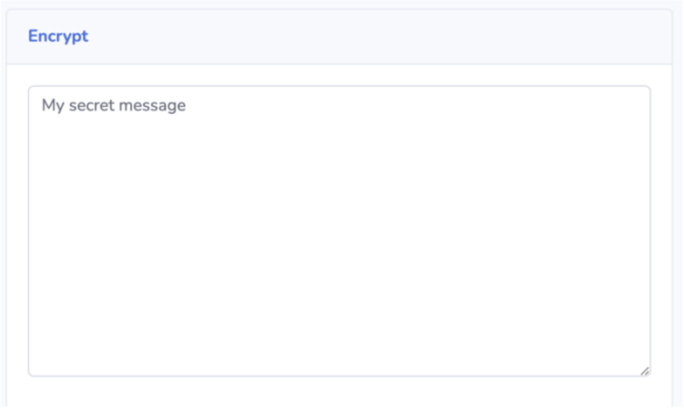
K used to encrypt	5
K used to decrypt	

- **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.

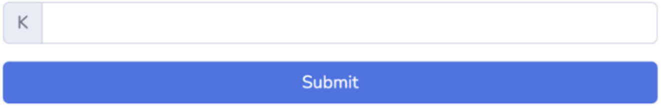


3. **Transposition Cipher System:** The first to see it's a is a brief explanation of the type of system, like: "Transposition cipher is the name given to any encryption that involves rearranging the plain text letters in a new order." Then you can find 3 boxes:

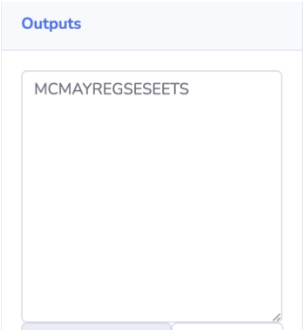
- **Encrypt:** Where you put your top-secret message or just something you want to say in a plain text.



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.

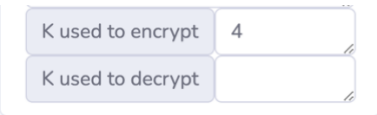


- **Outputs:** You will find the encrypted or the plaint text. If you use the Encrypt box you will be find the encrypted text, in the other hand, if you use the Decrypt box you will see the decrypted text, i.e., plain text.



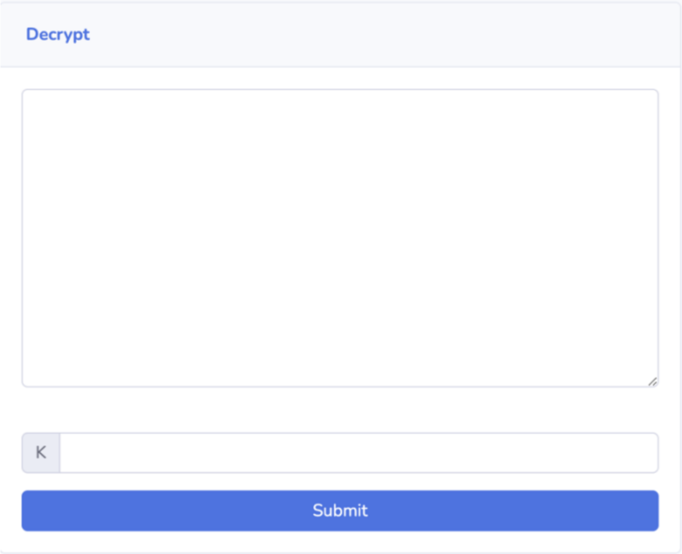
```
MCMAYREGSESEETS
```

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



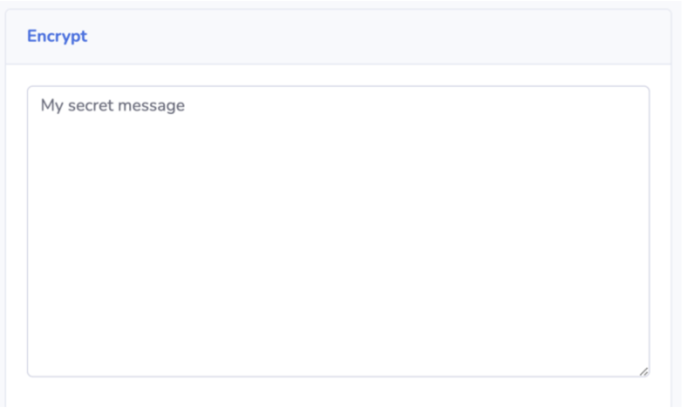
K used to encrypt	4
K used to decrypt	

- **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.

