UNIVERSIDAD NACIONAL DE COLOMBIA - 2022

MADAME X

MANUAL

Developed by:

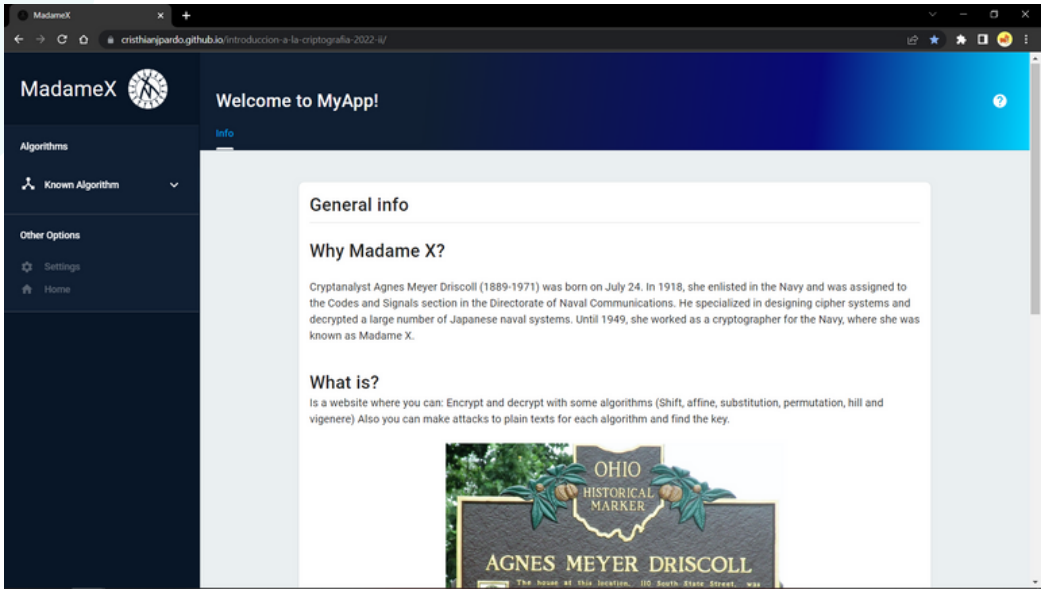
CRISTHIAN PARDO
TANIA CASTILLO
GABRIEL QUINCHE
JUAN LARA

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

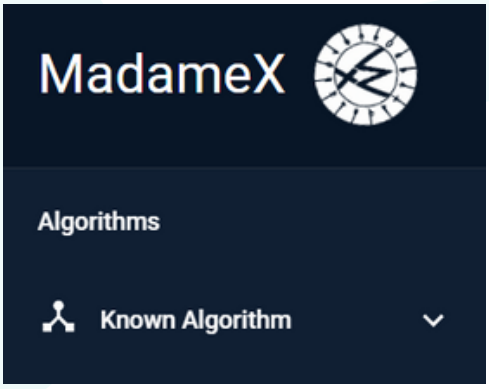
This is the first page that you can see:



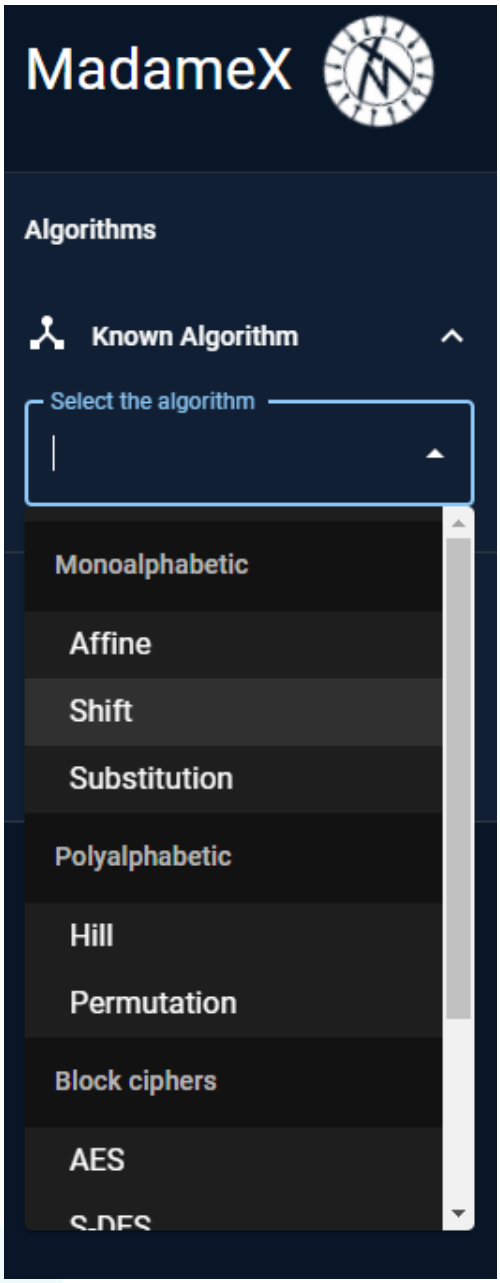
Here you can find a short description of this project, the answers of questions like why Madame X? or whats it this about.

Algorithms

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



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



MONOALPHABETICS

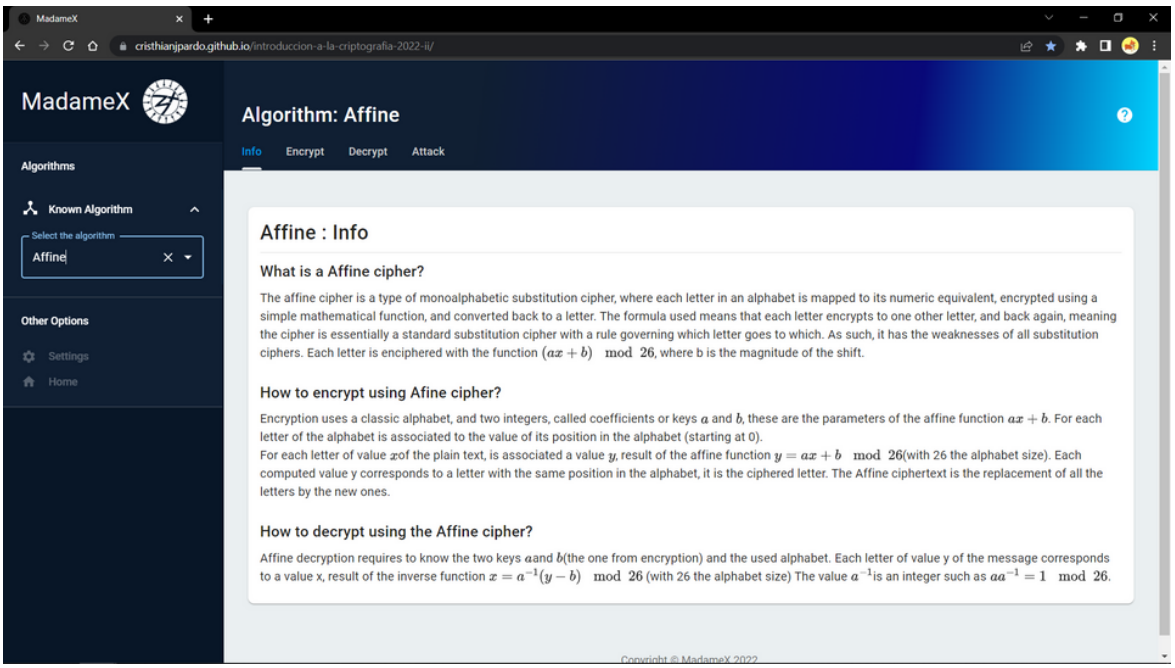
In the algorithms you see two sections:

Monoalphabetic and Polyalphabetics

Let's see the monoalphabetic algorithms:

