

# MADAME X

## MANUAL



**Developed by:**

CRISTHIAN PARDO  
TANIA CASTILLO

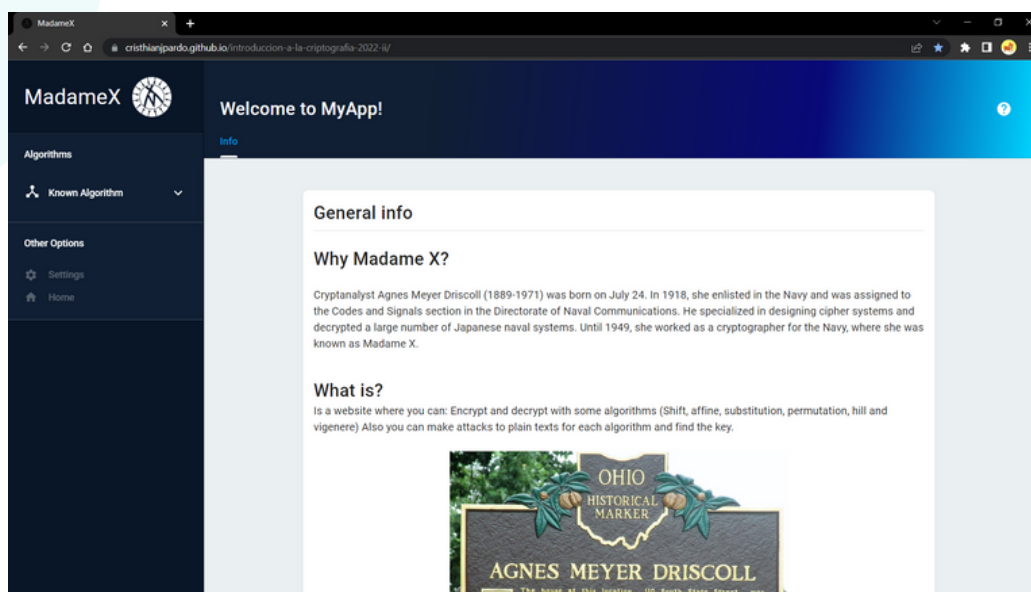
GABRIEL QUINCHE  
JUAN LARA

# Content

- 1. Inicio
- 2. Interface
- 3. Algorithms
  - a. Classic cryptosystems
    - i. Monoalphabetics
      - 1. **Affine**
      - 2. **Shift**
      - 3. **Substitution**
    - ii. Polyalphabetics
      - 1. **Hill**
      - 2. **Permutation**
      - 3. **Vigenere**
  - b. Block cryptosystems
    - i. S-DES
    - ii. DES
      - 1. ECB
      - 2. CBC
      - 3. OFB
      - 4. CFB
      - 5. CTR
    - iii. T-DES
      - 1. ECB
      - 2. CBC
      - 3. OFB
      - 4. CFB
      - 5. CTR
    - iv. AES
      - 1. ECB
      - 2. CBC
      - 3. OFB
      - 4. CFB
      - 5. CTR
  - c. Gamma Pentagonal
  - d. RSA
  - e. Rabin
  - f. ElGammal
  - g. ECC 25519

# Inicio

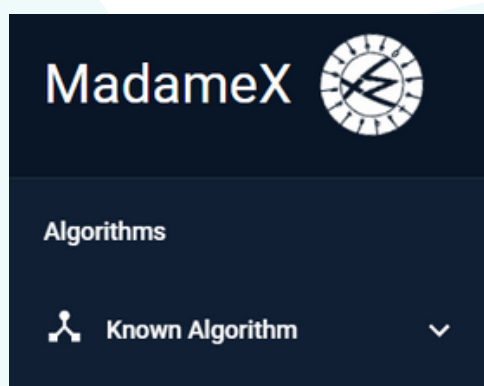
This is the first page that you can see:



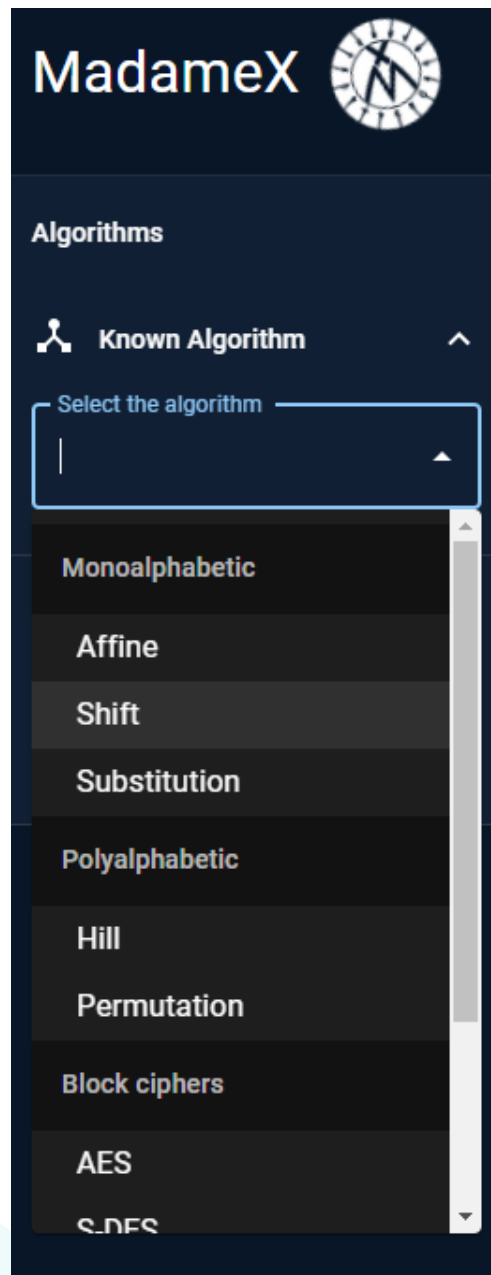
Here you can find a short description of this project, the answers of questions like why Madame X? or whats it this about.

# Algorithms

To see the menu with the algorithms you have to click in "Known Algorithm":



Then you can see a menu where you can search or select the algorithm that you prefer or you need:



## MONOALPHABETICS

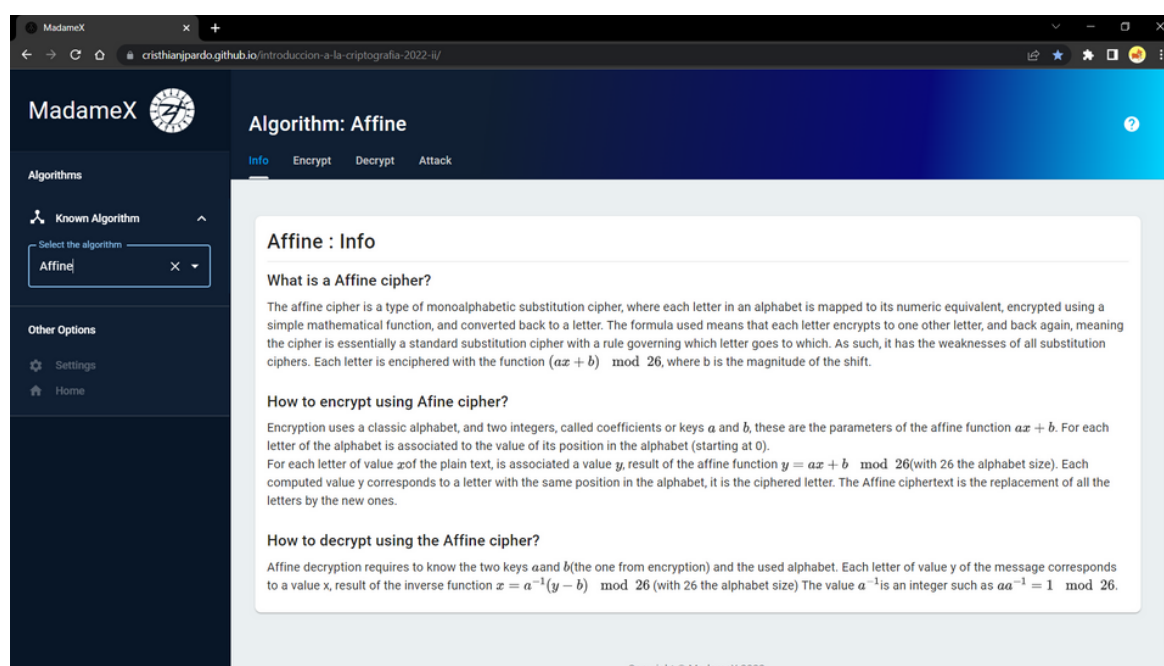
In the algorithms you see two sections:

### Monoalphabetic and Polyalphabetics

Let's see the monoalphabetic algorithms:

# Affine

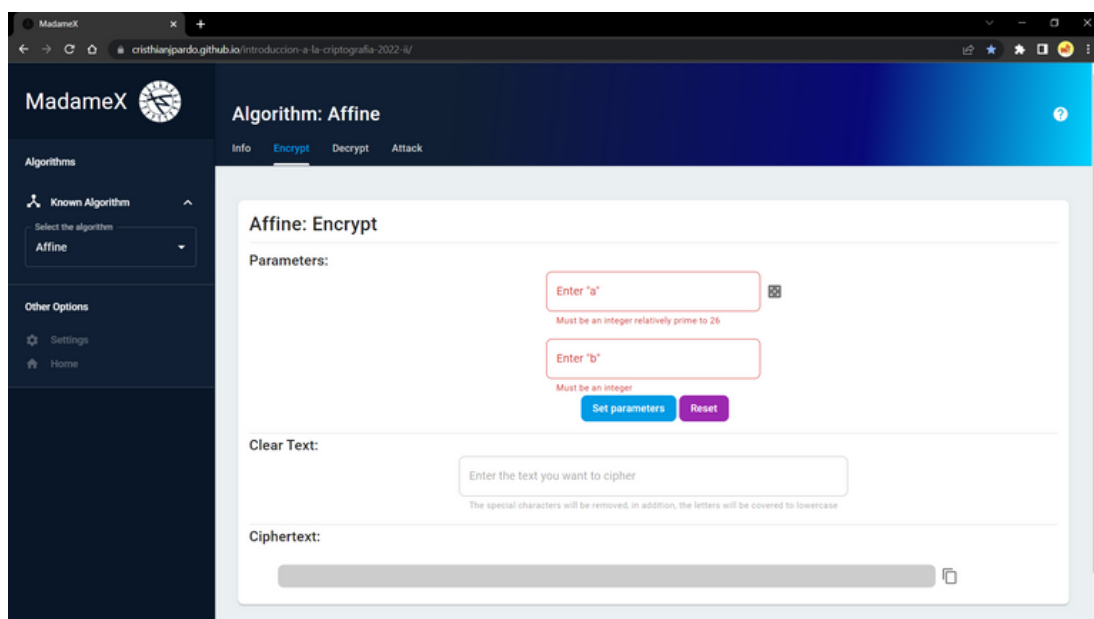
This is what you see when



Here you can find summary info about this algorithm, how to encrypt and decrypt whit it. Also you have different enviroments: Encrypt, Decrypt and Attack

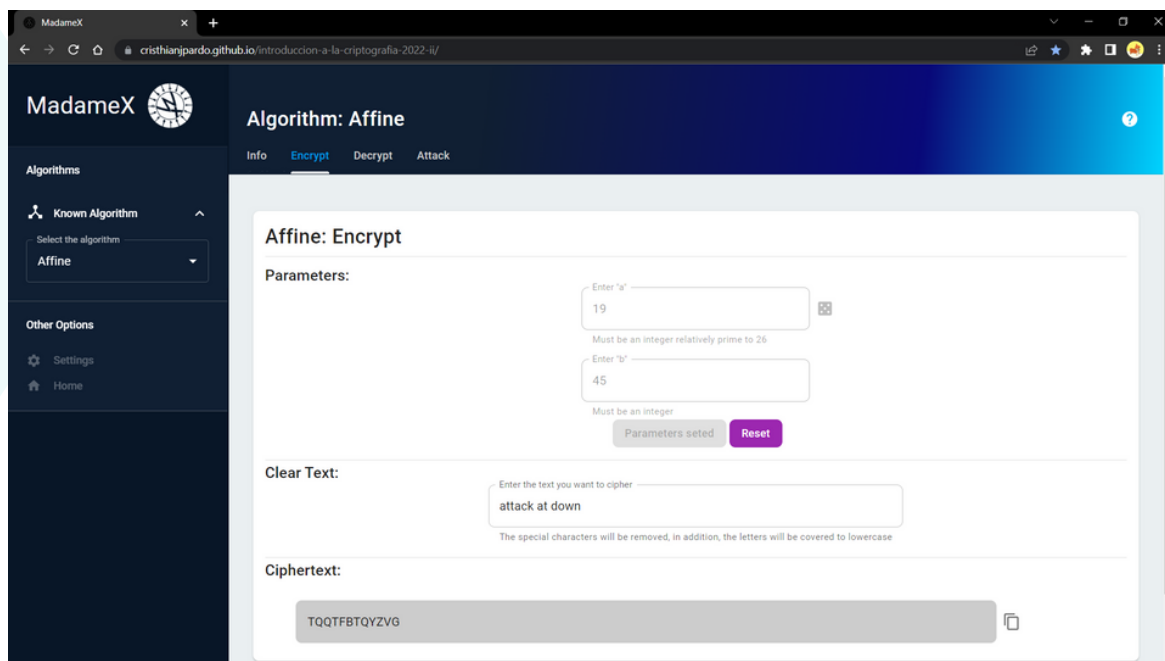
## Encrypt

In this part you have to write the parameters for a and b, in this case you can set a random number for "a". Once you already write valid parameters you click on "Set Parameters".



The screenshot shows the 'Affine: Encrypt' interface of the MadameX application. The left sidebar contains 'Algorithms' (with 'Affine' selected), 'Other Options' (Settings, Home), and 'Known Algorithm'. The main area has tabs for 'Info', 'Encrypt', 'Decrypt', and 'Attack'. Under 'Parameters:', there are two input fields: 'Enter "a"' (with a note 'Must be an integer relatively prime to 26') and 'Enter "b"' (with a note 'Must be an integer'). Below these are 'Set parameters' and 'Reset' buttons. The 'Clear Text:' section has an input field with the placeholder 'Enter the text you want to cipher' and a note 'The special characters will be removed, in addition, the letters will be covered to lowercase'. The 'Ciphertext:' section shows a grey box with a copy icon.

Once you already set the parameters you can encrypt a plain text that you write in "Clear text" box and in real time you'll see the cipher text below. Additional you can copy that text click on the copy button at the right of the grey box.



The screenshot shows the 'Affine: Encrypt' interface after parameters have been set. The 'Parameters:' section now shows 'Enter "a"' with the value '19' and 'Enter "b"' with the value '45'. The 'Set parameters' button is now disabled and labeled 'Parameters seted', while the 'Reset' button remains active. The 'Clear Text:' input field now contains the text 'attack at down'. The 'Ciphertext:' section shows the resulting ciphertext 'TQQTFBTQYZVG' in a grey box with a copy icon.

## Decrypt

Here you can find summary info about this algorithm, how to encrypt and decrypt with it. Also you have different environments: Encrypt, Decrypt and Attack

The screenshot shows the 'MadameX' web application interface. The left sidebar contains a navigation menu with 'Algorithms' (Known Algorithm: Affine), 'Other Options' (Settings, Home), and a clock icon. The main content area is titled 'Algorithm: Affine' and has tabs for 'Info', 'Encrypt', 'Decrypt' (selected), and 'Attack'. The 'Affine: Decrypt' section includes a 'Parameters' area with input fields for 'a' (19) and 'b' (45), both with validation messages: 'Must be an integer relatively prime to 26' and 'Must be an integer'. Below these are 'Parameters seted' and 'Reset' buttons. The 'Ciphertext' section has an input field containing 'TQQTFBTQYZVG' and a note: 'The special characters will be removed, in addition, the letters will be covered to uppercase'. The 'Clear Text' section shows the result 'ATTACKATDOWN' in a grey box with a copy icon.

## Attack

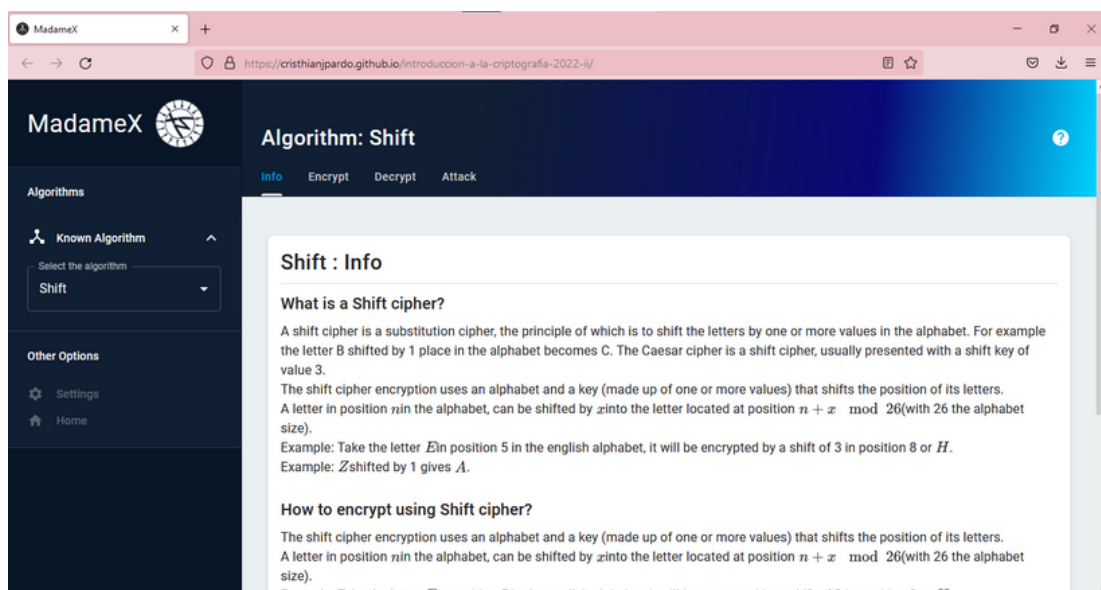
Here you can try to decipher a text that used the affine cipher, just write your text and our algorithm will suggest possible decryptions

