Block ciphers

David Felipe Mora, Eduards Mendez,Juan Carlos Sanchez Orjuela,María Sol Botello

October 25, 2022

Abstract

In this document we explain how to use and the innerworkings of the block ciphers present in this GitHub project.

1 DES

1.1 Feistel

In a Feistel cipher, each state ui is divided into two halves of equal length, say Li and Ri. The round function g has the following form: $(L^i, R^i) = g(L^{i-1}, R^{i-1}, K^i)$ where

$$L^i = R^{i-1}$$

$$R^i = L^{i-1} + f(R^{i-1}, K^i)$$

Observe that the function f does not need to satisfy any type of injective property. This is because a Feistel-type round function is always invertible, given the round key:

$$L^{i-1} = R^i + f(L^i, K^i)$$

$$R^{i-1} = L^i$$

1.2 DES

DES is a 16-round Feistel cipher having block length 64: it encrypts a plaintext bitstring x (of length 64) using a 56-bit key, K, obtaining a ciphertext bitstring (of length 64).

Prior to the 16 rounds of encryption, there is a fixed initial permutation IP that is applied to the plaintext. We denote $IP(x) = L^0R^0$.

After the 16 rounds of encryption, the inverse permutation IP^{-1} is applied to the bitstring R^16L^16, yielding the ciphertext y. That is, $y = IP^{-1}(R^{16}L^{16})$ (note that L^{16} and R^{16} are swapped before IP^{-1} is applied). The application of IP and IP^{-1} has no cryptographic significance.

Each L^i and R^i is 32 bits in length. The function $f : 0,1^32 \times 0,1^48 \rightarrow 0,1^32$ takes as input a 32-bit string (the right half of the current state) and a round key. The key schedule, $(K1, K2, ..., K16)$, consists of 48-bit round keys that are derived from the 56-bit key, K. Each K^i is a certain permuted selection of bits from K. The f function is shown in Figure 2. Basically, it consists of a substitution (using an S-box) followed by a (fixed) permutation, denoted P. Suppose we denote the first argument of f by A, and the second argument by J. Then, in order to compute $f(A, J)$, the following steps are executed.

1. A is "expanded" to a bitstring of length 48 according to a fixed expansion function E. $E(A)$ consists of the 32 bits from A, permuted in a certain way, with 16 of the bits appearing twice.

2. Compute $E(A) \oplus J$ and write the result as the concatenation of eight 6-bit strings $B = B_1B_2B_3B_4B_5B_6B_7B_8$.

3. The next step uses eight S-boxes, denoted $S_1, ..., S_8$. Each S-box

$$Si : \{0,1\}^6 \rightarrow \{0,1\}^4$$

maps six bits to four bits. Using these eight S-boxes, we compute $C_j = S_j(B_j)$, $1 \leq j \leq 8$.

4. The bitstring $C = C_1C_2C_3C_4C_5C_6C_7C_8$ of length 32 is permuted according to the permutation P. The resulting bit- string $P(C)$ is defined to be $f(A, J)$.

Figure 1: Overview de la página

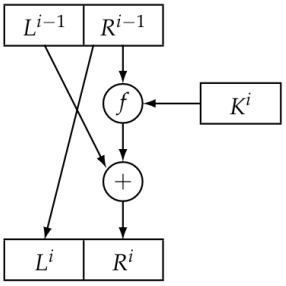

Figure 2: One round of DES cipher.