Affine

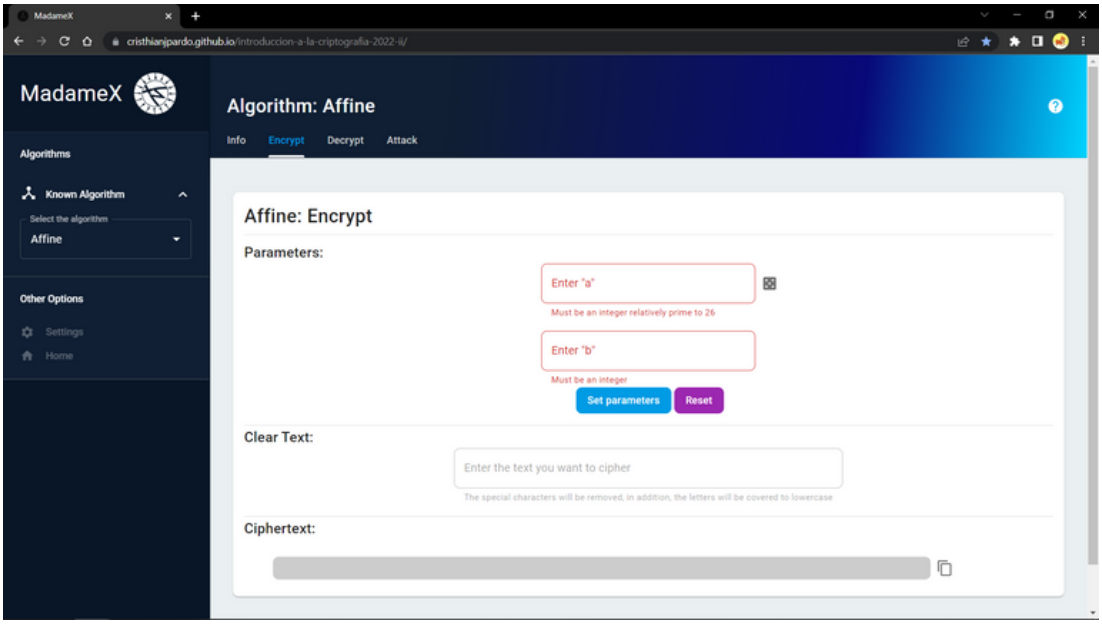
This is what you see when



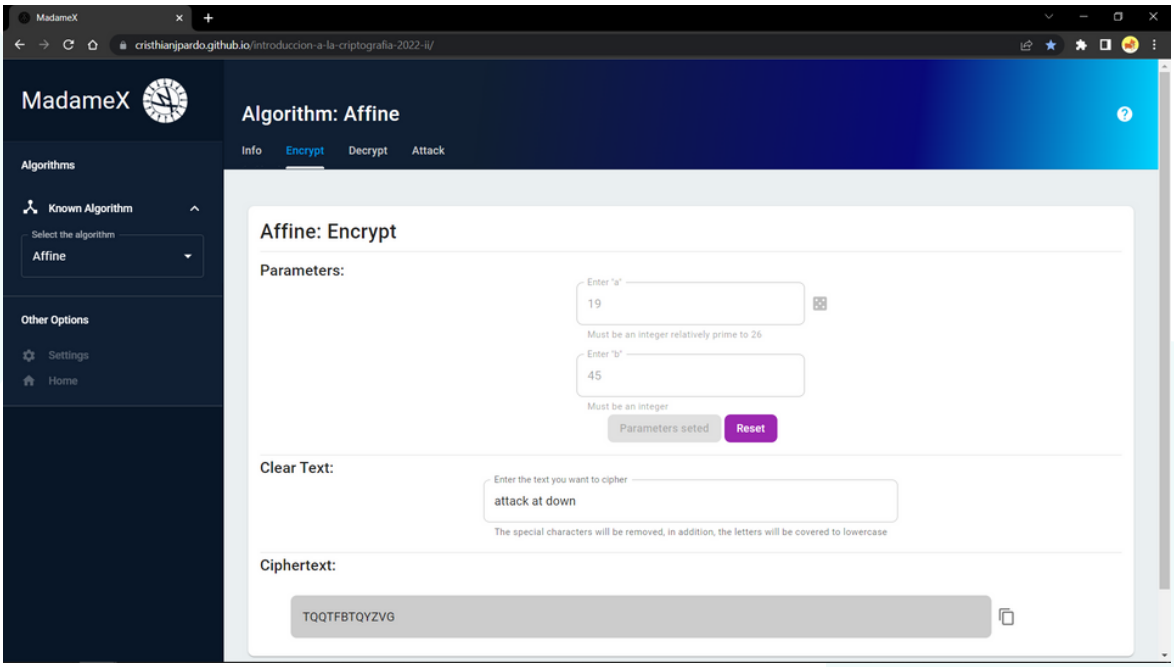
Here you can find summary info about this algorithm, how to encrypt and decrypt whit it. Also you have different enviroments: Encrypt, Decrypt and Attack

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.

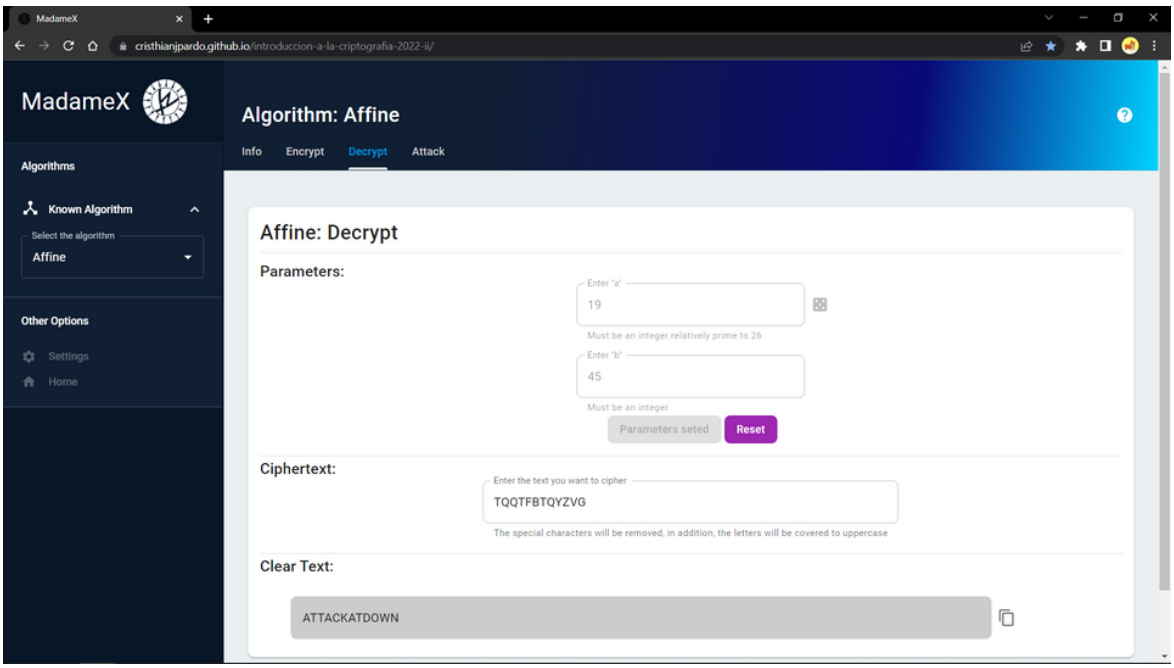


Once you already set the parameters you can encrypt a plain text that you write in "Clear text" box and in real time you'll see the cipher text below. Additional you can copy that text click on the copy button at the right of the grey box.