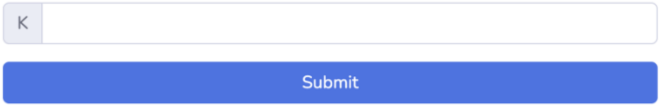


4. **Vigenère Cipher System:** The first to see it's a is a brief explanation of the type of system, like: "Vigenère Cipher is a method of encrypting alphabetic text. It uses a simple form of polyalphabetic substitution. A polyalphabetic cipher is any cipher based on substitution, using multiple substitution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

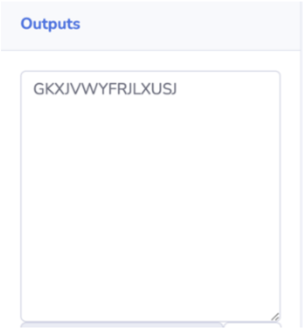
- **Encrypt:** Where you put your top-secret message or just something you want to say in a plain text.



It is also needed a string key (K), it 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.

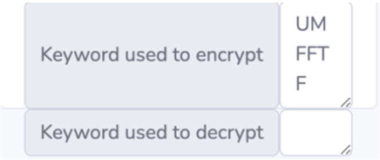


- **Outputs:** You will find the encrypted or the plaint text. If you use the Encrypt box you will be find the encrypted text, in the other hand, if you use the Decrypt box you will see the decrypted text, i.e., plain text.



GKXJVWYFRJLXUSJ

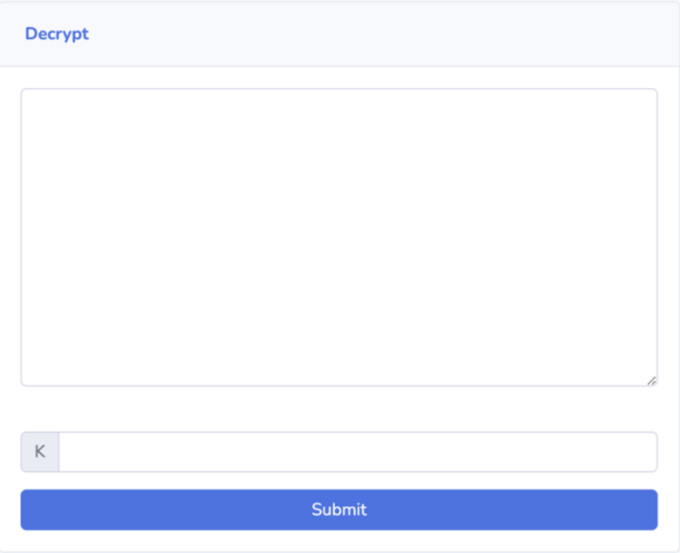
Under that box it will be shown de key (K) used to encrypt and decrypt ither it's encrypted or decrypted.



Keyword used to encrypt: UM FFT F

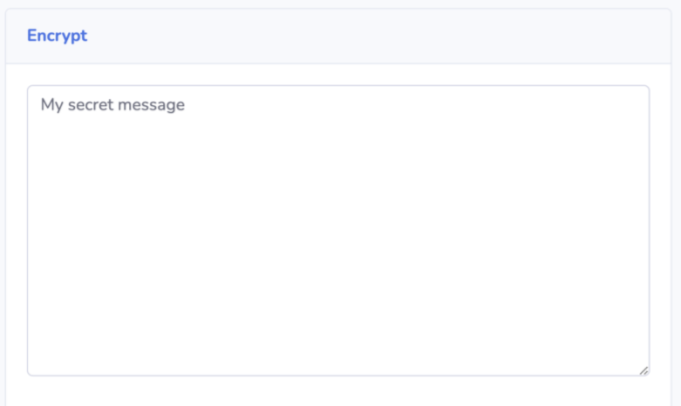
Keyword used to decrypt:

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

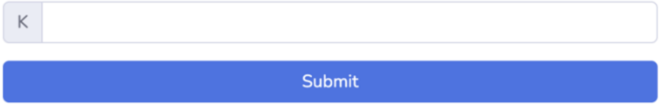


5. **Affine Cipher System:** The first to see it's a is a brief explanation of the type of system, like: "The affine cipher is a type of monoalphabetic substitution cipher, where each letter in an alphabet is mapped to its numeric equivalent, encrypted using a simple mathematical function, and converted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

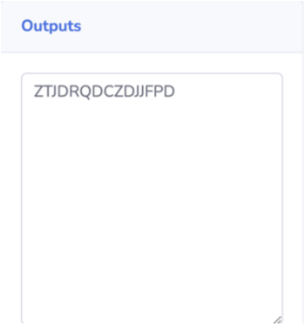
   - **Encrypt:** Where you put your top-secret message or just something you want to say in a plain text.



It is also needed a key (K), it can be a tuple that are relative numbers mod 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 key (K) with the specifications mentioned before by just pressing submit.

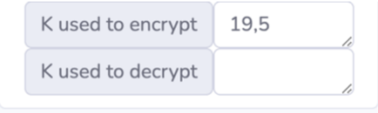


- **Outputs:** You will find the encrypted or the plaint text. If you use the Encrypt box you will be find the encrypted text, in the other hand, if you use the Decrypt box you will see the decrypted text, i.e., plain text.