The screenshot shows the 'MadameX' web application interface with the 'Attack' tab selected. The 'Ciphertext' section contains the same input 'TQQTFBTQYZVG'. The 'Attack Results' section displays four possible decryptions, each with its corresponding 'a' and 'b' values and a copy icon:

a	b	Decryption
5	25	ETTEWQETFAUR
7	16	TAATRJTQFXG
19	19	ATTACKATDOWN
21	10	TEETBHATESXDG

# Shift

This is what you see when



Here you can find summary info about this algorithm, how to encrypt and decrypt with it. Also you have different environments: Encrypt, Decrypt and Attack



## Encrypt

Here you can find summary info about this algorithm, how to encrypt and decrypt whit it. Also you have different enviroments: Encrypt, Decrypt and Attack

MadameX

Algorithm: Shift

Info Encrypt Decrypt Attack

Shift: Encrypt

Parameters:

Enter the number of shifts

Must be an integer (positive or negative)

Set parameters Reset

Clear Text:

Enter the text you want to cipher

The special characters will be removed, in addition, the letters will be covered to lowercase

Ciphertext:

Here you can find summary info about this algorithm, how to encrypt and decrypt whit it. Also you have different enviroments: Encrypt, Decrypt and Attack

MadameX

Algorithm: Shift

Info Encrypt Decrypt Attack

Shift: Encrypt

Parameters:

Enter the number of shifts

10

Must be an integer (positive or negative)

Parameters seted Reset

Clear Text:

Enter the text you want to cipher

ATTACKATDAWN

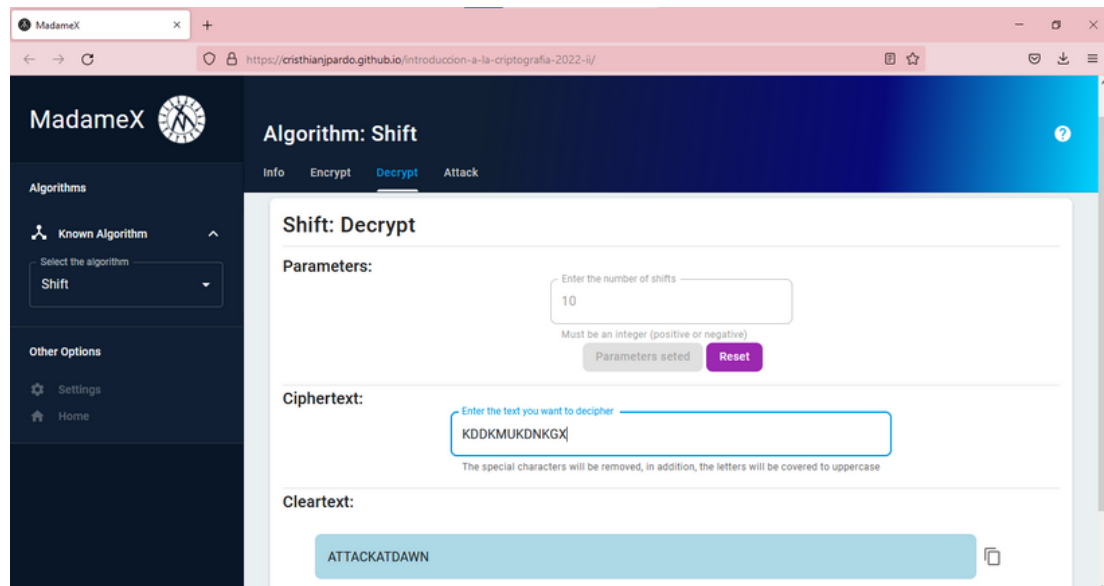
The special characters will be removed, in addition, the letters will be covered to lowercase

Ciphertext:

KDDKMUKDNKGX

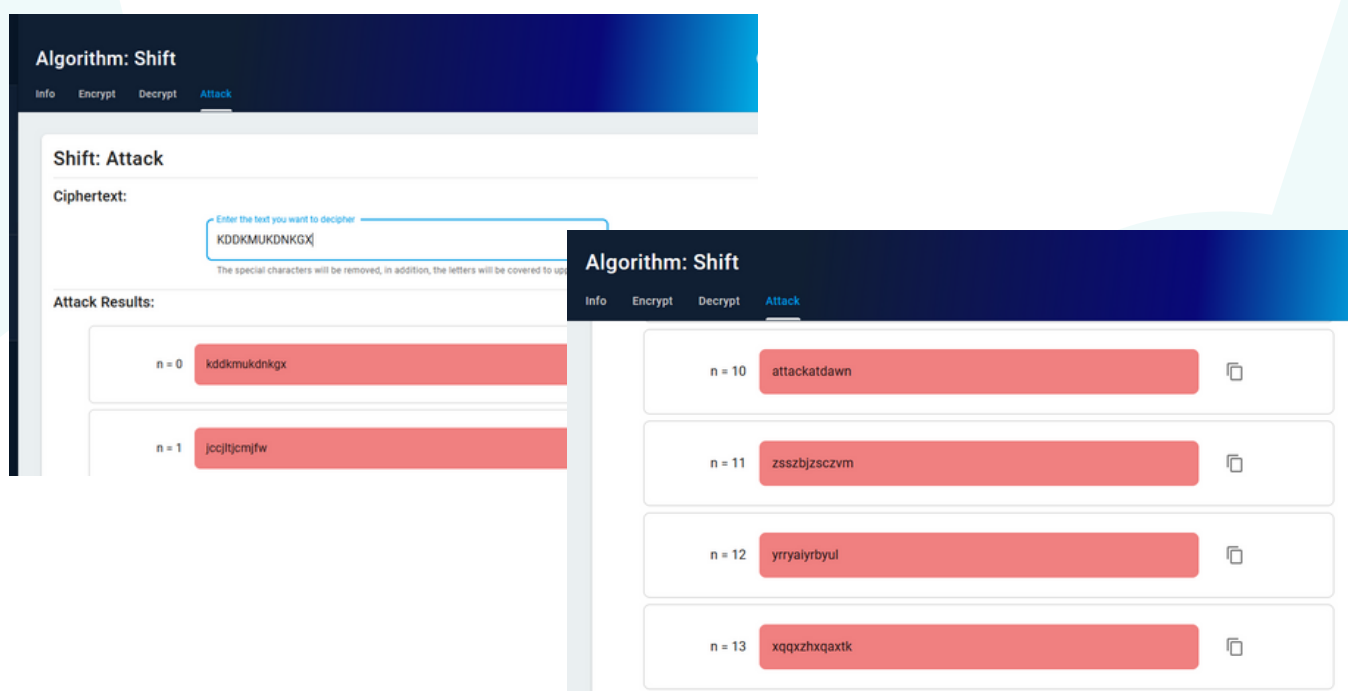
## Decrypt

Here you can find summary info about this algorithm, how to encrypt and decrypt with it. Also you have different environments: Encrypt, Decrypt and Attack



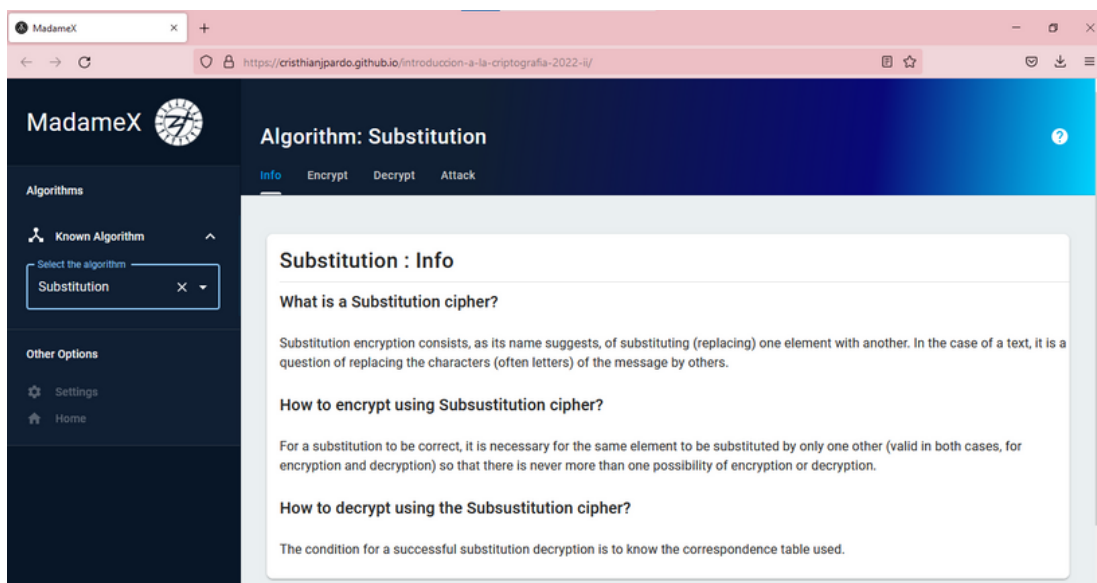
## Attack

Here you can try to decipher a text that used the shift cipher. Also you have different environments: Encrypt, Decrypt and Attack