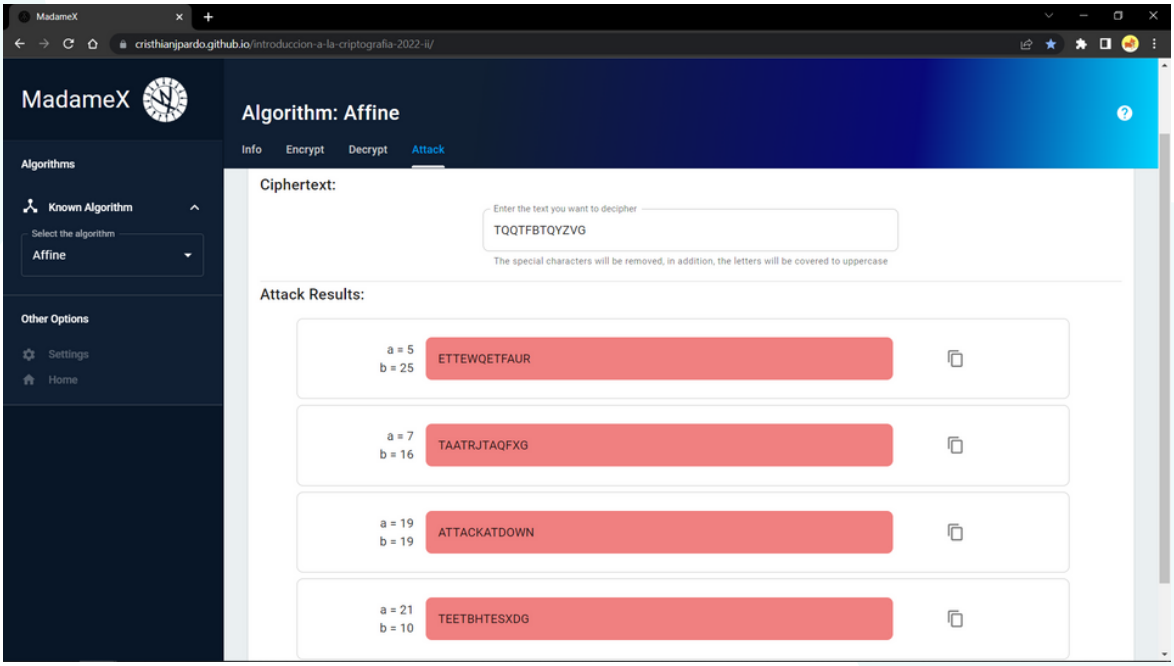
Decrypt

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



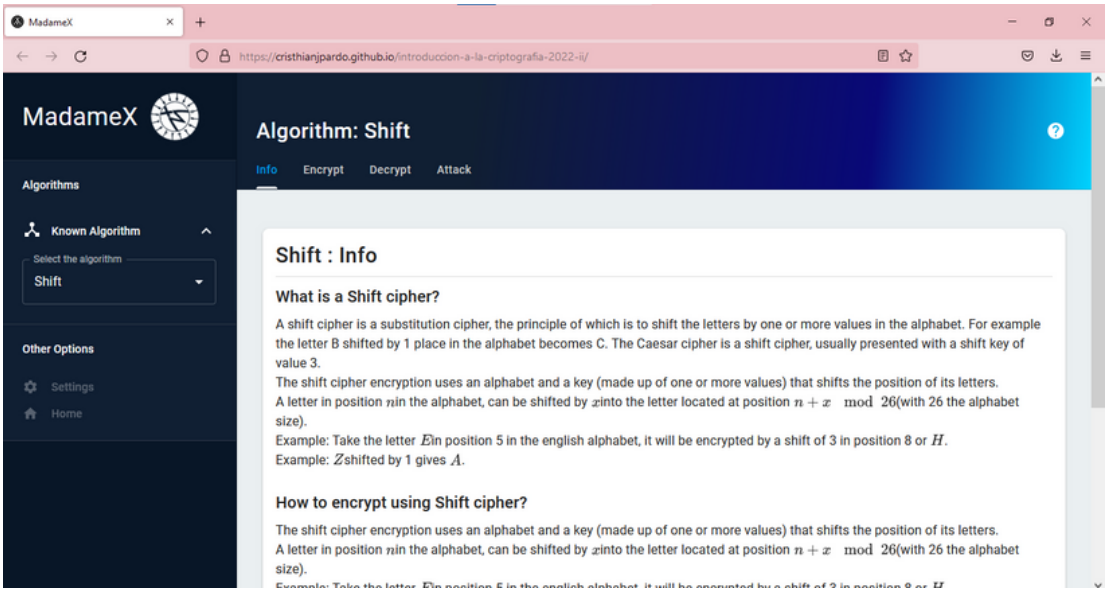
Attack

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



Shift

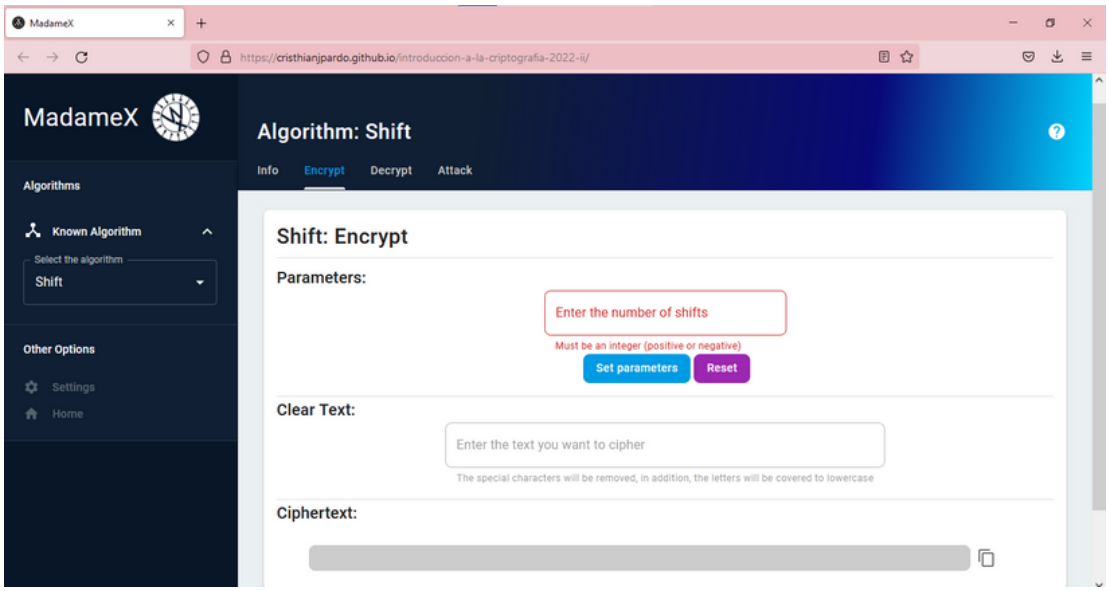
This is what you see when



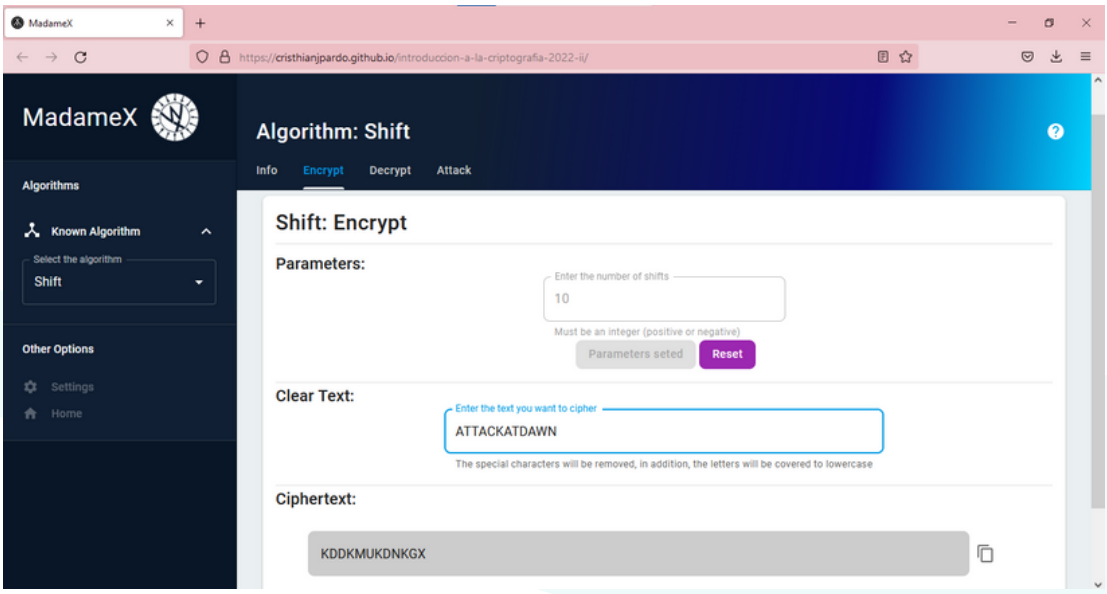
Here you can find summary info about this algorithm, how to encrypt and decrypt whit it. Also you have different enviroments: Encrypt, Decrypt and Attack

Encrypt

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

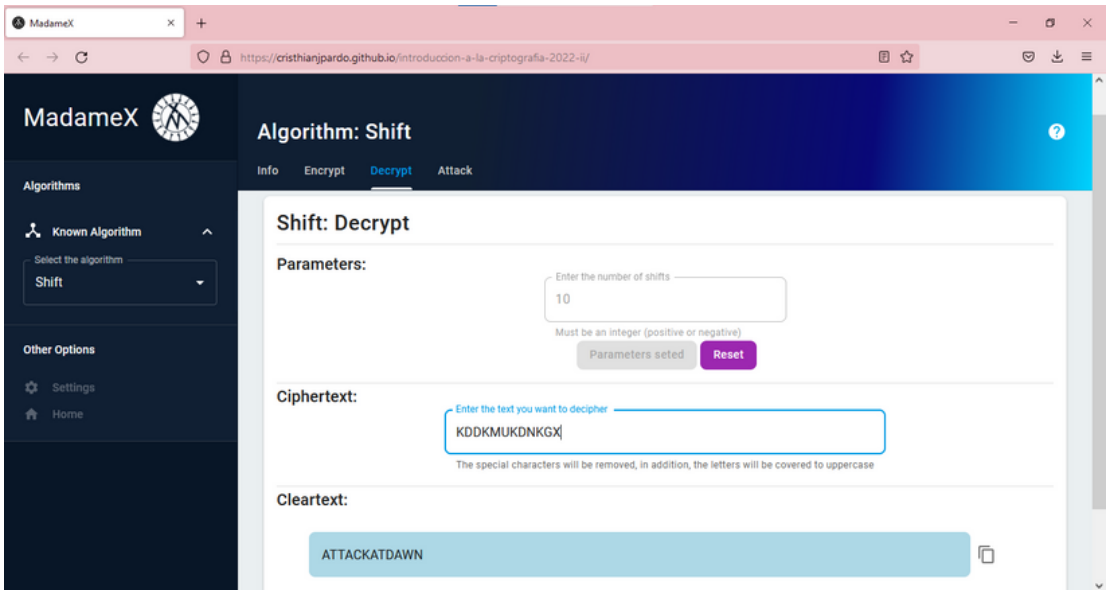


Here you can find summary info about this algorithm, how to encrypt and decrypt whit it. Also you have different enviroments: Encrypt, Decrypt and Attack