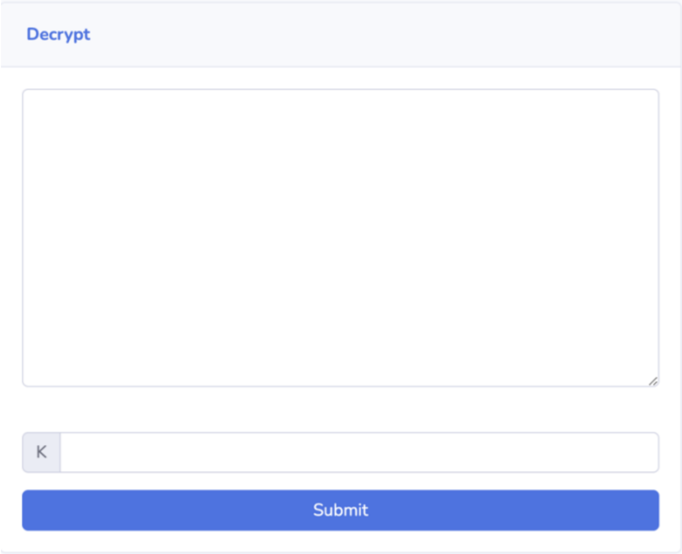

Outputs

ZTJDRQDCZDJJFPD

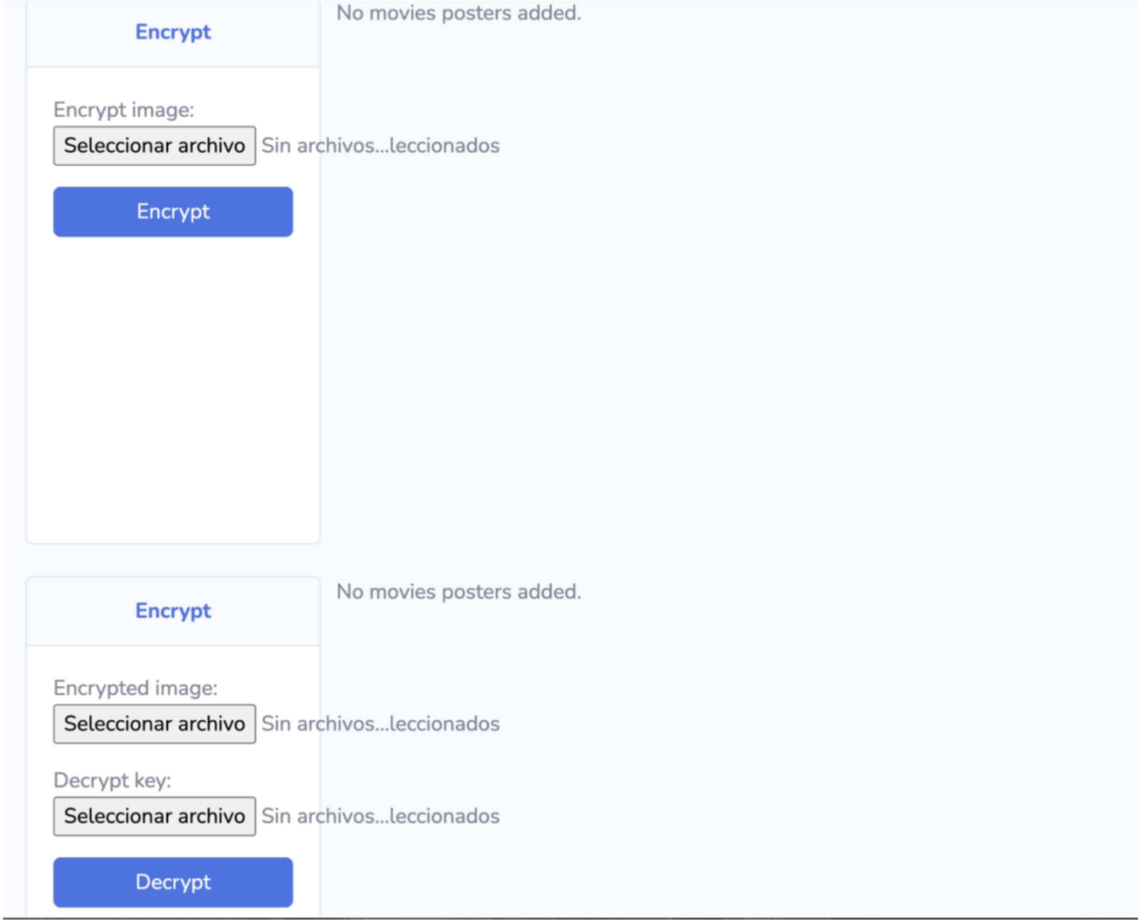
Under that box it will be shown de key (K) used to encrypt and decrypt ither it's encrypted or decrypted.


K used to encrypt	19,5
K used to decrypt	

- **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.


Decrypt

6. **Hill Image System:** The Hill cipher algorithm is one of the symmetric key algorithms that have 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, then encrypted text cannot be decrypted. In the Involutory matrix generation method the key matrix used for the encryption is itself invertible.



No movies posters added.