# Substitution

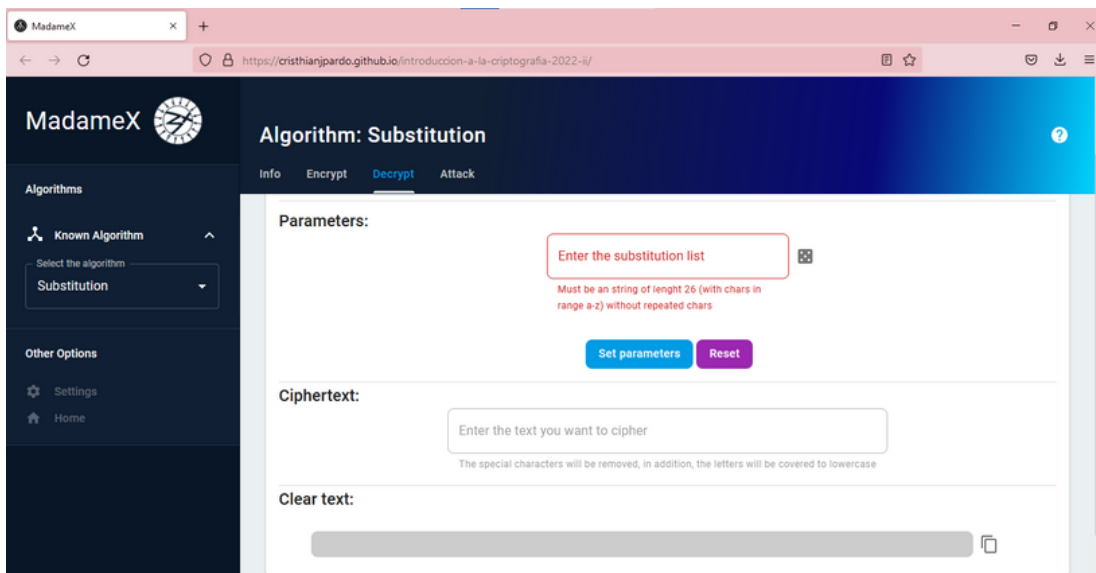
This is what you see when



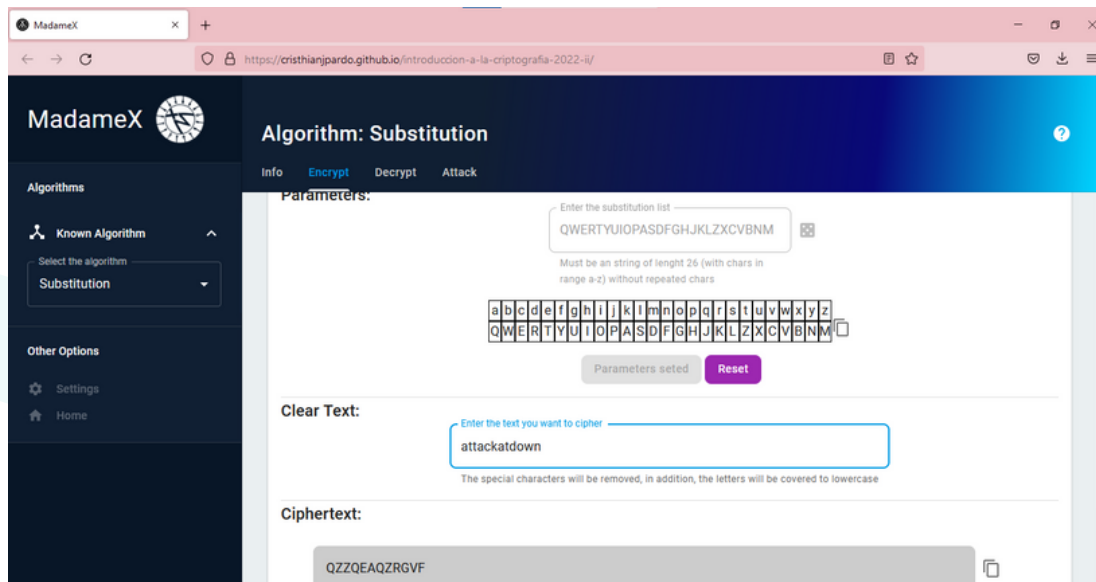
Here you can find summary info about this algorithm, how to encrypt and decrypt with it. Also you have different environments: Encrypt, Decrypt and Attack

# Encrypt

Here you can find summary info about this algorithm, how to encrypt and decrypt whit it. Also you have different enviroments: Encrypt, Decrypt and Attack

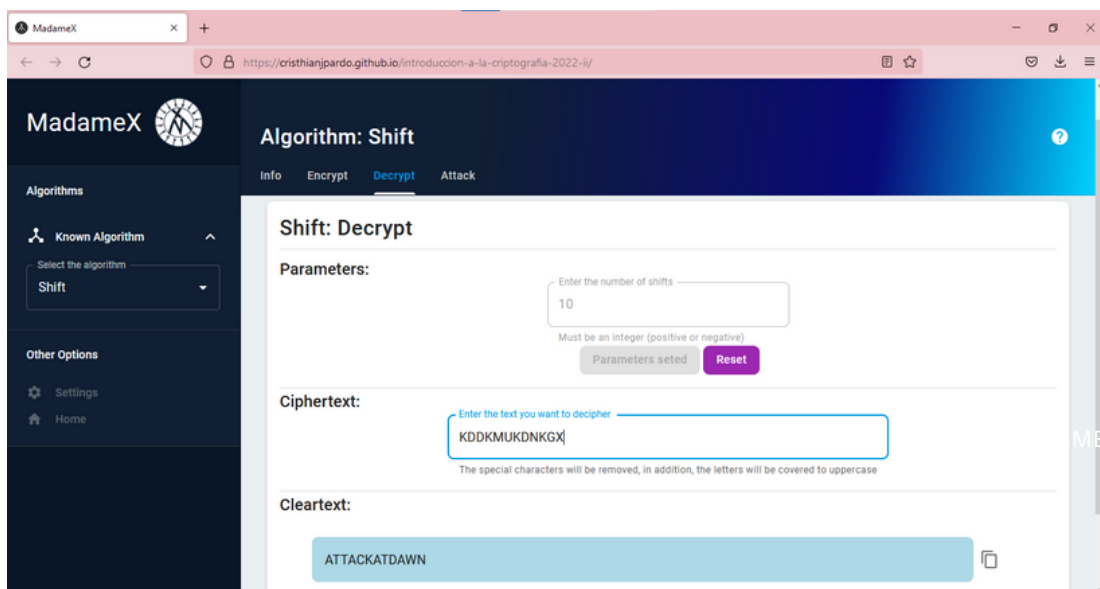


Here you can find summary info about this algorithm, how to encrypt and decrypt whit it. Also you have different enviroments: Encrypt, Decrypt and Attack