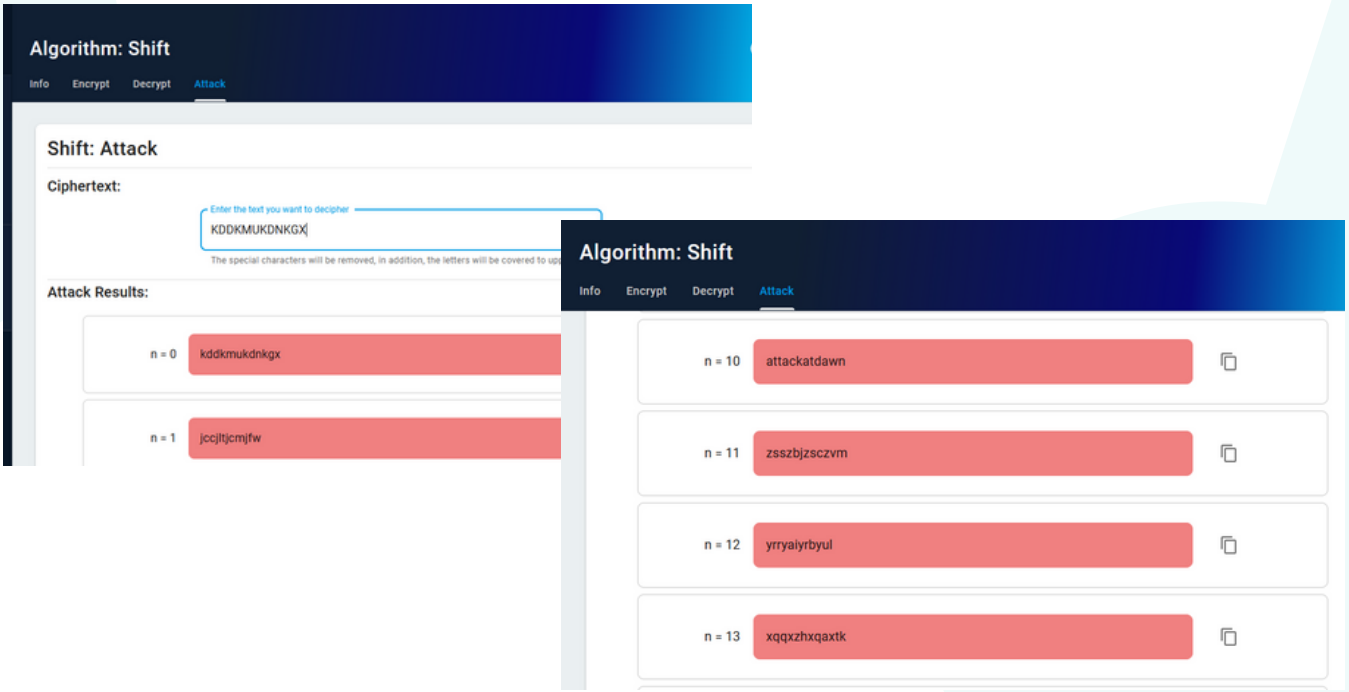
Decrypt

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



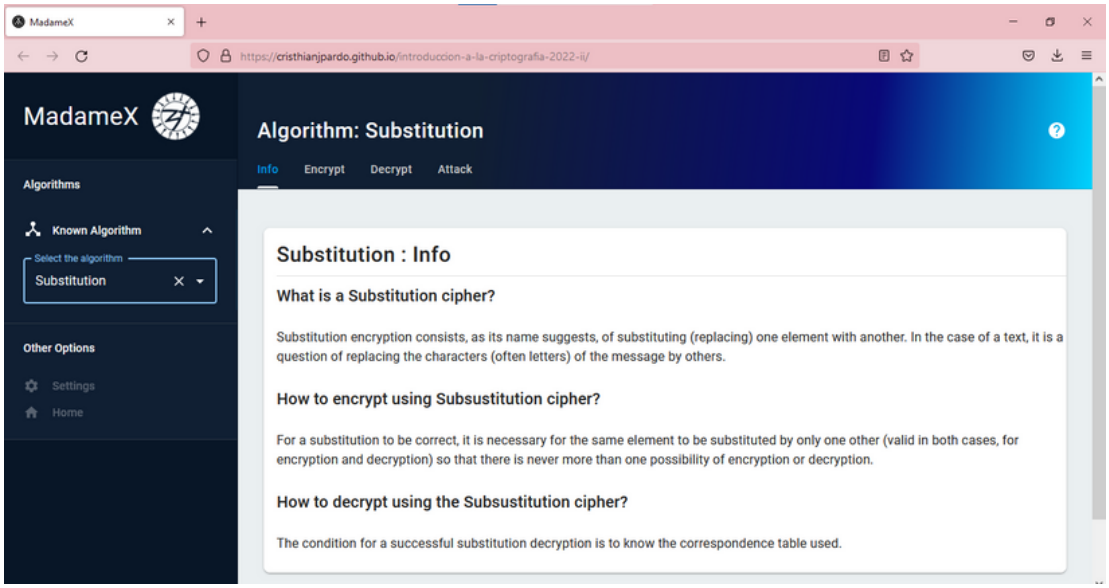
Attack

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



Substitution

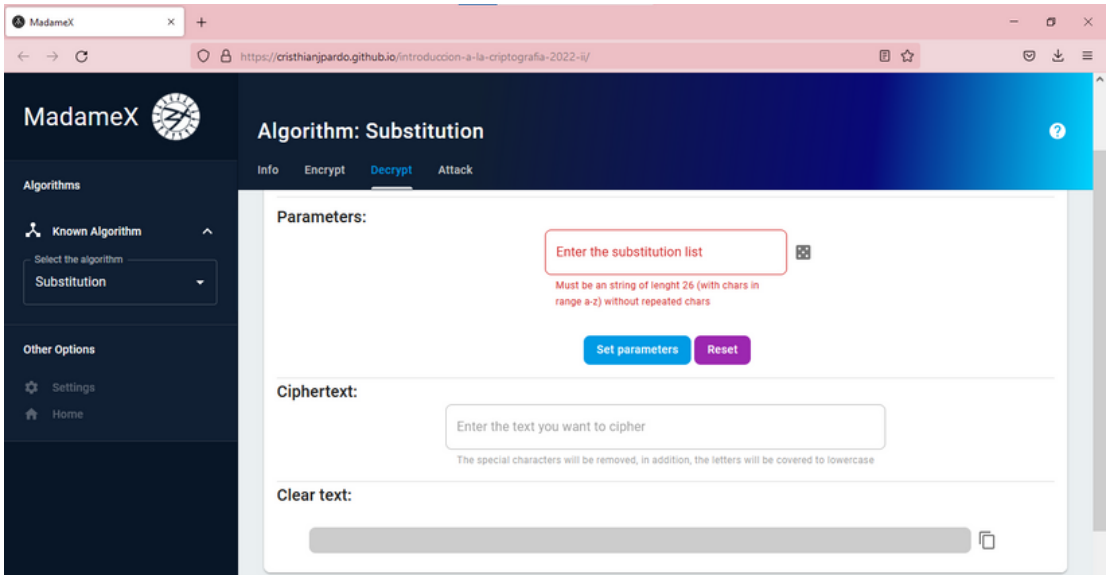
This is what you see when



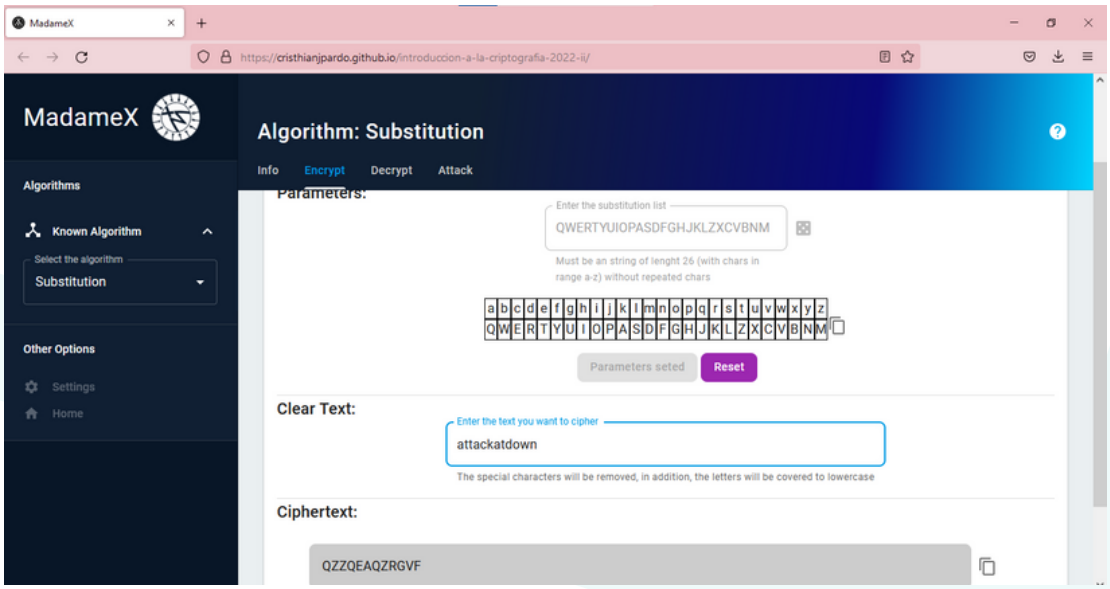
Here you can find summary info about this algorithm, how to encrypt and decrypt whit it. Also you have different enviroments: Encrypt, Decrypt and Attack

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

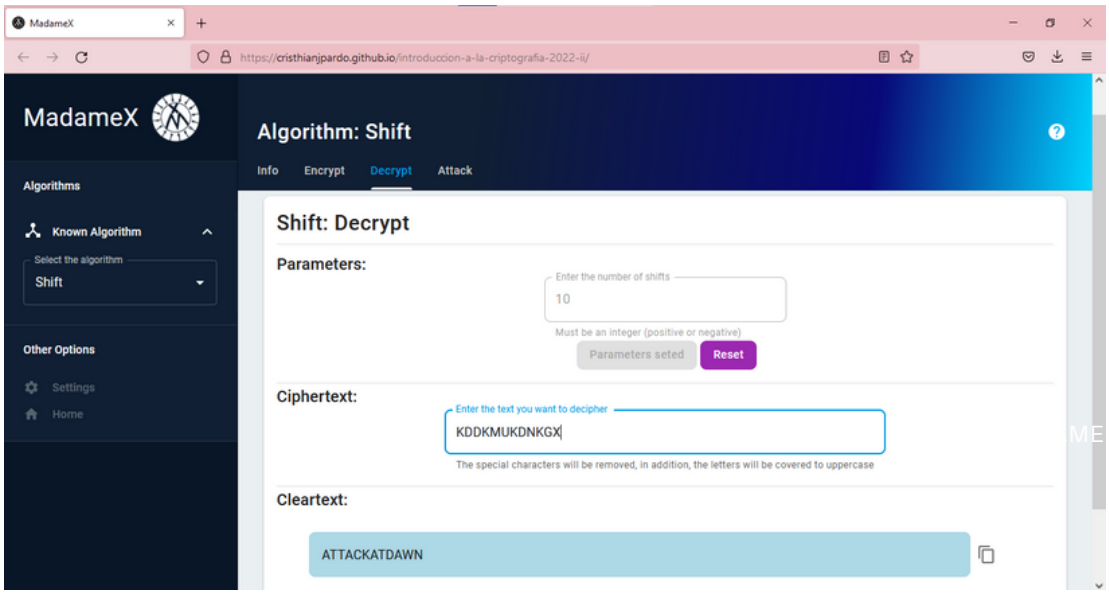


Here you can find summary info about this algorithm, how to encrypt and decrypt whit it. Also you have different enviroments: Encrypt, Decrypt and Attack