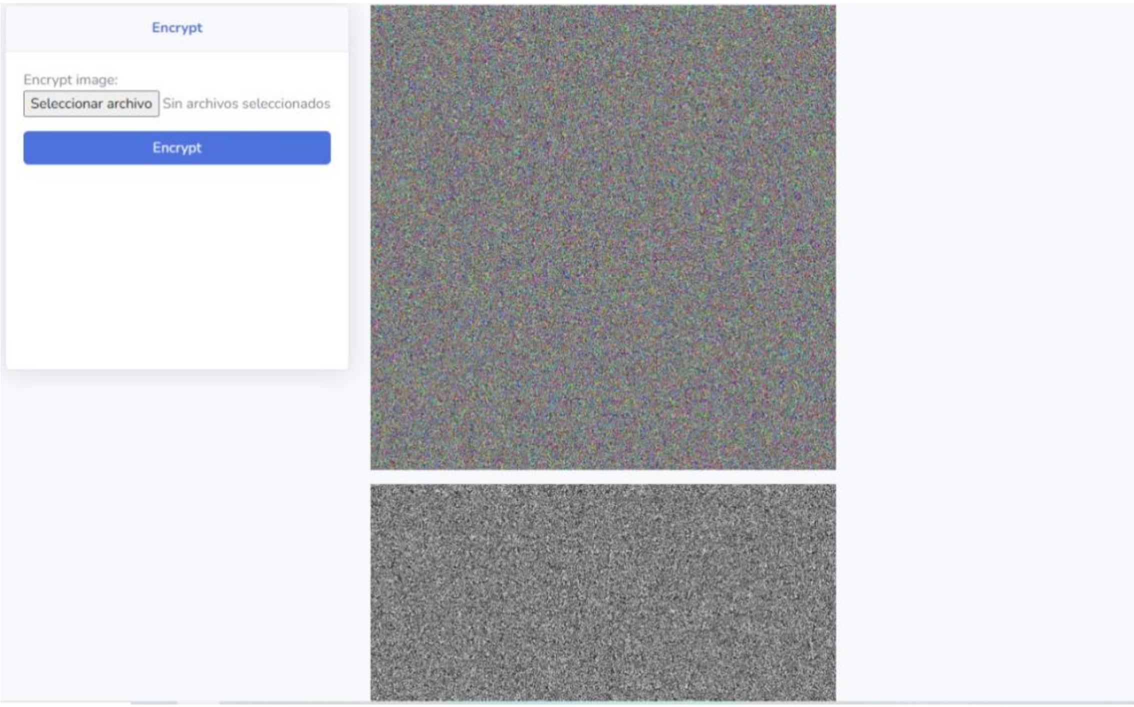
Sin archivos...leccionados

No movies posters added.

Sin archivos...leccionados

Sin archivos...leccionados

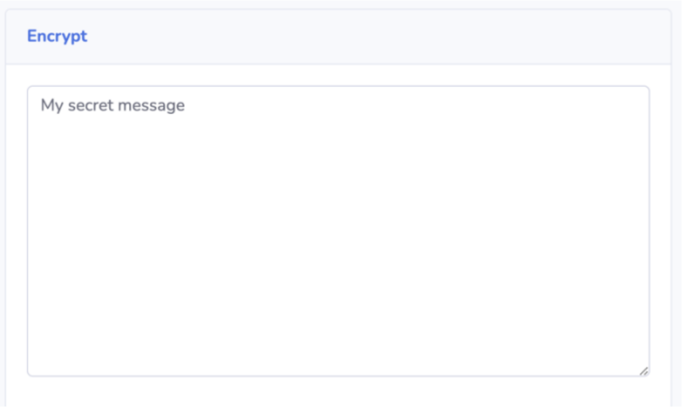
Implemented Hill Cipher technique one is cover image which act as key image which is shared by both sender and receiver and other is Informative image. As first step, we add cover image and informative image to obtained resultant image. Uploading and image



Sin archivos seleccionados

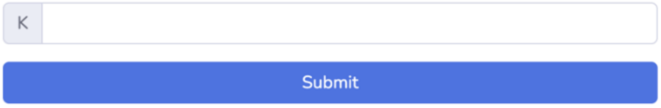
7. **Substitution Cipher System:** The first to see it's a is a brief explanation of the type of system, like: "Substitution cipher is a method of encrypting in which units of plaintext are replaced with the ciphertext, in a defined manner, with the help of a key; the "units" may be single letters (the 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 a plain text.

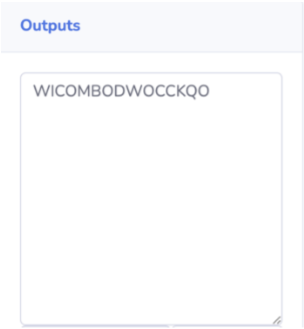


My secret message

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.