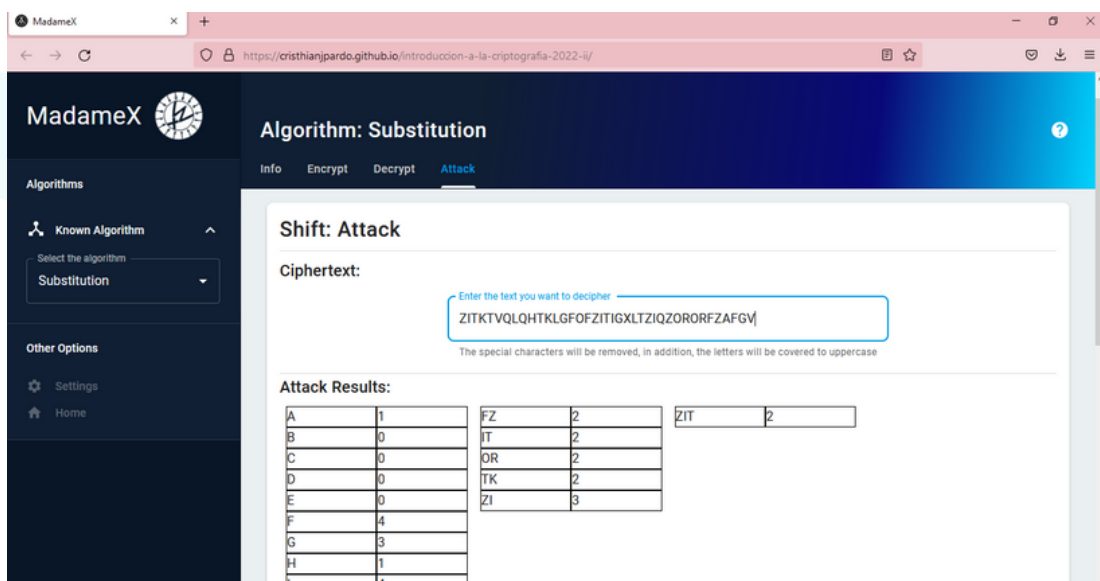
# Decrypt

Here you can find summary info about this algorithm, how to encrypt and decrypt whit it. Also you have different enviroments: Encrypt, Decrypt and Attack



# Attack

Here you can try to decipher a text that used the substitution cipher. Also you have different enviroments: Encrypt, Decrypt and Attack

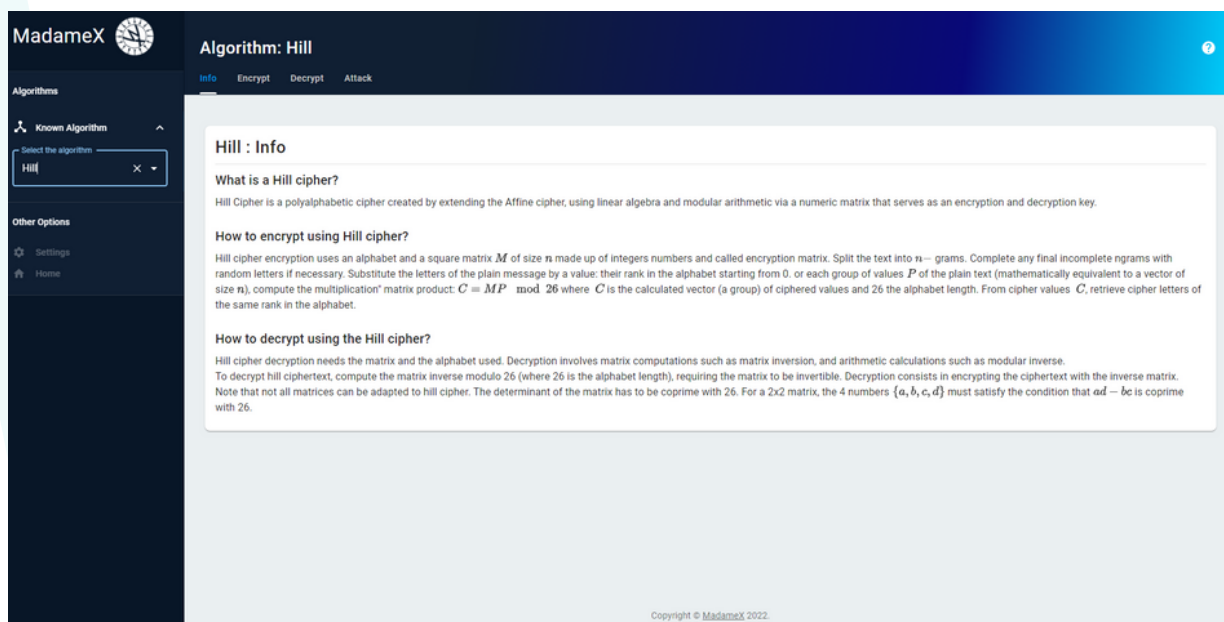


# POLYALPHABETIC

Let's see the poly alphabetic algorithms:

## Hill

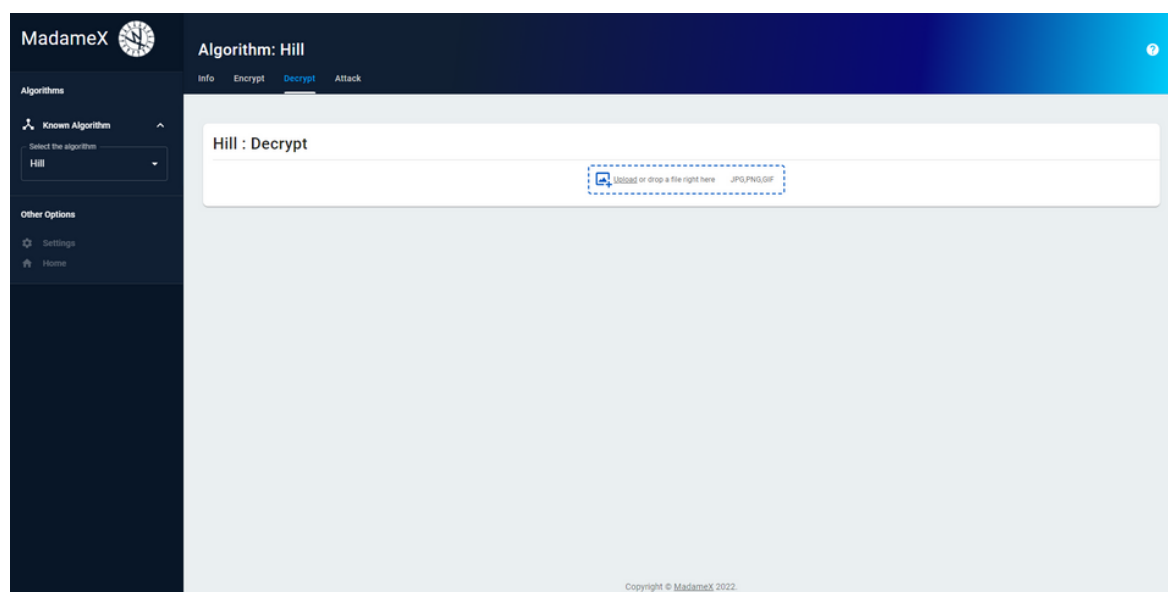
This is what you see when



Here you can find summary info about this algorithm, how to encrypt and decrypt with it. Also you have different environments: Encrypt, Decrypt and Attack

# Encrypt

Here you can find summary info about this algorithm, how to encrypt and decrypt whit it. Also you have different enviroments: Encrypt, Decrypt and Attack

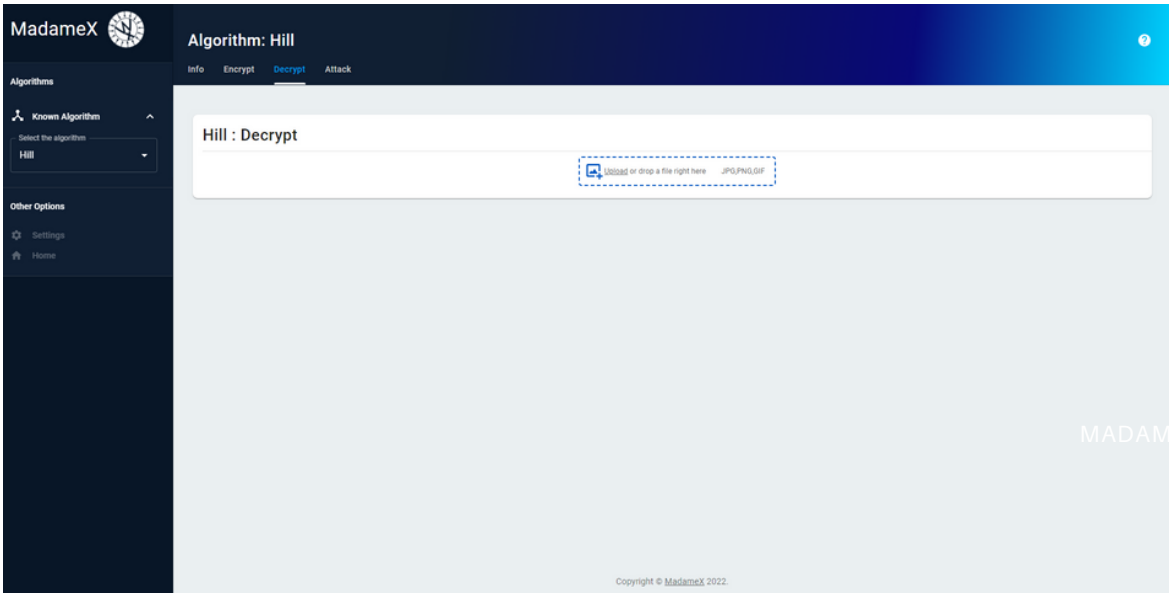


Click on the icon in the center to add the image to be encrypted. This will redirect you to your computer files where you can choose an image.