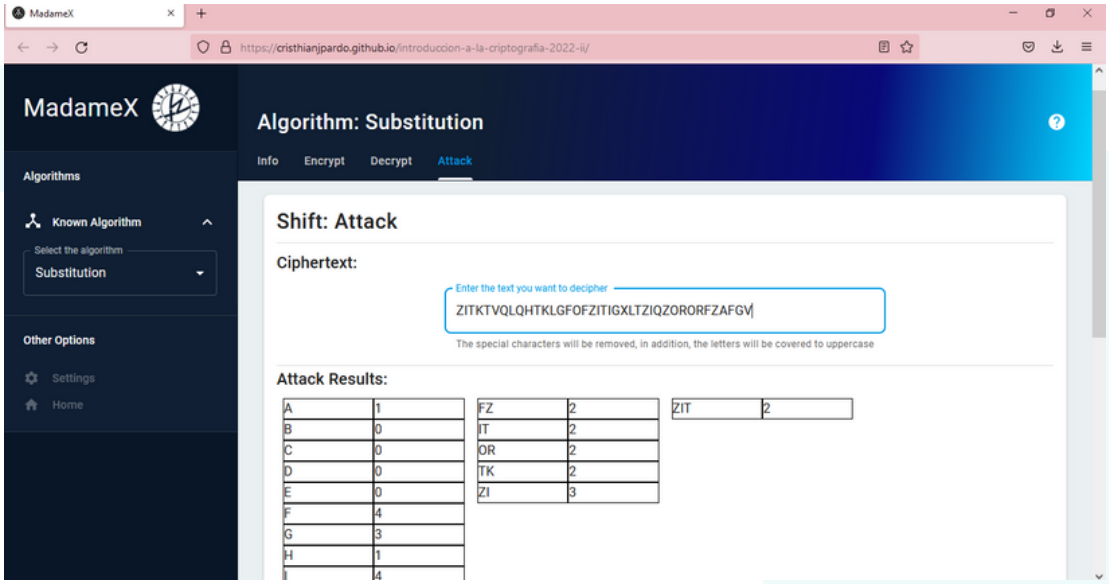
Decrypt

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

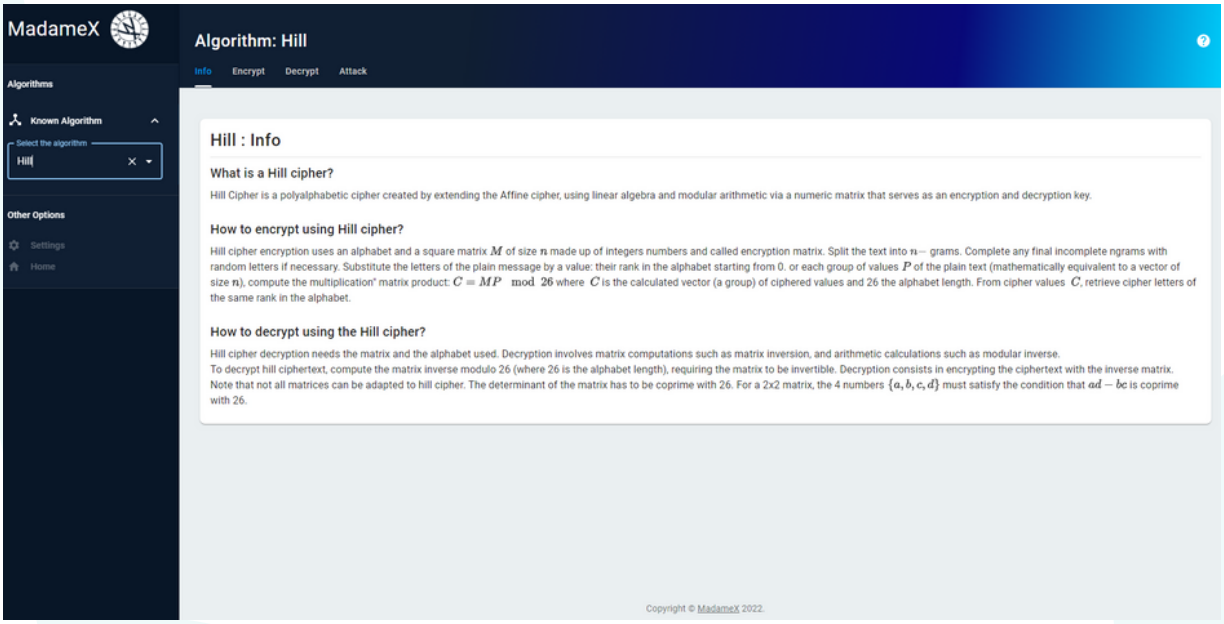


POLYALPHABETIC

Let's see the poly alphabetic algorithms:

Hill

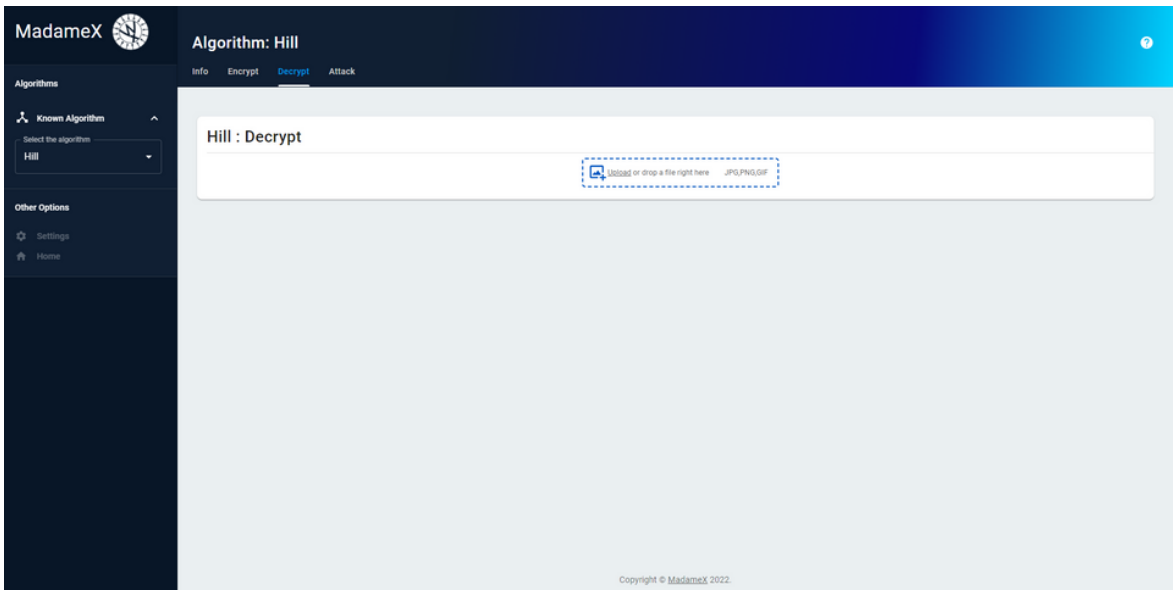
This is what you see when



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

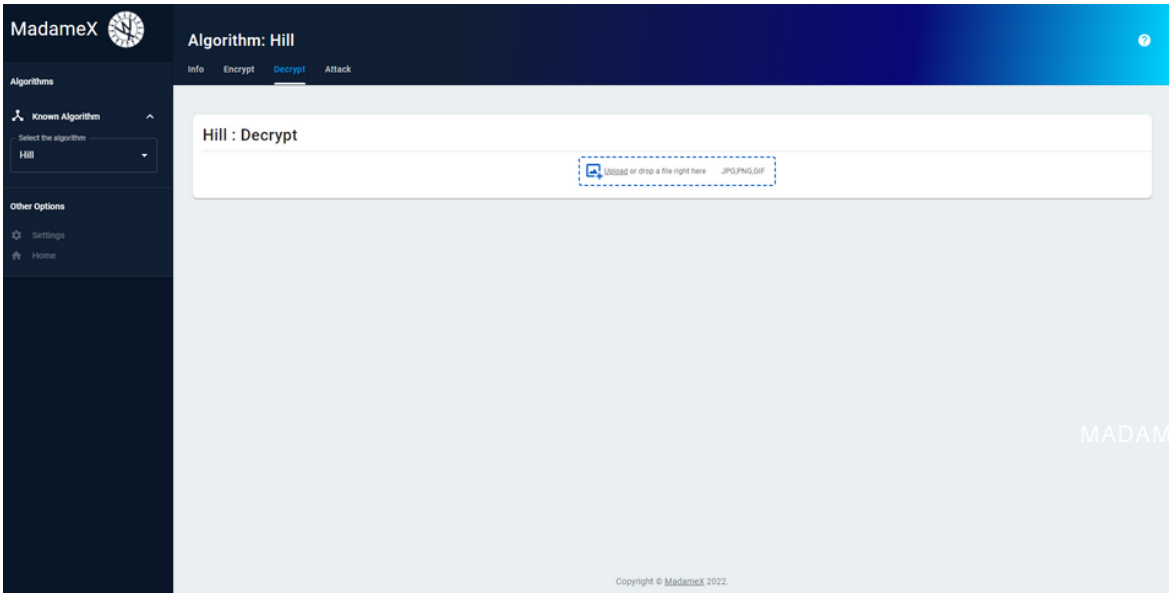


Click on the icon in the center to add the image to be encrypted. This will redirect you to your computer files where you can choose an image.

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.