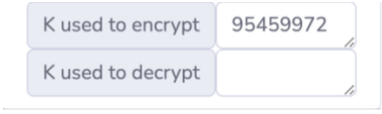


- **Outputs:** You will find the encrypted or the plaint text. If you use the Encrypt box you will be find the encrypted text, in the other hand, if you use the Decrypt box you will see the decrypted text, i.e., plain text.



WICOMBODWOCCKQO

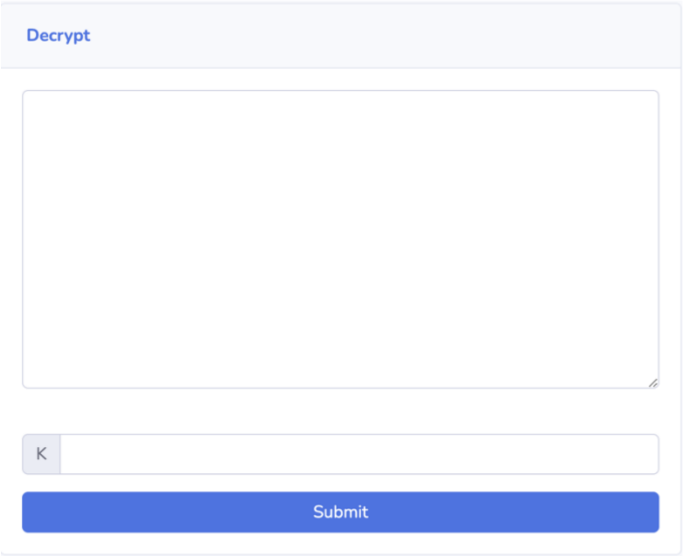
Under that box it will be shown de key (K) used to encrypt and decrypt ither it's encrypted or decrypted.



K used to encrypt 95459972

K used to decrypt

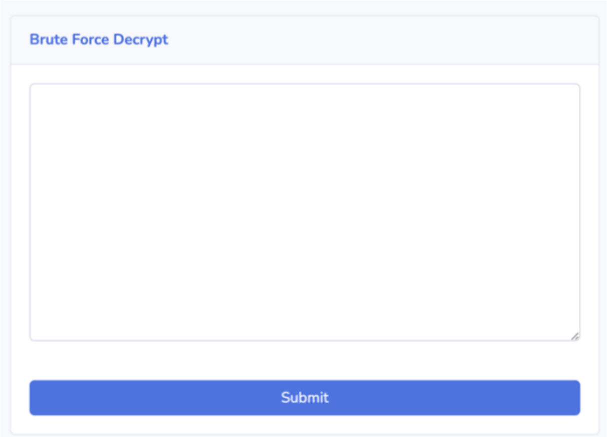
- **Decrypt**: If you have an encrypted text, use the decryption box to return to the plain text using a key (K) mentioned before.



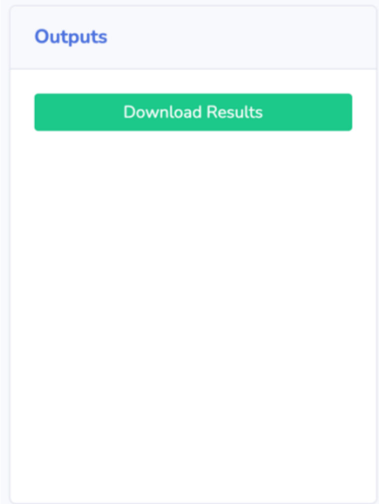
4. Crypto Analysis:

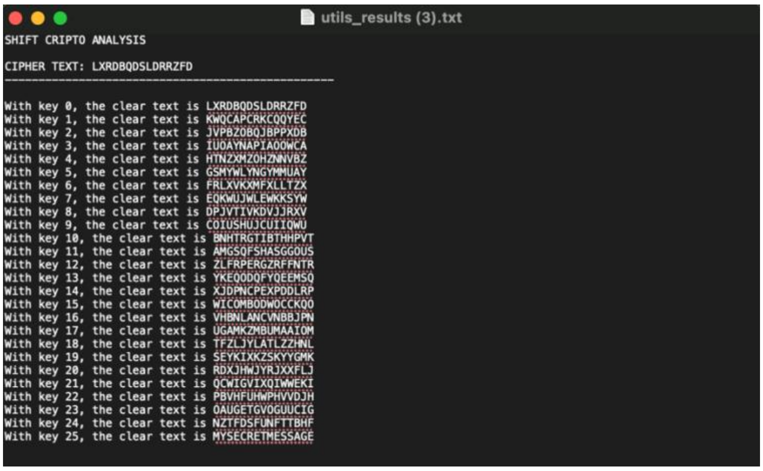
Cryptanalysis is the process of studying cryptographic systems to look for weaknesses or leaks of information. Let’s see how we can break-in.

1. **Shift Cryptanalysis:** With brute force we try every displacement of the cipher to find one that 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.