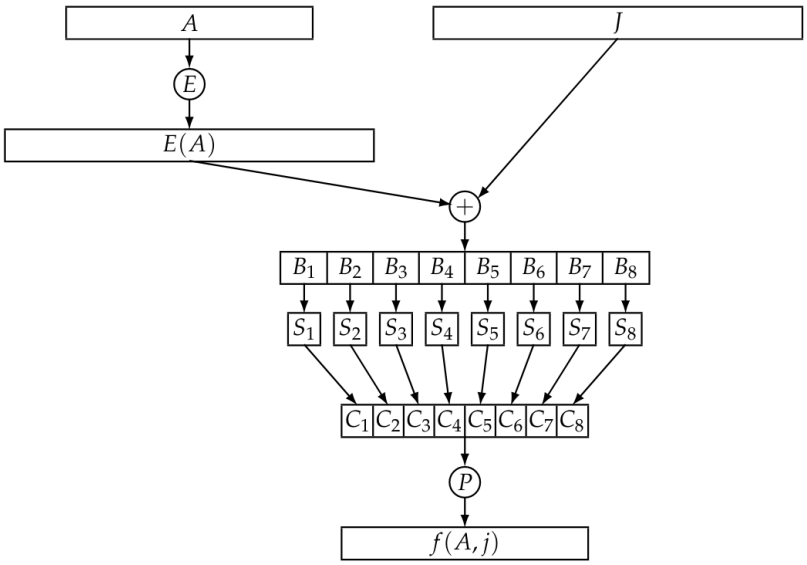

Figure 3: DES f function.

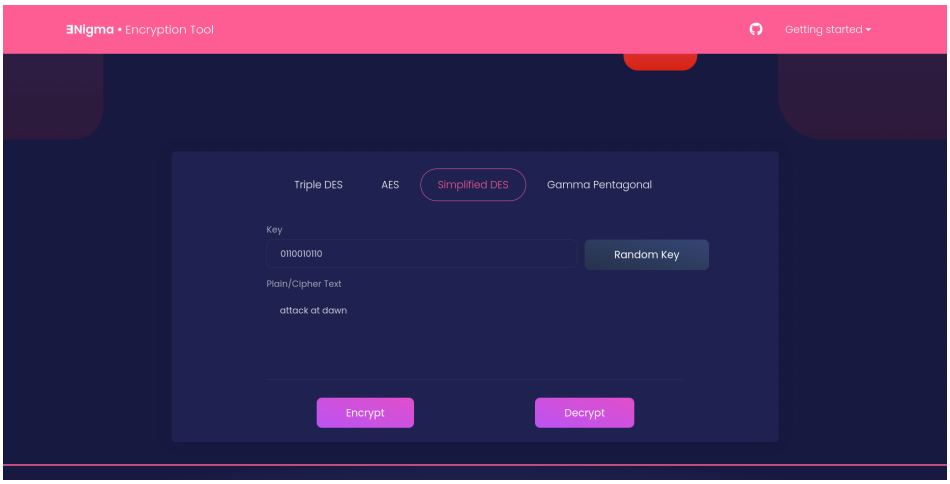

Figure 4: Hacer clic sobre 'Simplified DES' e ingresar claave y texto plano, también se puede generear clave aleatoria

1.2.1 False Positives

Let us assume that the attacker has a single plaintext/ciphertext pair, that is, two eight byte values P,C with $C = DES_k(P)$, where k is the correct unknown key.

Then, let us consider the values $DES'_k(P)$ there k' ranges over the $256 - 1$ possible incorrect keys. If we model DES with the incorrect key as a random permutation, then what we get is a list of $256 - 1$ random 8 byte values, each one of which has a 2^{-64} probability of just happening to be C.

Hence, the expected number of times the value C appears on that list is $(256 - 1)2^{-64} \equiv 2^{-8}$ (and the probability that the value C appears at least once on the list is a tad smaller).

Hence, there does indeed exist a nontrivial probability that a brute force search would find two keys; the correct key k , and another key k' that just happens to map P to C.

1.3 S-DES

The Simplified Data Encryption Standard is a simple version of Data Encryption Standard developed for educational purposes, it is a 2-round Feistel cipher that encrypts an 8-bit plain text using a 10-bit key.