Note: please note that depending on the size of the selected image the encryption process may take longer.

## Decrypt

It works in a similar way to encryption, just select the image from your computer and it will be decrypted.



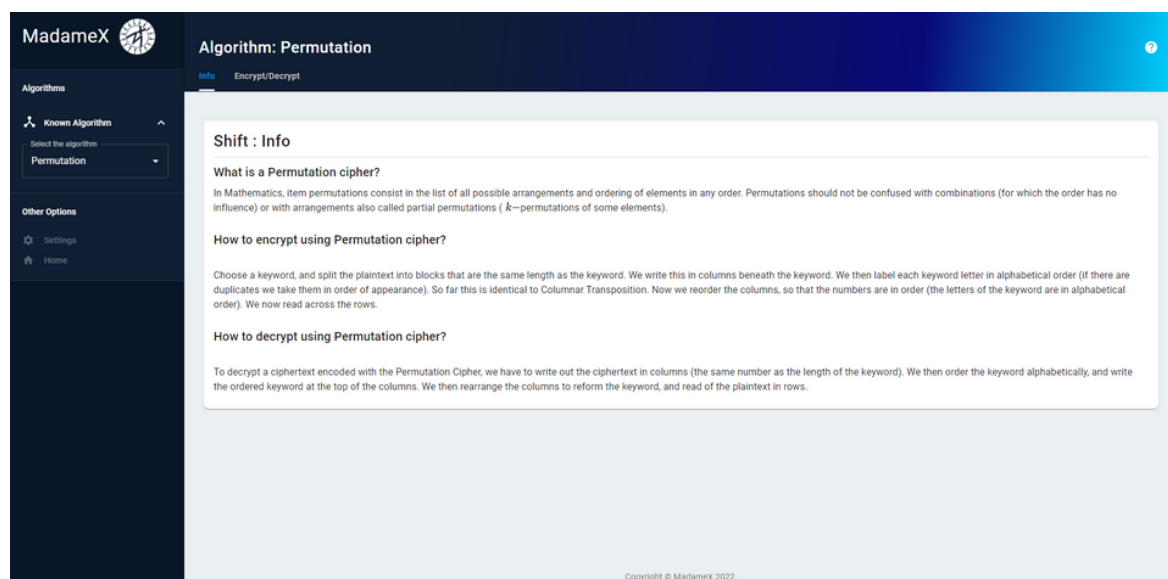
## Attack

At the moment this functionality is not available due to compilation problems. We hope to fix it soon



# Permutation

This is what you see when



Here you can find summary info about this algorithm, how to encrypt and decrypt with it. Also you have different environments: Encrypt, Decrypt and Attack

# Encrypt

Here you can find summary info about this algorithm, how to encrypt and decrypt with it. Also you have different environments: Encrypt, Decrypt and Attack

MadameX

Algorithm: Permutation

Info Encrypt/Decrypt

Algorithms

Known Algorithm

Select the algorithm

Permutation

Other Options

Settings

Home

Permutation: Encrypt

Parameters:

Enter the permutation

Must be a permutation of length between 2 and 6, e.g. 2413

x

xyz

Set parameters Reset

Clear Text:

Enter the text you want to cipher

The special characters will be removed, in addition, the letters will be covered to lowercase

Ciphertext:

Copyright © MadameX 2022.

We enter the permutation written as a sequence of integers whose total length is between 2 and 6. Then we can enter the plaintext to be encrypted like this:

Permutation: Encrypt

Parameters:

Enter the permutation

312456

Must be a permutation of length between 2 and 6, e.g. 2413

x	1	2	3	4	5	6
xyz	3	1	2	4	5	6

Parameters setted Reset

Clear Text:

Enter the text you want to cipher

este es un mensaje oculto

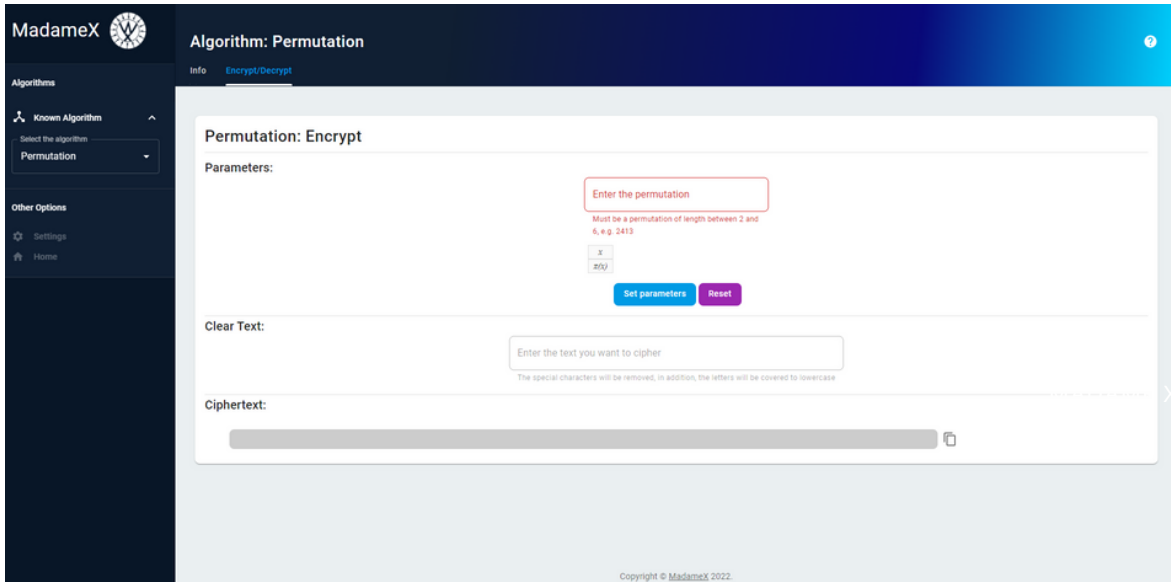
The special characters will be removed, in addition, the letters will be covered to lowercase

Ciphertext:

TESEESMUNENSEAJOCUOLTBKL

# Decrypt

It works in a similar way to encryption, just select the image from your computer and it will be decrypted.



# Attack

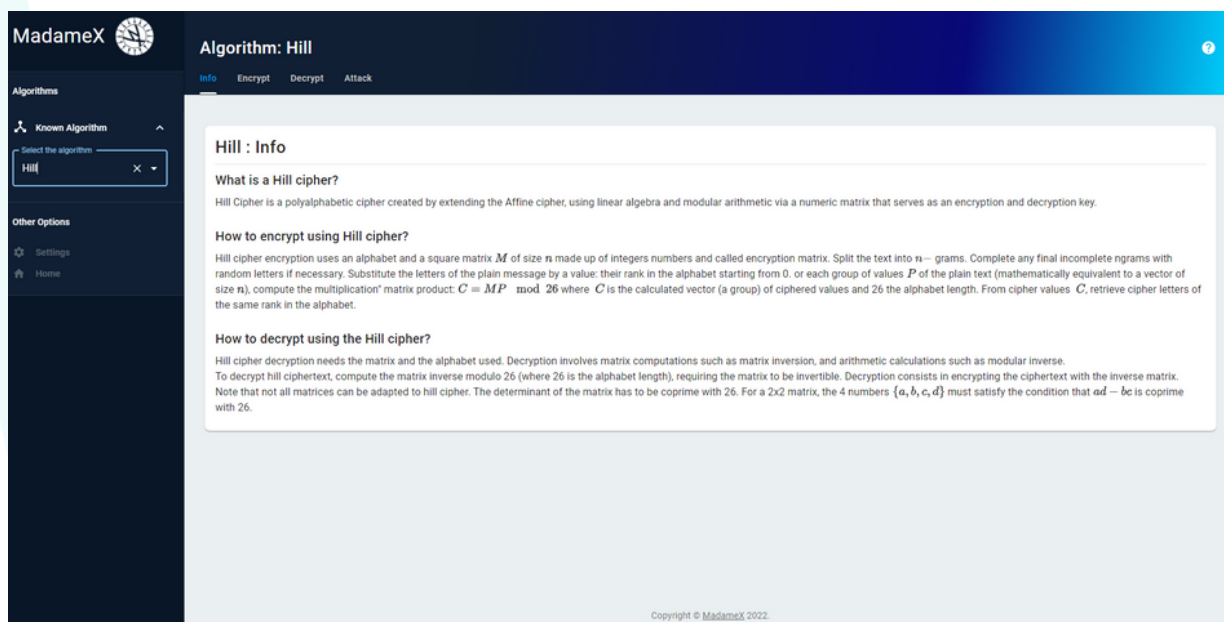
At the moment this functionality is not available due to compilation problems. We hope to fix it soon

# Block ciphers

Let's see the poly alphabetic algorithms:

## AES

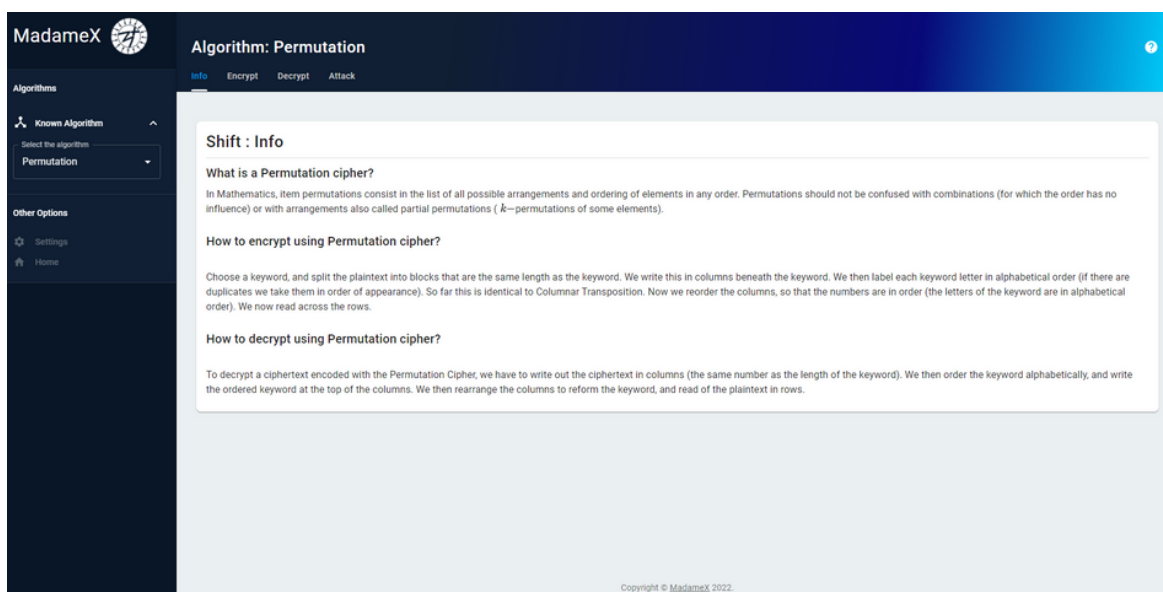
This is what you see when



Here you can find summary info about this algorithm, how to encrypt and decrypt with it. Also you have different environments: Encrypt, Decrypt and Attack

# DES

This is what you see when



Here you can find summary info about this algorithm, how to encrypt and decrypt whit it. Also you have different enviroments: Encrypt, Decrypt and Attack

# Block cryptosystems

Let's see the poly alphabetic algorithms:

## Gamma Pentagonal

This is what you see when

The screenshot shows a web application interface for the Gamma Pentagonal encryption algorithm. It is divided into three main sections on the left and a large grid on the right.

- Punto Inicial:** Contains two input fields for 'X' and 'Y', both set to '0'.
- Permutación:** Contains a text input for 'Permutación' with the value '0, 1, 2, 3, 4, 5, 6, 7, 8, 9'. Below it are two buttons: 'GENERAR PERMUTACIÓN' (blue) and 'APLICAR PERMUTACIÓN' (orange).
- Tipo de Grafo:** Contains two radio buttons: 'Naturales' (selected) and 'Triangulares'. Below them is a blue button labeled 'DIBUJAR GRAFO'.

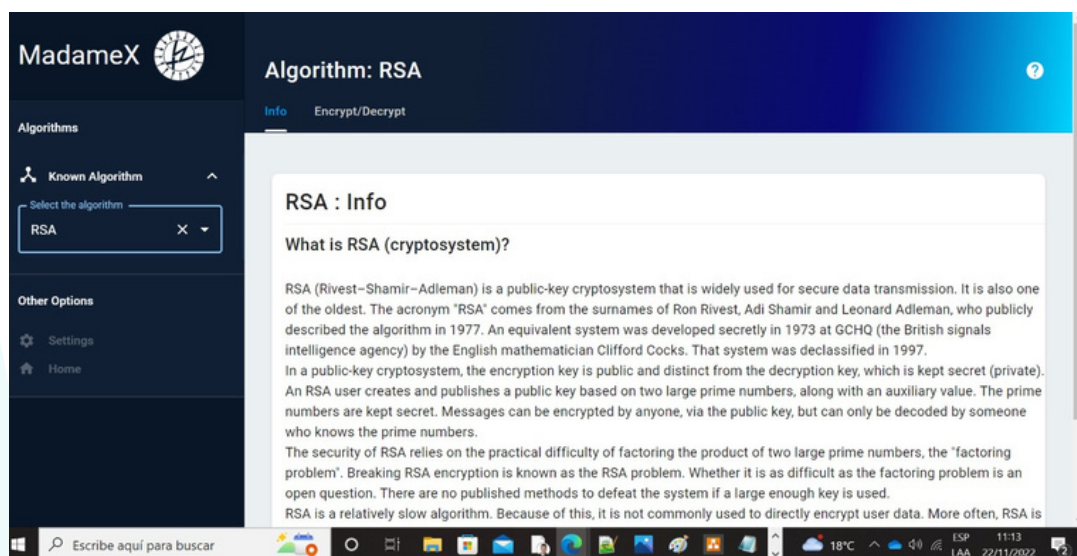
The right side of the interface features a large grid of blue dots. A series of green lines connect the dots in a complex, non-linear pattern, representing the encryption process. At the bottom of the grid, there is a label 'Cifrar con Gamma Pentagonal'.

Here you can find summary info about this algorithm, how to encrypt and decrypt with it. Also you have different environments: Encrypt, Decrypt and Attack

# Public key

Public key algorithms allow us secrecy in public

## RSA

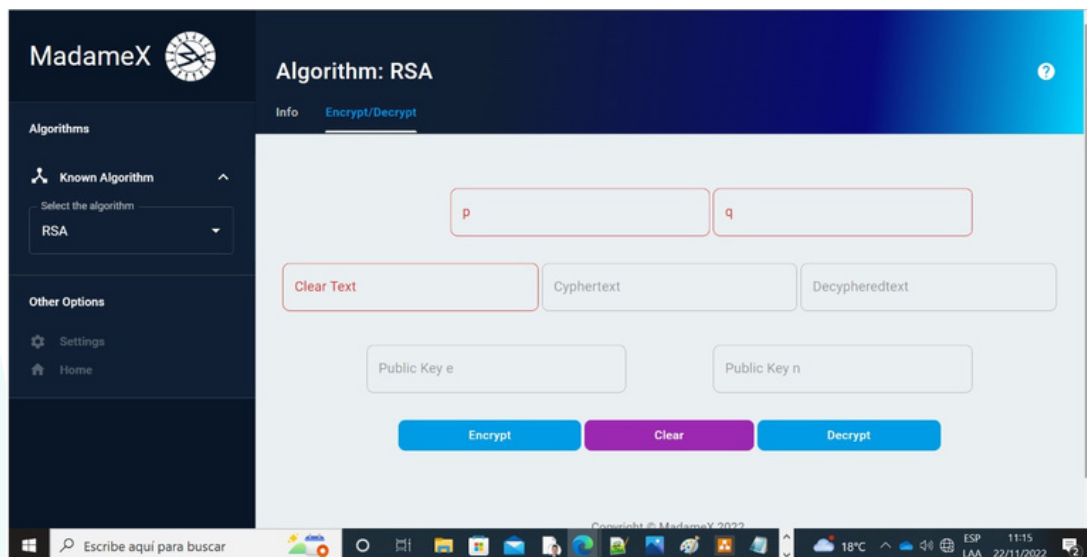


For Rsa encrypting the application returns three number, two are the private keys whereas the third is used as the public key for encryption, we encrypt text by reading the binaries of the characters as we need then this integer to be in the set of mod pq this make us use big private keys i.e big primes, for the moment this are fixed parameters and we recommend maintaining them as primality tests are costly. but the user can insert other primes of his choice.