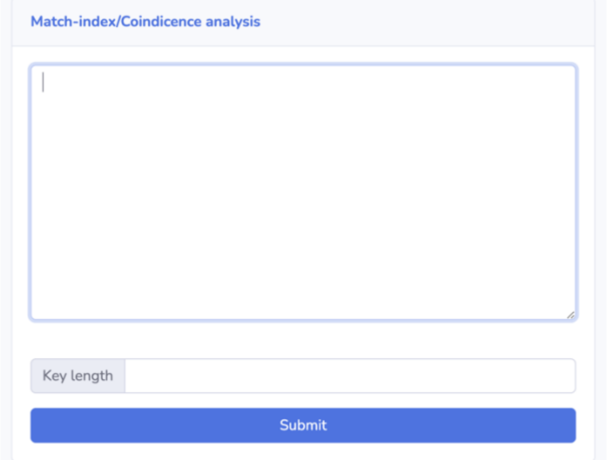




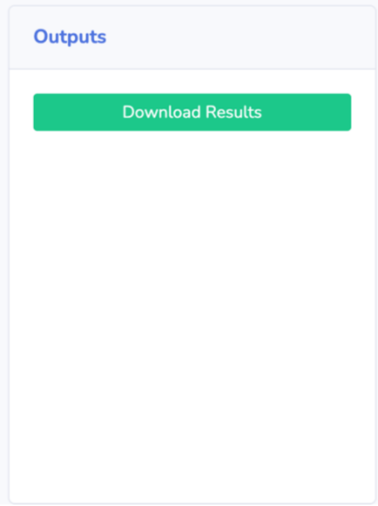
```
SHIFT CRIPTO ANALYSIS

CIPHER TEXT: LXRDBQDSLDRRZFD
--------------------------------------------------

With key 0, the clear text is LXRDBQDSLDRRZFD
With key 1, the clear text is KWQCAPCRKCQQYEC
With key 2, the clear text is JVPBZOBQJBPPXDB
With key 3, the clear text is IUOAYNAPIAOOWCA
With key 4, the clear text is HTNZXMZOHZNNVBZ
With key 5, the clear text is GSMYWLYNGYMMUAY
With key 6, the clear text is FRLXVKXMFXLLTZX
With key 7, the clear text is EQKWUJWLEWKKSYW
With key 8, the clear text is DPJVTIVKDVJJRXV
With key 9, the clear text is COIUSHUJCUIIQWU
With key 10, the clear text is BNHTRGTIBTHHPVT
With key 11, the clear text is AMGSQFSHASGGOUS
With key 12, the clear text is ZLFRPERGZRFFNTR
With key 13, the clear text is YKEQODQFYQEEMSQ
With key 14, the clear text is XJDPNCPEXPDDLRP
With key 15, the clear text is WICOMBODWOCCKQO
With key 16, the clear text is VHBNLANCVNBBJPN
With key 17, the clear text is UGAMKZMBUMAAIOM
With key 18, the clear text is TFZLJYLATLZZHNL
With key 19, the clear text is SEYKIXKZSKYYGMK
With key 20, the clear text is RDXJHWJYRJXXFLJ
With key 21, the clear text is QCWIGVIXQIWWEKI
With key 22, the clear text is PBVHFUHWPHVVDJH
With key 23, the clear text is OAUGETGVOGUUCIG
With key 24, the clear text is NZTFDSFUNFTTBHF
With key 25, the clear text is MYSECRETMESSAGE
```

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

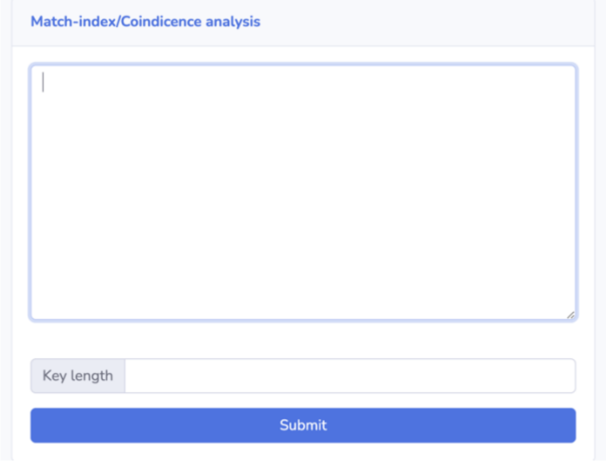
2. **Vigenère Cryptanalysis:** Using the match index method, the ciphered text is attacked and the results are obtained as an output. The user is required to provide the length of the key and press Submit.



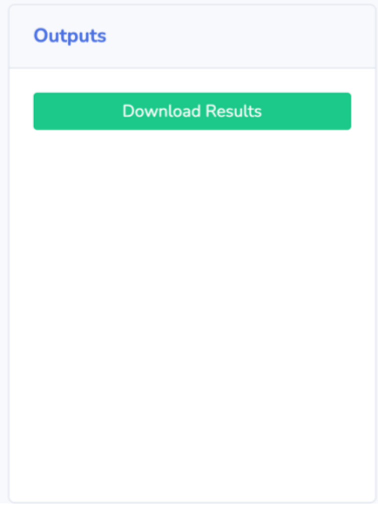
In the box shown above we write de encrypted message we want to decrypt, the by pressing submit we get a result we will be downloading, giving us a .txt file with the possible key and the decrypted code.