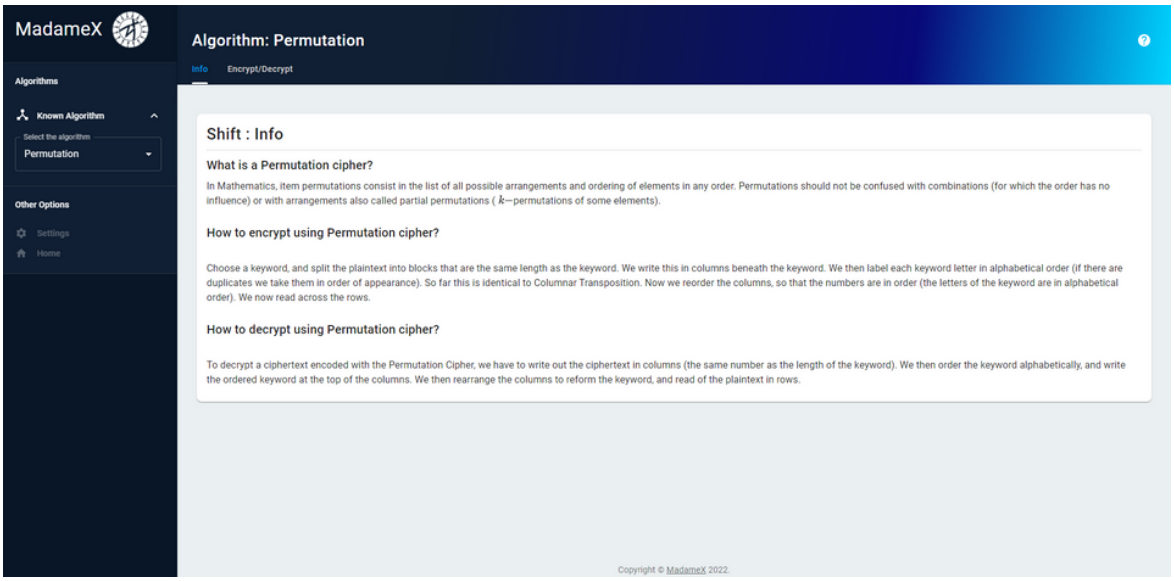


Attack

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

Permutation

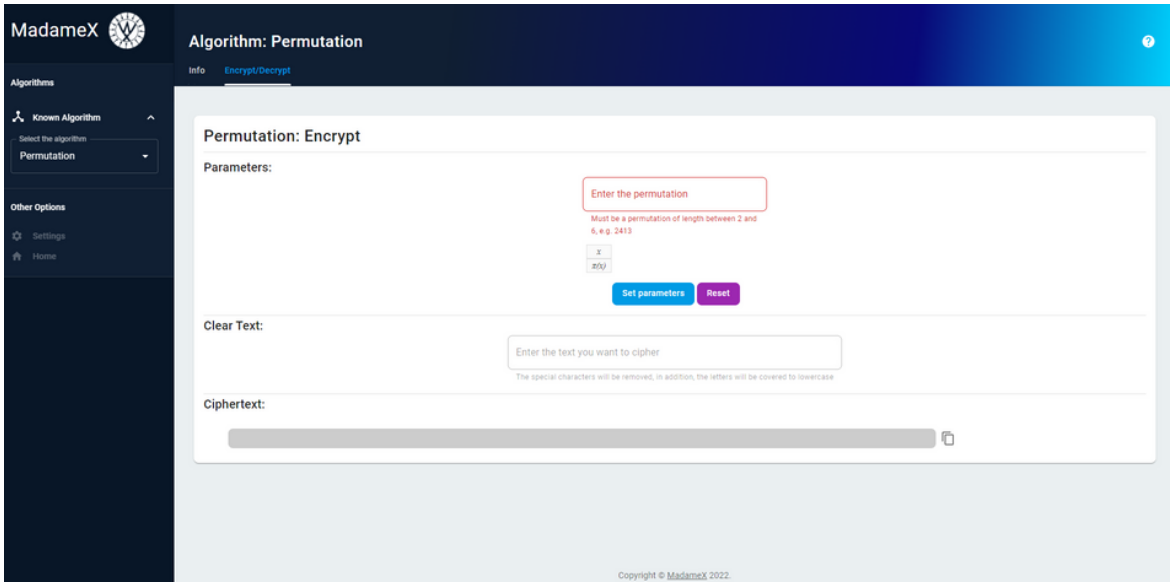
This is what you see when



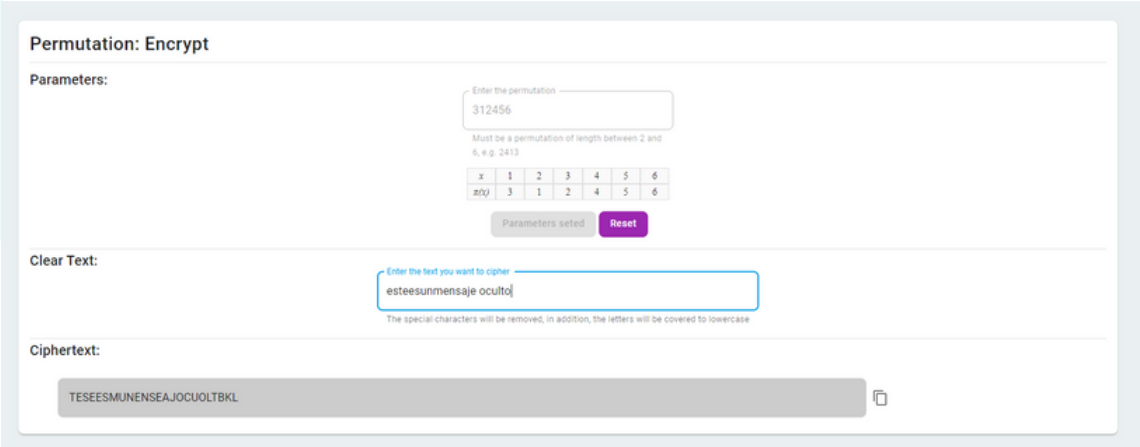
Here you can find summary info about this algorithm, how to encrypt and decrypt whit it. Also you have different enviroments: Encrypt, Decrypt and Attack

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

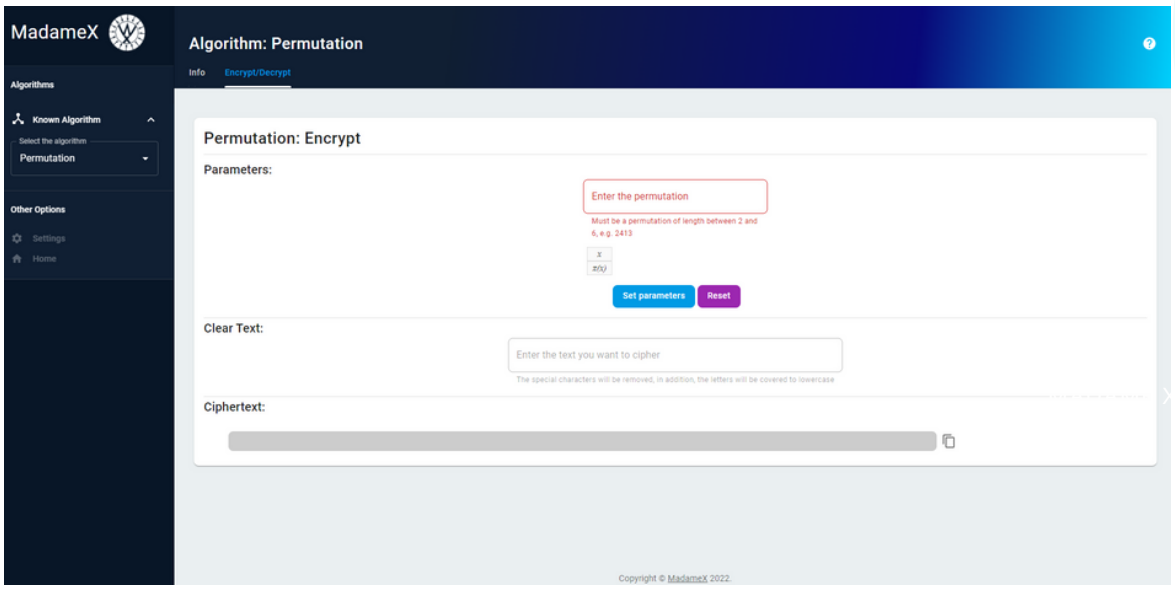


We enter the permutation written as a sequence of integers whose total length is between 2 and 6. Then we can enter the plaintext to be encrypted like this:



Decrypt

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



Attack

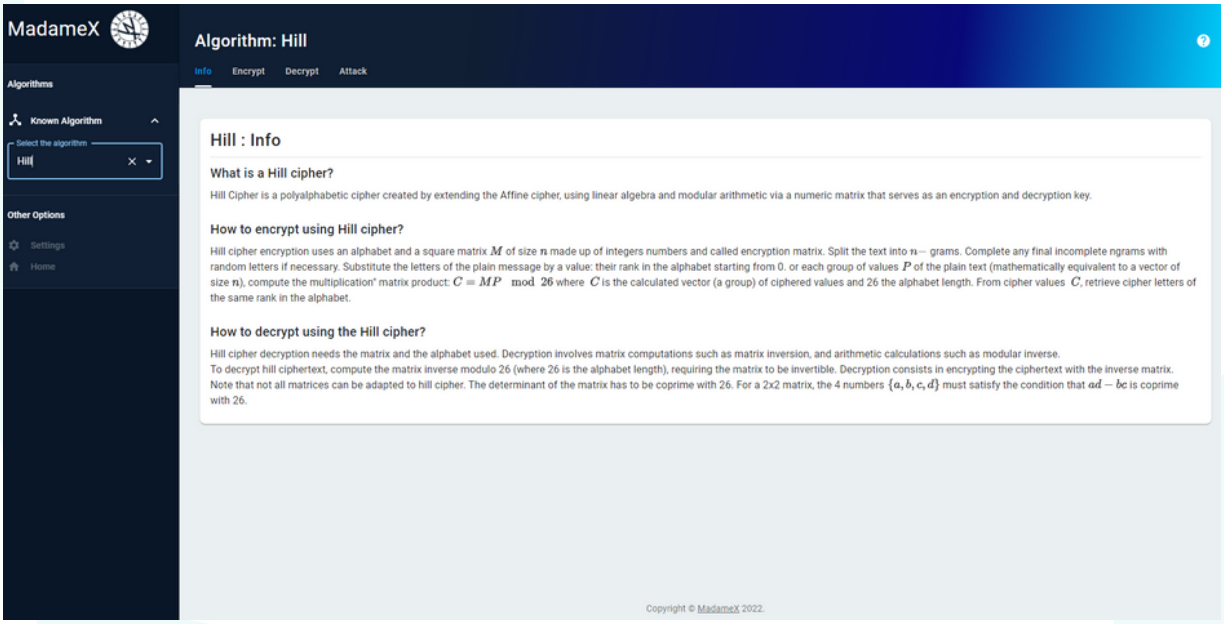
At the moment this functionality is not available due to compilation problems. We hope to fix it soon