# Public key

Public key algorithms allow us secrecy in public

## RSA

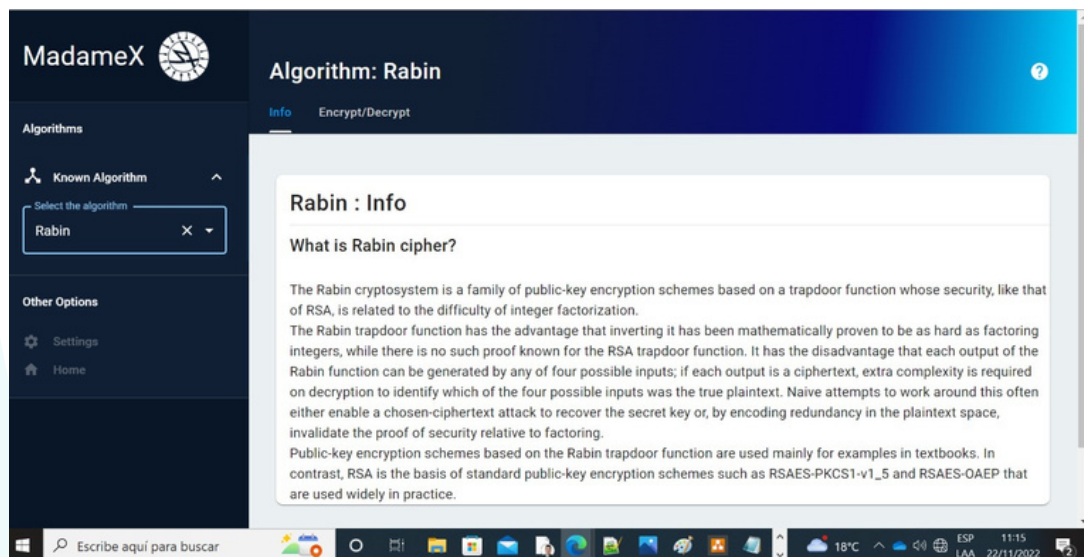


For Rsa encrypting the application returns three number, two are the private keys whereas the third is used as the public key for encryption, we encrypt text by reading the binaries of the characters as we need then this integer to be in the set of mod  $pq$  this make us use big private keys i.e big primes, for the moment this are fixed parameters and we recommend maintaining them as primality tests are costly. but the user can insert other primes of his choice.



# Public key

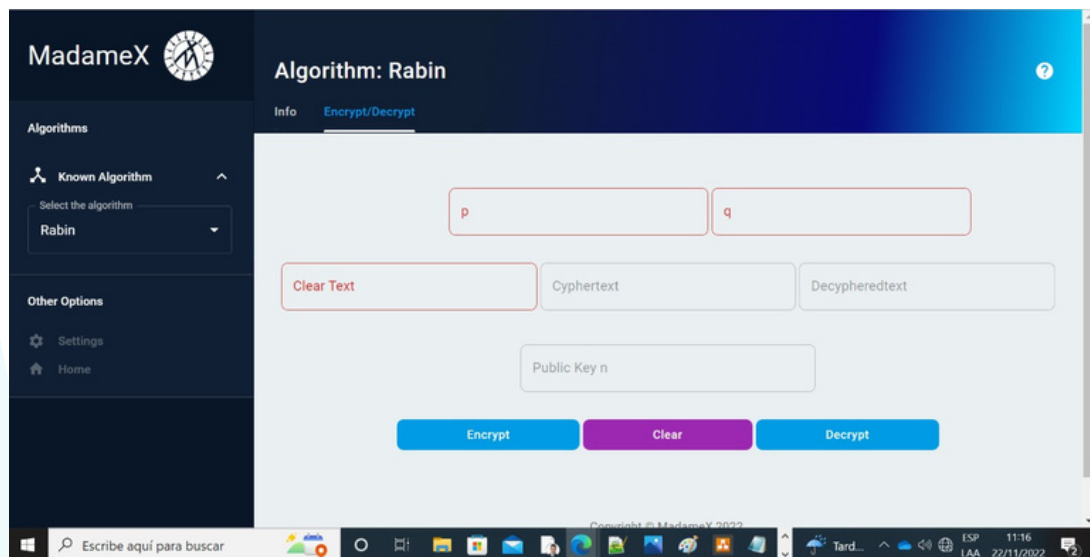
## Rabin



With rabin you can get a proven to be hard decrypting scheme. the regular scheme give us 4 possible decrypted plain text but with redundancy we only give back one of the,.

# Public key

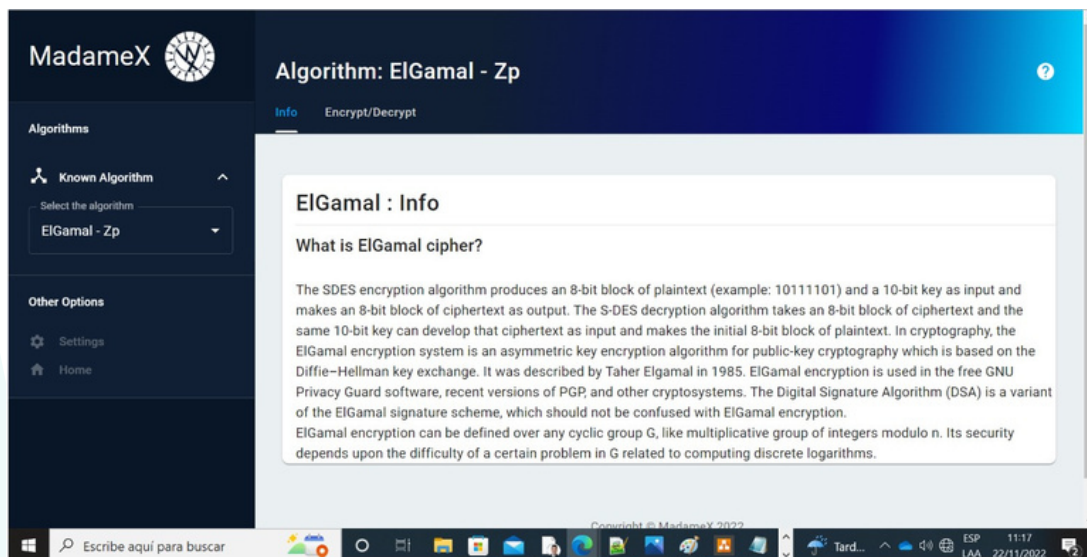
## Rabin



With rabin you can get a proven to be hard decrypting scheme. the regular scheme give us 4 possible decrypted plain text but with redundancy we only give back one of the,.

# Public key

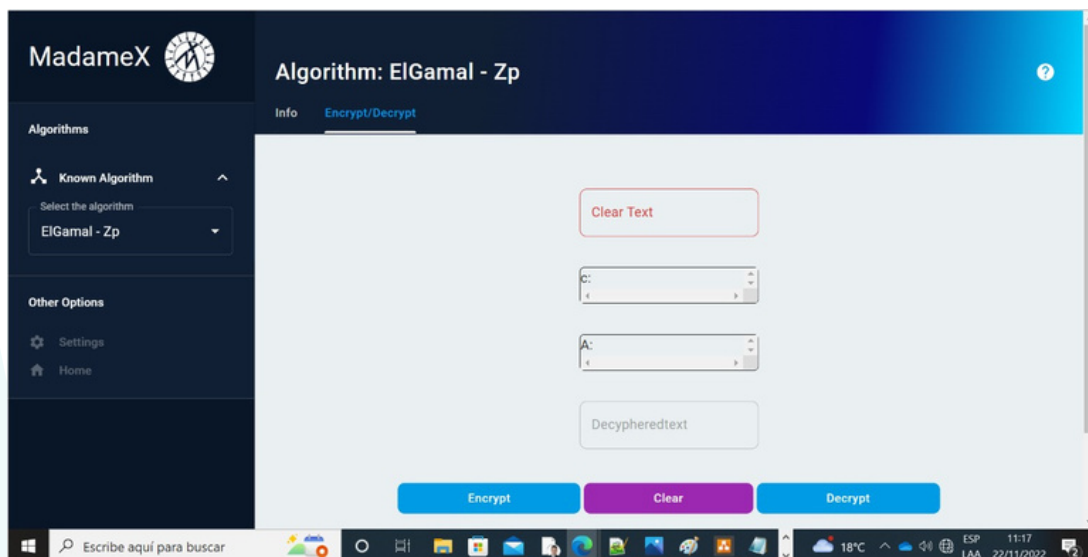
## ElGammal



One of the first implementations of the Diffie Helman protocol ELgammal comes in two flavors, we can choose to use elliptic curves or regular prime fields, elliptic curves although with more complex arithmetic allow us to protect ourselves from logarithm tables as they would be infeasible to create for users

# Public key

## ElGammal



One of the first implementations of the Diffie Helman protocol ELgammal comes in two flavors, we can choose to use elliptic curves or regular prime fields, elliptic curves although with more complex arithmetic allow us to protect ourselves from logarithm tables as they would be infeasible to create for users

## References

- [1] *Agnes Meyer Driscoll, criptoanalista. (2014, July 24). Mujeres con ciencia.* <https://mujeresconciencia.com/2014/07/24/agnes-meyer-driscoll-criptoanalista/>
- [2] *Web components - react. (n.d.).* Retrieved 13 September 2022, from <https://es.reactjs.org/docs/web-components.html>
- [3] *Github pages documentation. (n.d.).* GitHub Docs. Retrieved 13 September 2022, from <https://ghdocs-prod.azurewebsites.net/en/pages>
- [4] *Stallings, W. (2017). Cryptography and network security: Principles and practice (Seventh edition).* Pearson.