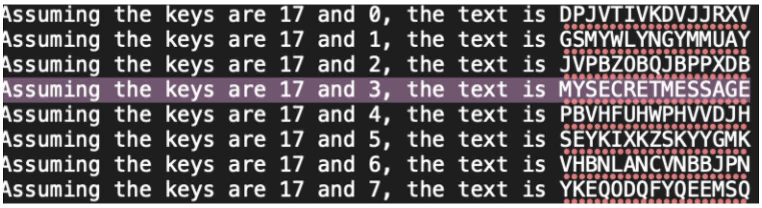


3. **Affine Cryptoanalysis:** With brute force we try every possible combination of keys to find one that makes sense. We go through the 312 possible keys. And that because there are finites combinations of a and b.



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

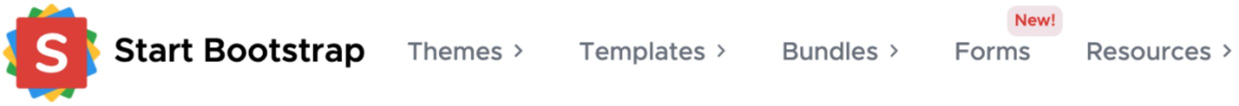




```
Assuming the keys are 17 and 0, the text is DPJVTIVKDVJJRXV
Assuming the keys are 17 and 1, the text is GSMYWLYNGYMMUAY
Assuming the keys are 17 and 2, the text is JVPBZOBQJBPPXDB
Assuming the keys are 17 and 3, the text is MYSECRETMESSAGE
Assuming the keys are 17 and 4, the text is PBVHFUHWPHVVDJH
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
```

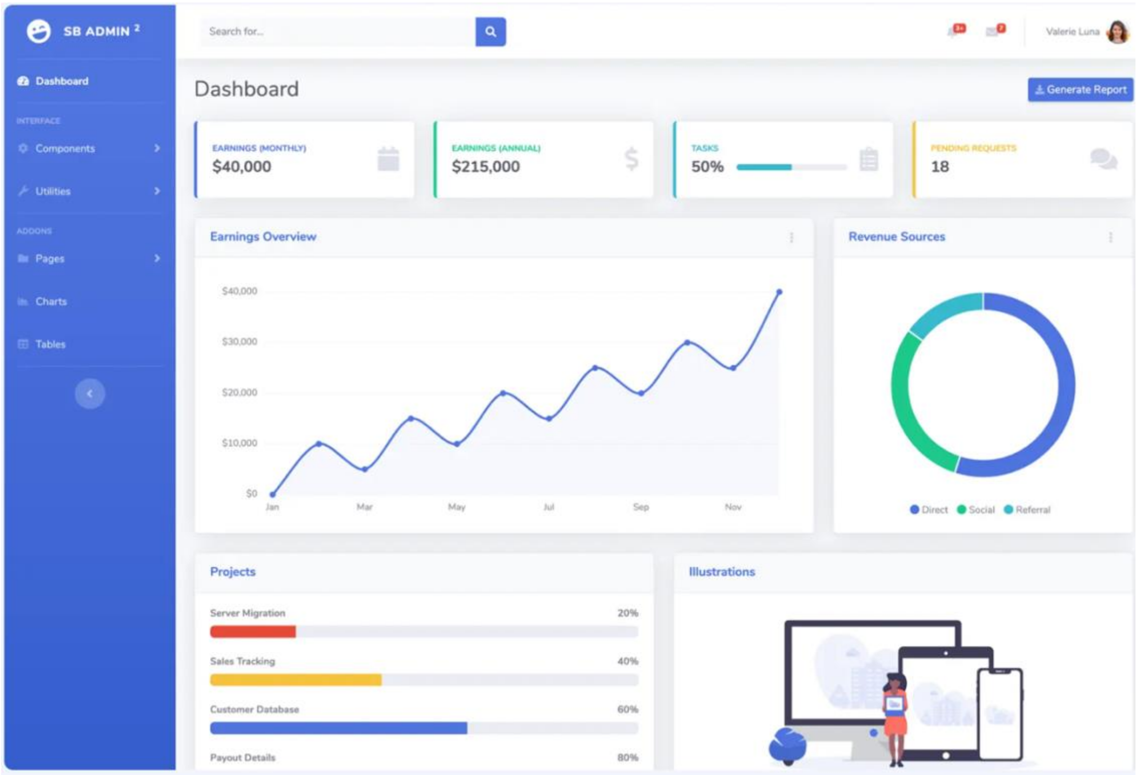
5. Page Design:

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

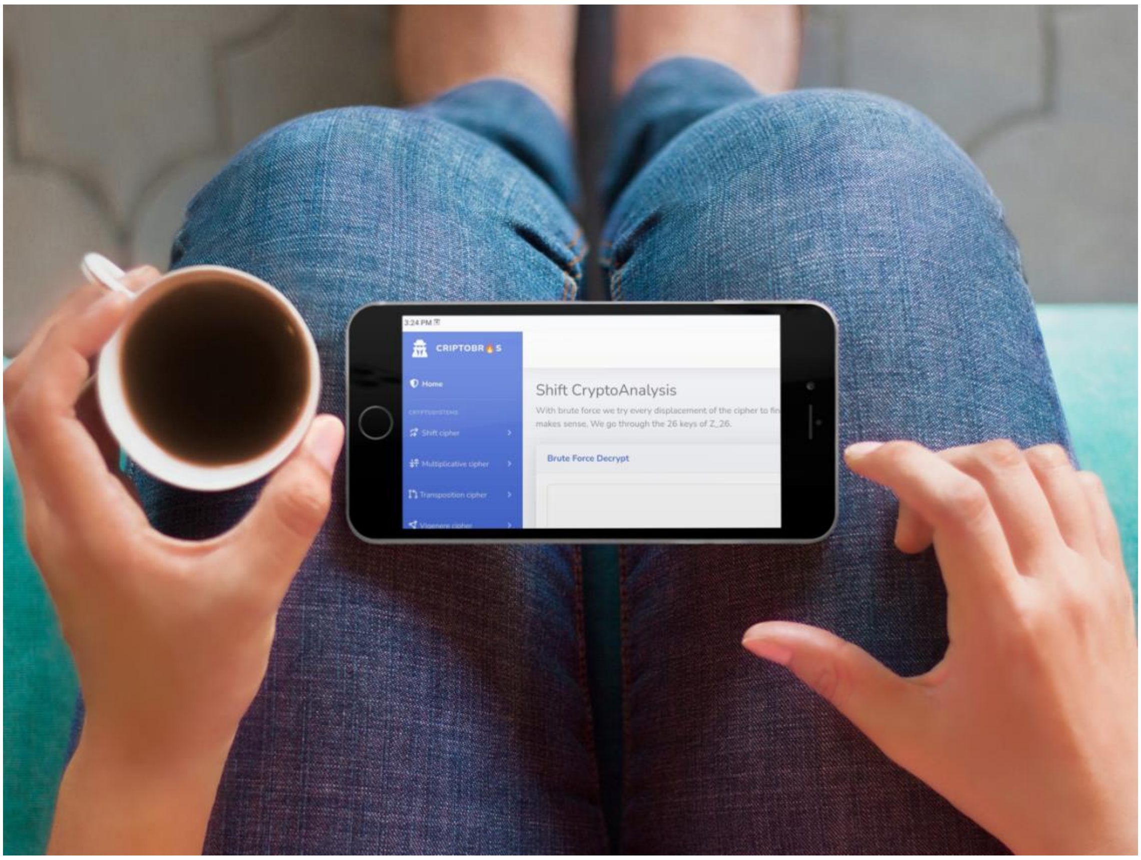


- Templete:

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. It's 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, focus on utility, classes to minimize CSS bloat, custom card and button components, custom utility classes for extended functionality.



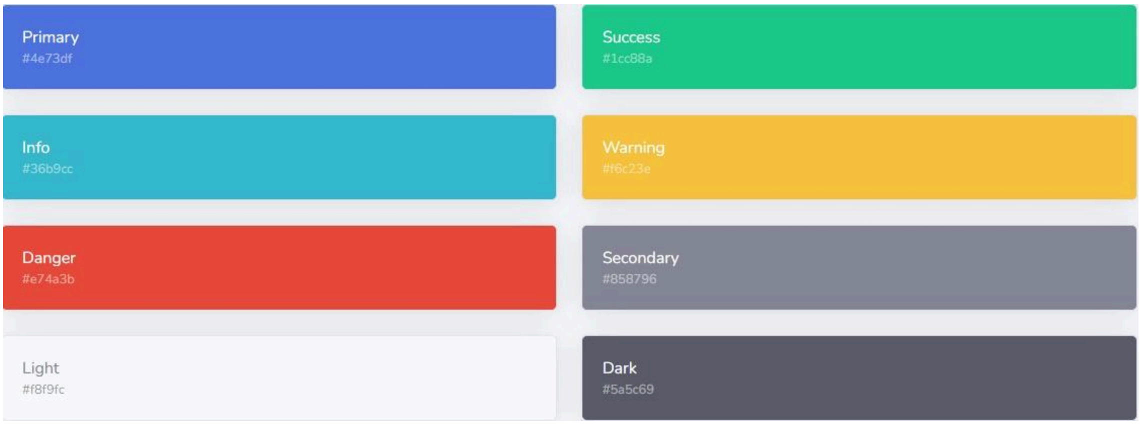
Shift CryptoAnalysis

With brute force we try every displacement of the cipher to fin
makes sense. We go through the 26 keys of Z_26.

- ## 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's vibrant vibe.



Primary #4e73df	Success #1cc88a
Info #36b9cc	Warning #f6c23e
Danger #e74a3b	Secondary #858796
Light #f8f9fc	Dark #5a5c69