Block ciphers

Let's see the poly alphabetic algorithms:

AES

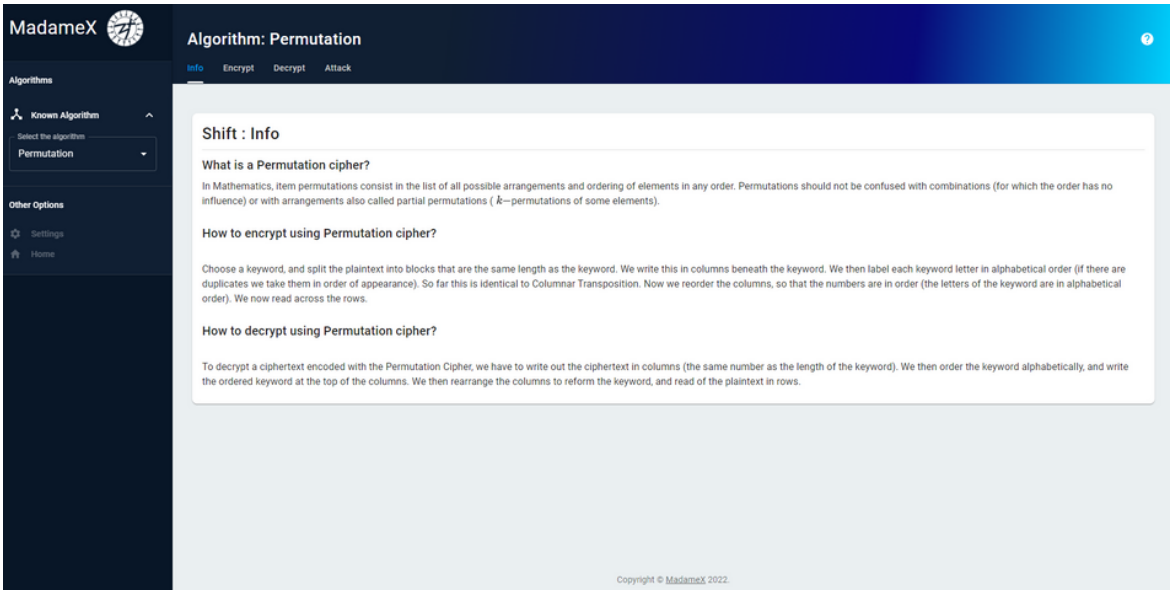
This is what you see when



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

DES

This is what you see when



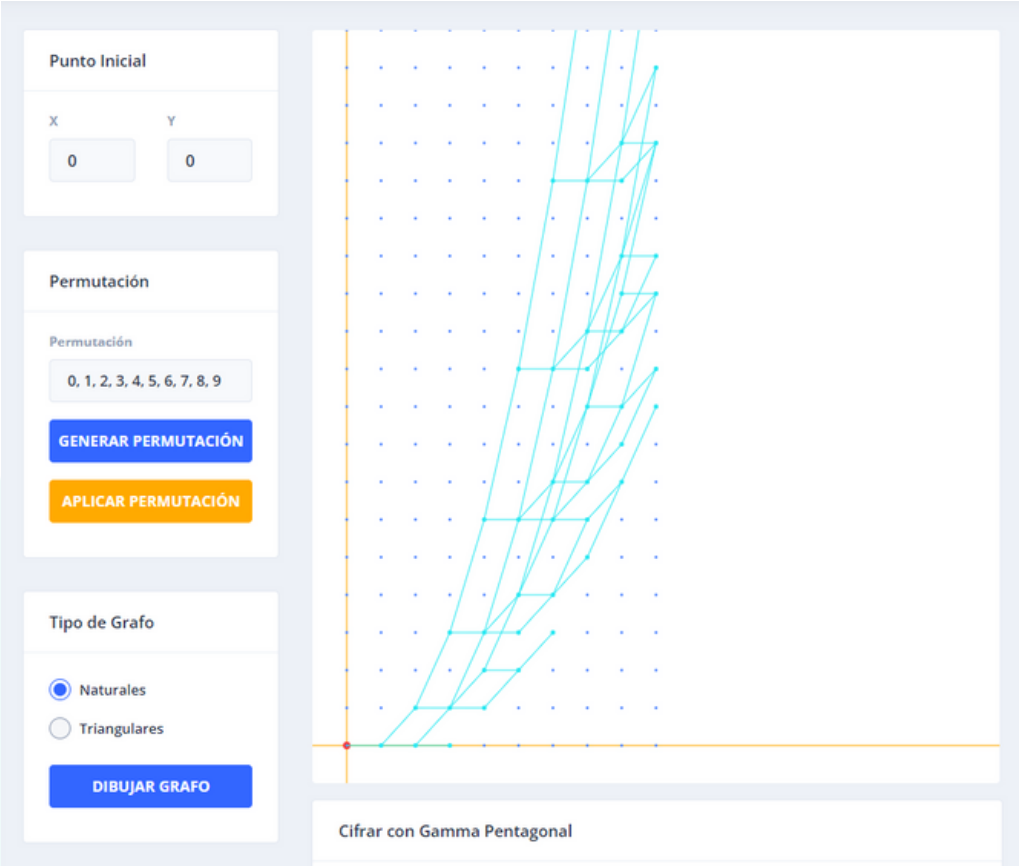
Here you can find summary info about this algorithm, how to encrypt and decrypt whit it. Also you have different enviroments: Encrypt, Decrypt and Attack

Block cryptosystems

Let's see the poly alphabetic algorithms:

Gamma Pentagonal

This is what you see when

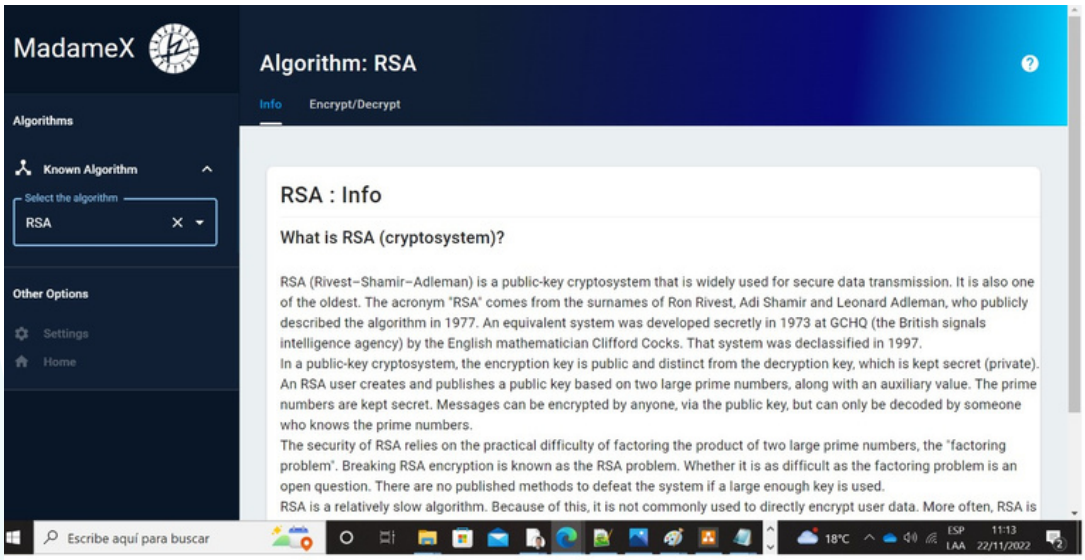


Here you can find summary info about this algorithm, how to encrypt and decrypt whit it. Also you have different enviroments: Encrypt, Decrypt and Attack