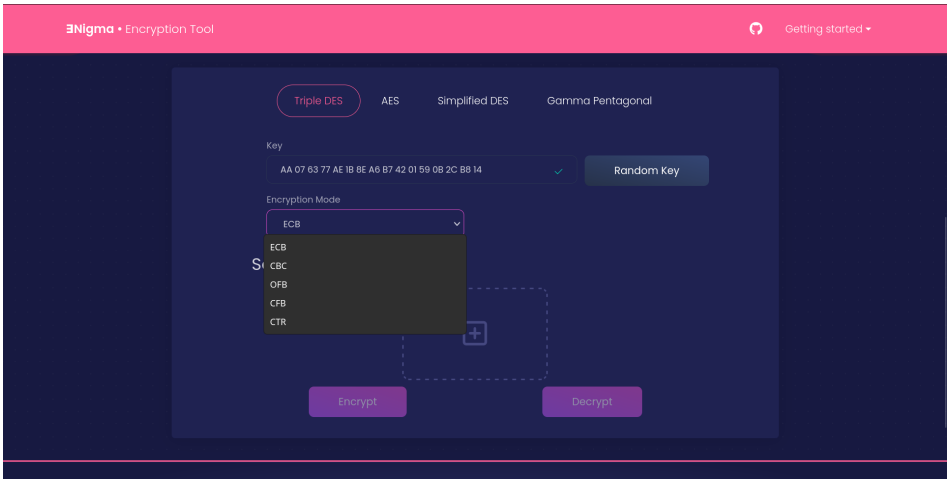

Figure 5: Se puede escoger el modo DES que se quiera

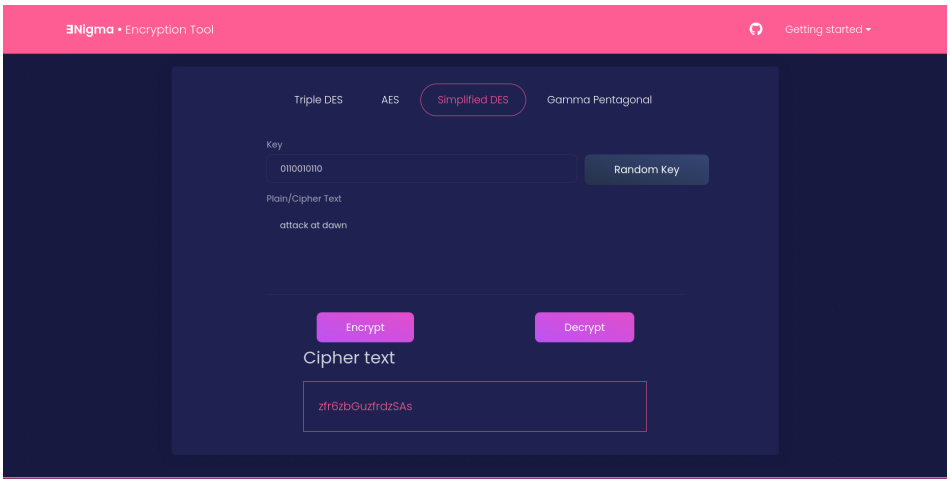

Figure 6: Al presionar Encrypt, aparece el texto encriptado abajo

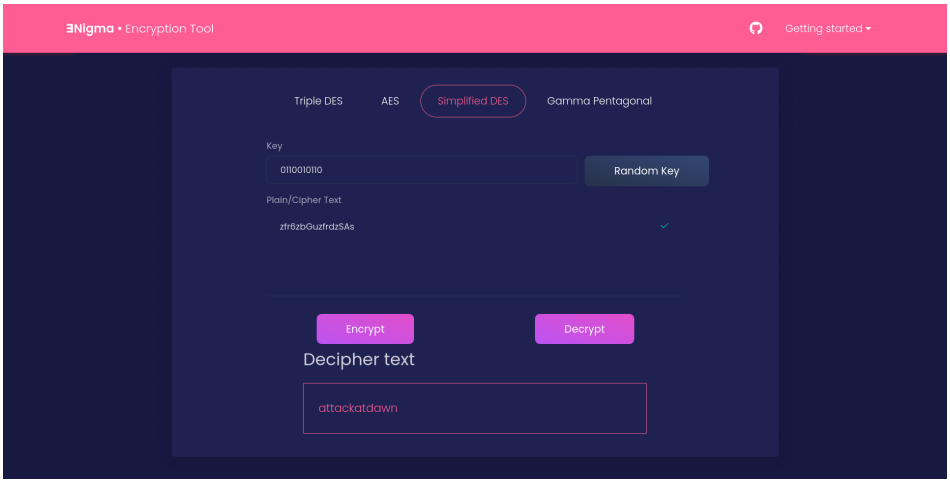

Figure 7: Usando la misma clave y escribiendo el texto encriptado, se decripta

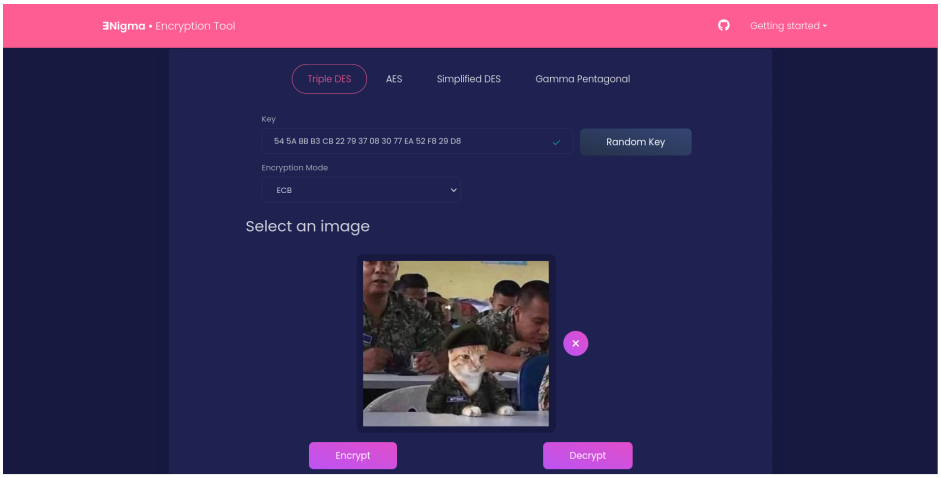

Figure 8: Funciona como S-DES, pero encripta imágenes, hacer clic sobre el + para subir una nueva imágen

1.4 TDES

The Triple Data Encryption Standard applies the DES cipher algorithm three times to each data block, each time with a different key.

2 AES

AES has block length 128, and there are three allowable key lengths, namely 128 bits, 192 bits, and 256 bits. AES is an iterated cipher; the number of rounds, which we denote by N , depends on the key length.

$N = 10$ if the key length is 128 bits, $N = 12$ if the key length is 192 bits and $N = 14$ if the key length is 256 bits.

The algorithm proceeds as follows:

1. Given a plaintext x, initialize State to be x and perform an operation ADD-ROUNDKEY, which x-ors the RoundKey with State.
2. For each of the first $N-1$ rounds, on State perform SUBBYTES using an S-box, a permutation SHIFTROWS, an operation MIXCOLUMNS.
3. Perform ADDROUNDKEY, SUBBYTES, SHIFTROWS and ADDROUNDKEY.
4. Define the ciphertext y to be State.

3 Gamma Pentagonal

References

[1] Stinson, D. Paterson, B.: Cryptography: Theory and Practice. Taylor & Francis Group **14**(3), 105–116 (2019)

[2] DES Bruteforce attack and false positive keys. Available at https://crypto.stackexchange.com/questions/50693/des-bruteforce-attack-and-false-positive-keys/50708#50708. Accessed: 2022-10-24