Public key

Public key algorithms allow us secrecy in public

RSA

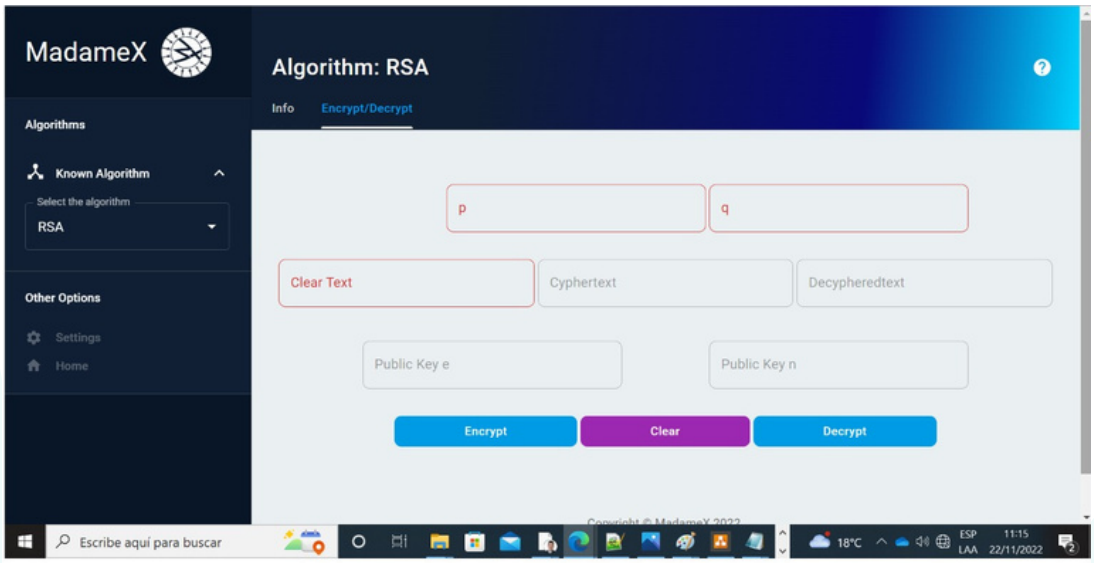


For Rsa encrypting the application returns three number, two are the private keys whereas the third is used as the public key for encryption, we encrypt text by reading the binaries of the characters as we need then this integer to be in the set of mod pq this make us use big private keys i.e big primes, 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

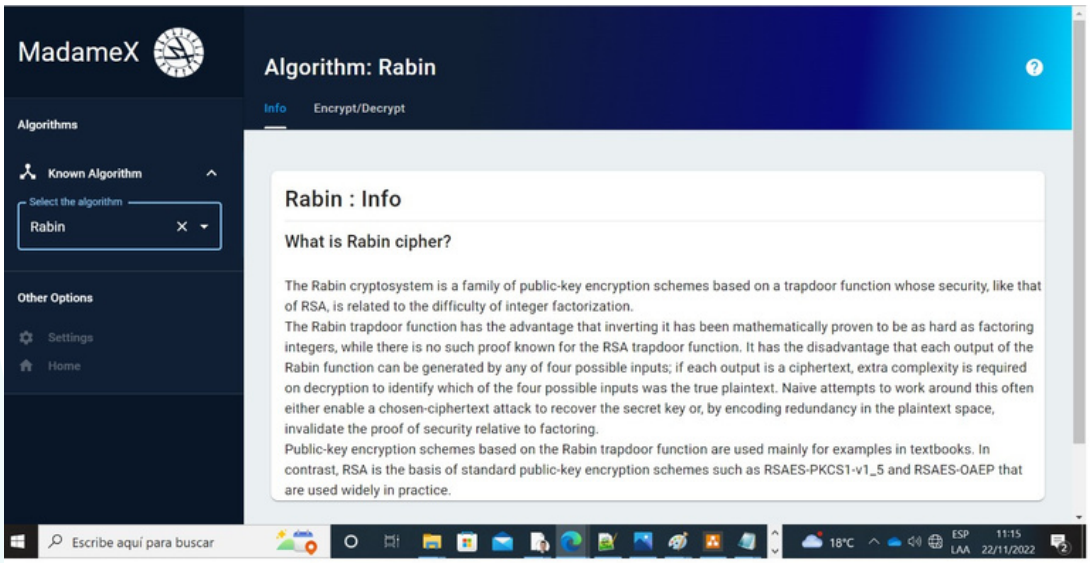
RSA



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

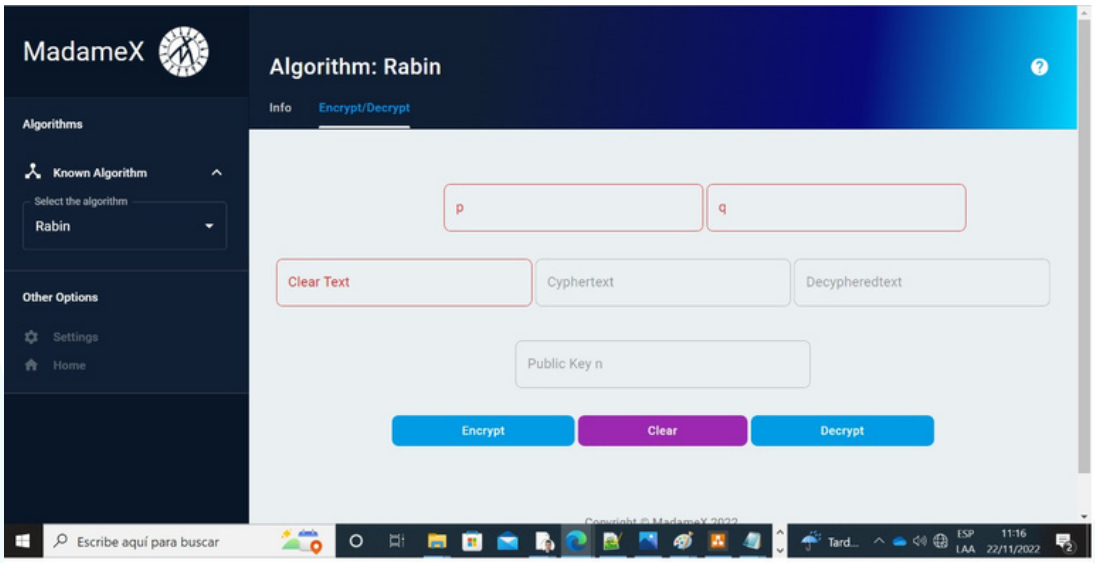
Rabin



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

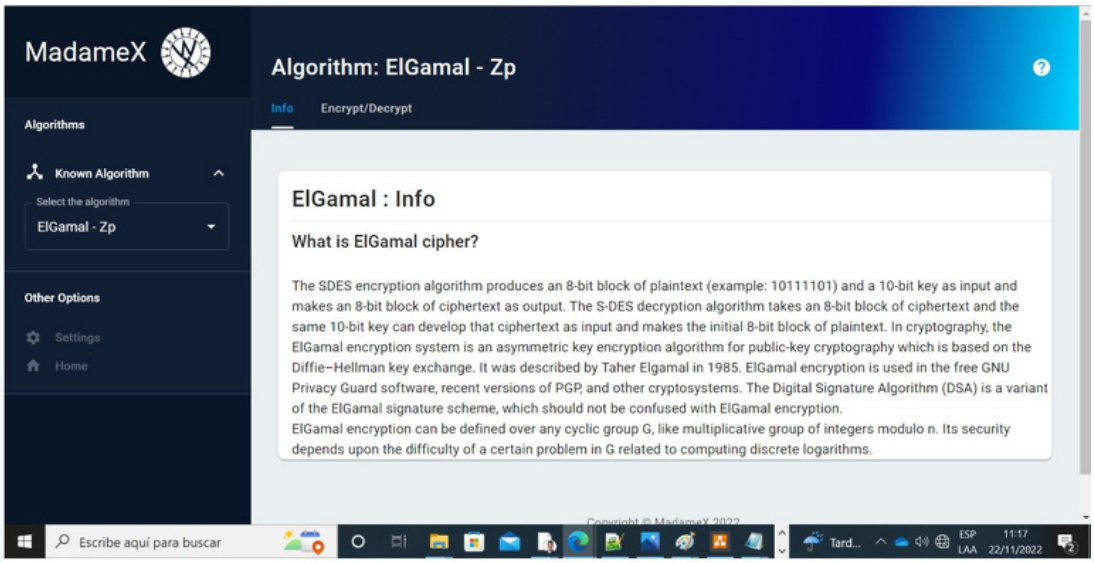
Rabin



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

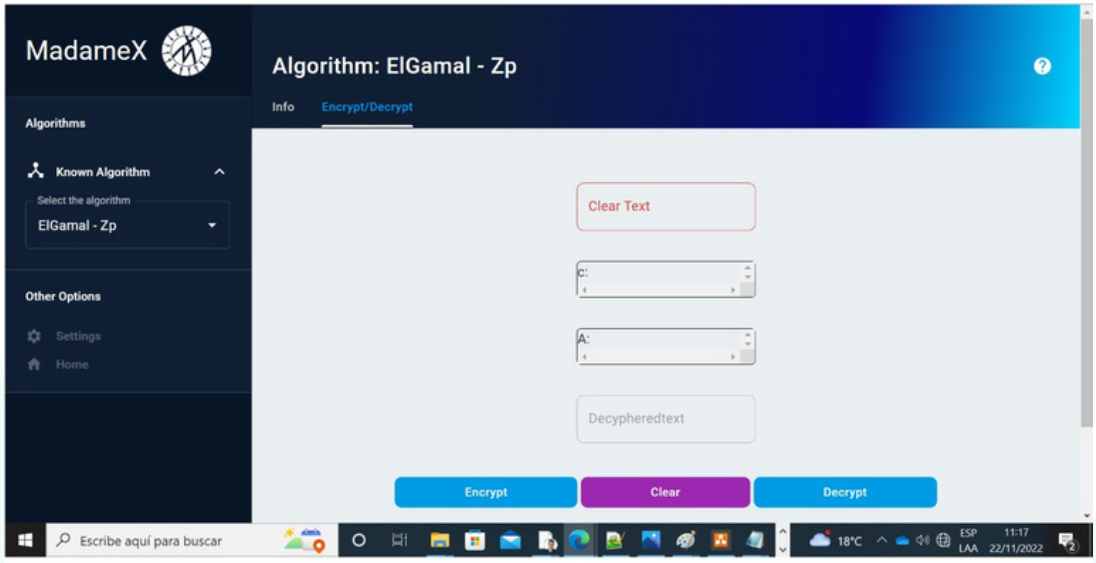
ElGammal



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 aritmethic 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 aritmethic 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.