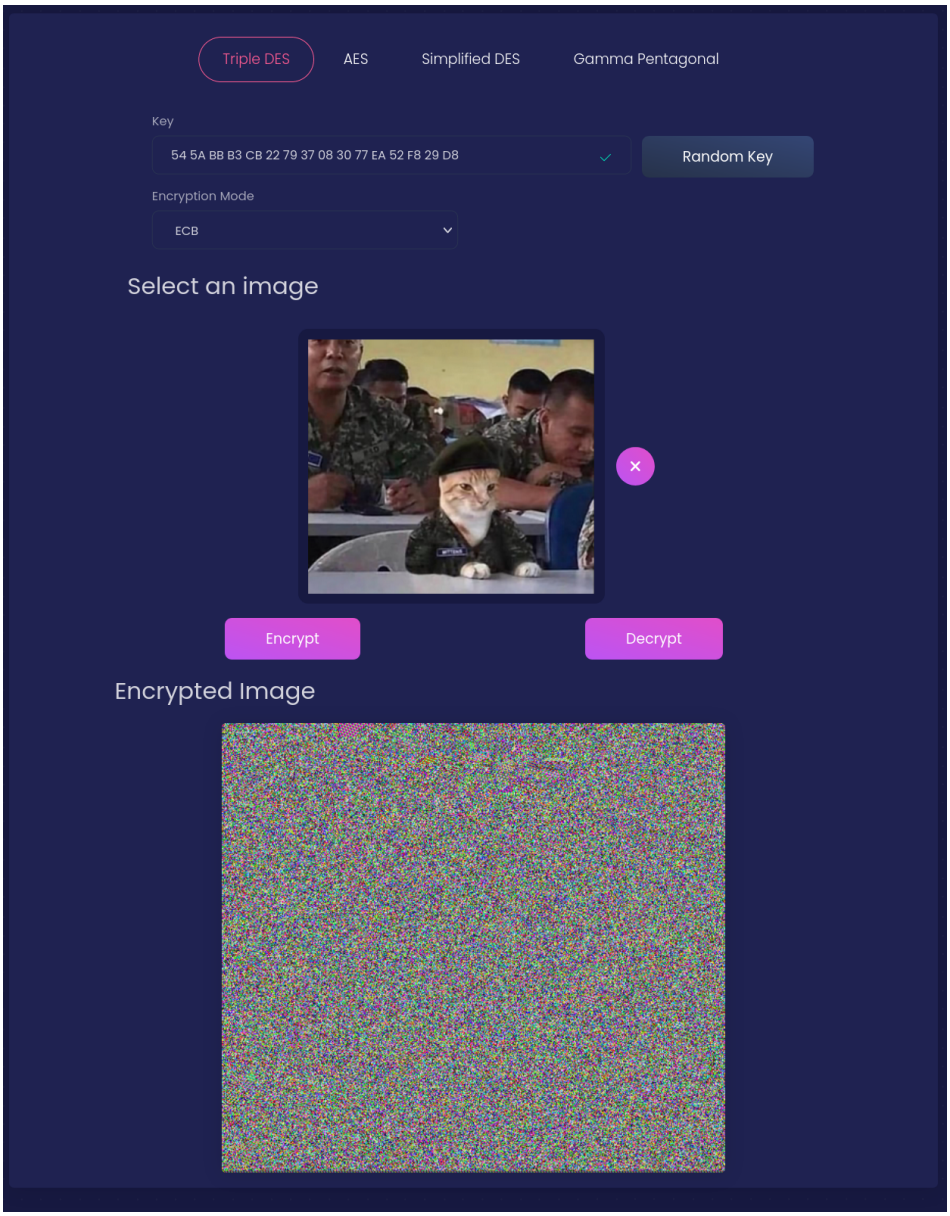

Figure 9: Al hacer clic en encrypt aparece la imagen encriptada

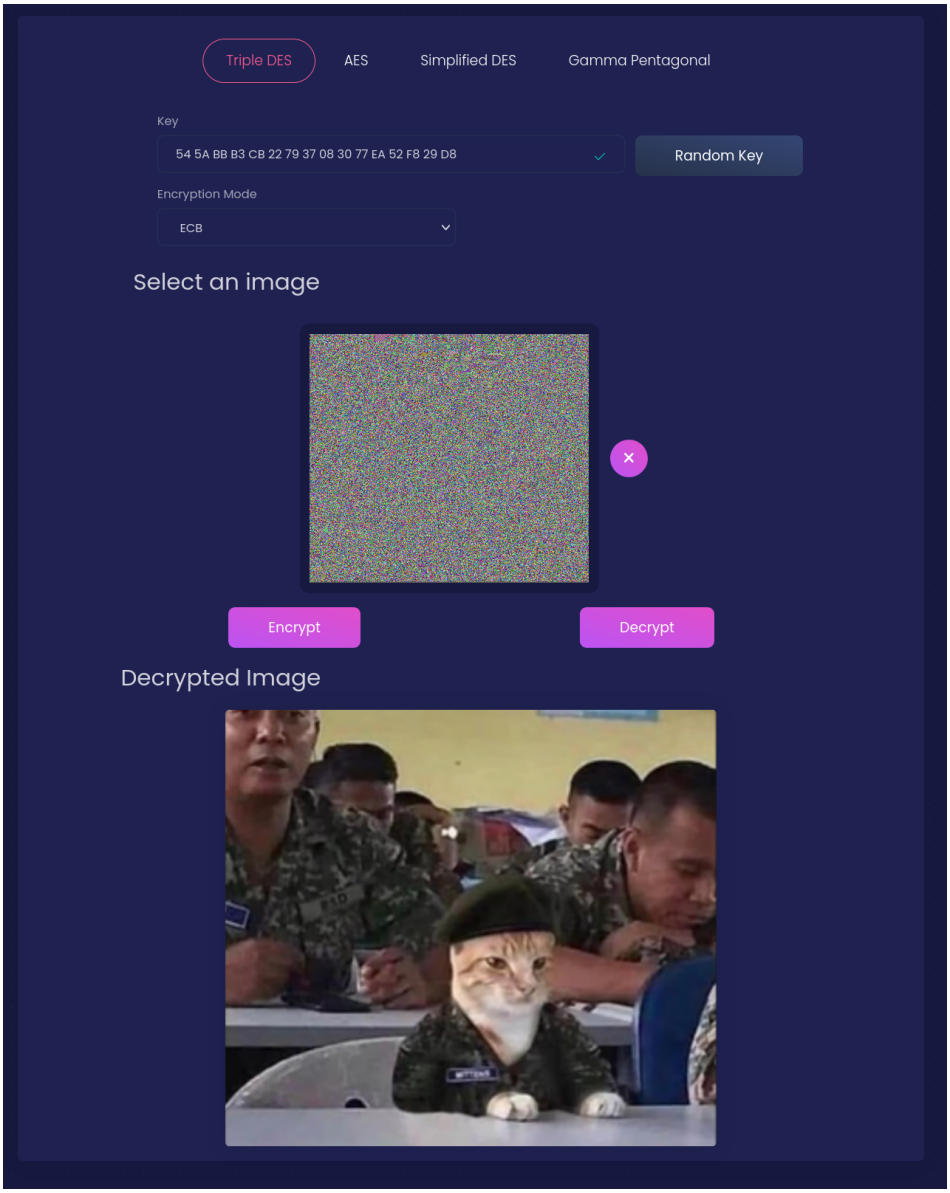

Figure 10: Con la misma clave y el texto encriptado, se decripta a la imagen original

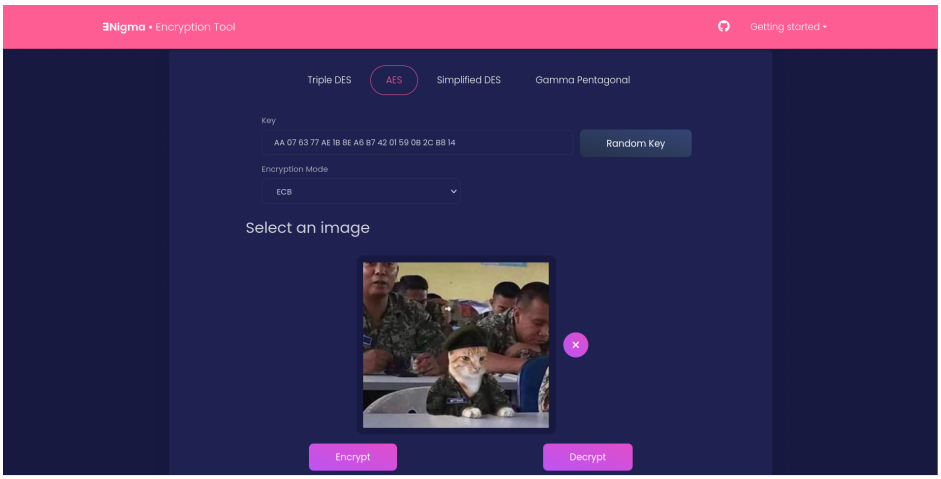

Figure 11: Encriptación AES: encripta imágenes, se puede escoger el modo y generar clave aleatoria como fue explicado anteriormente

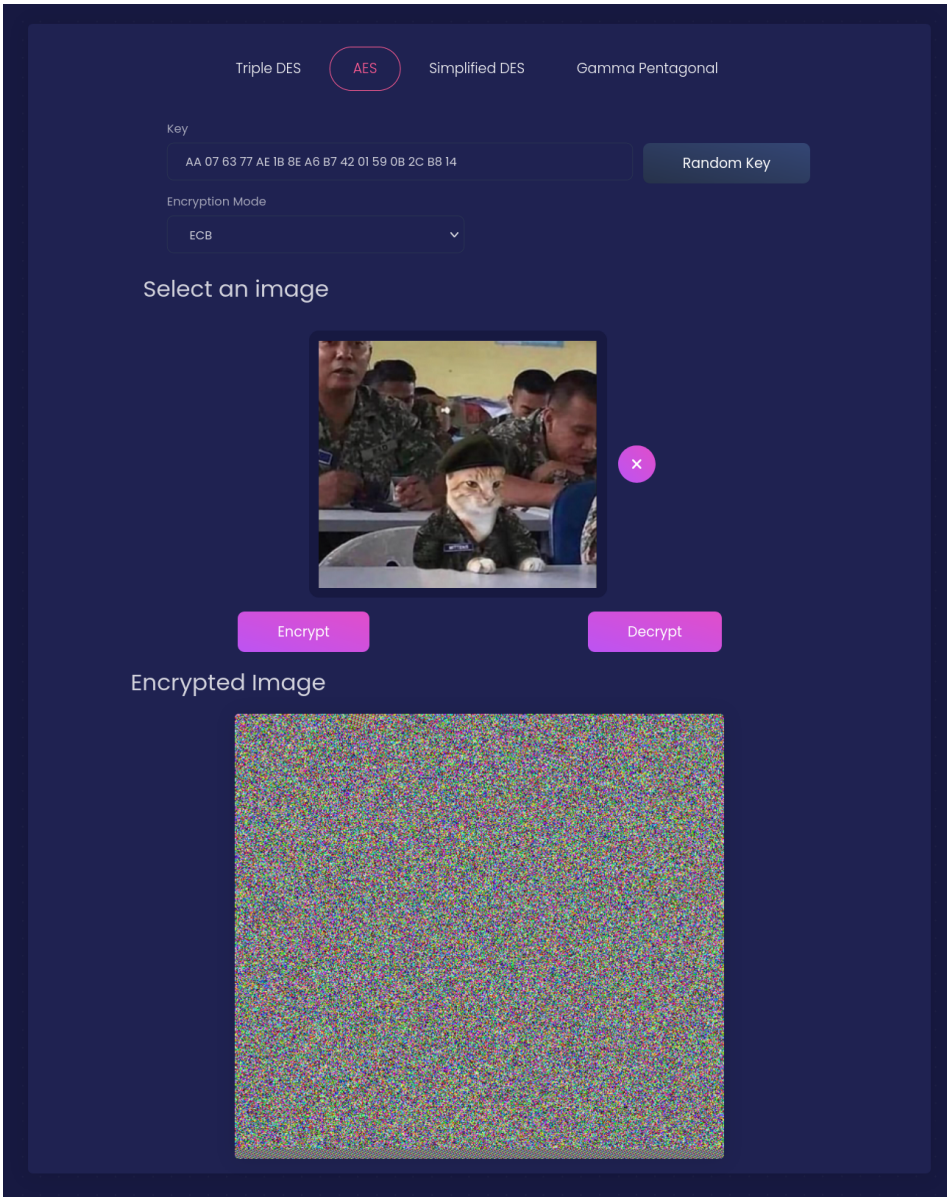

Figure 12: Al presionar Encrypt se genera la imagen encriptada abajo

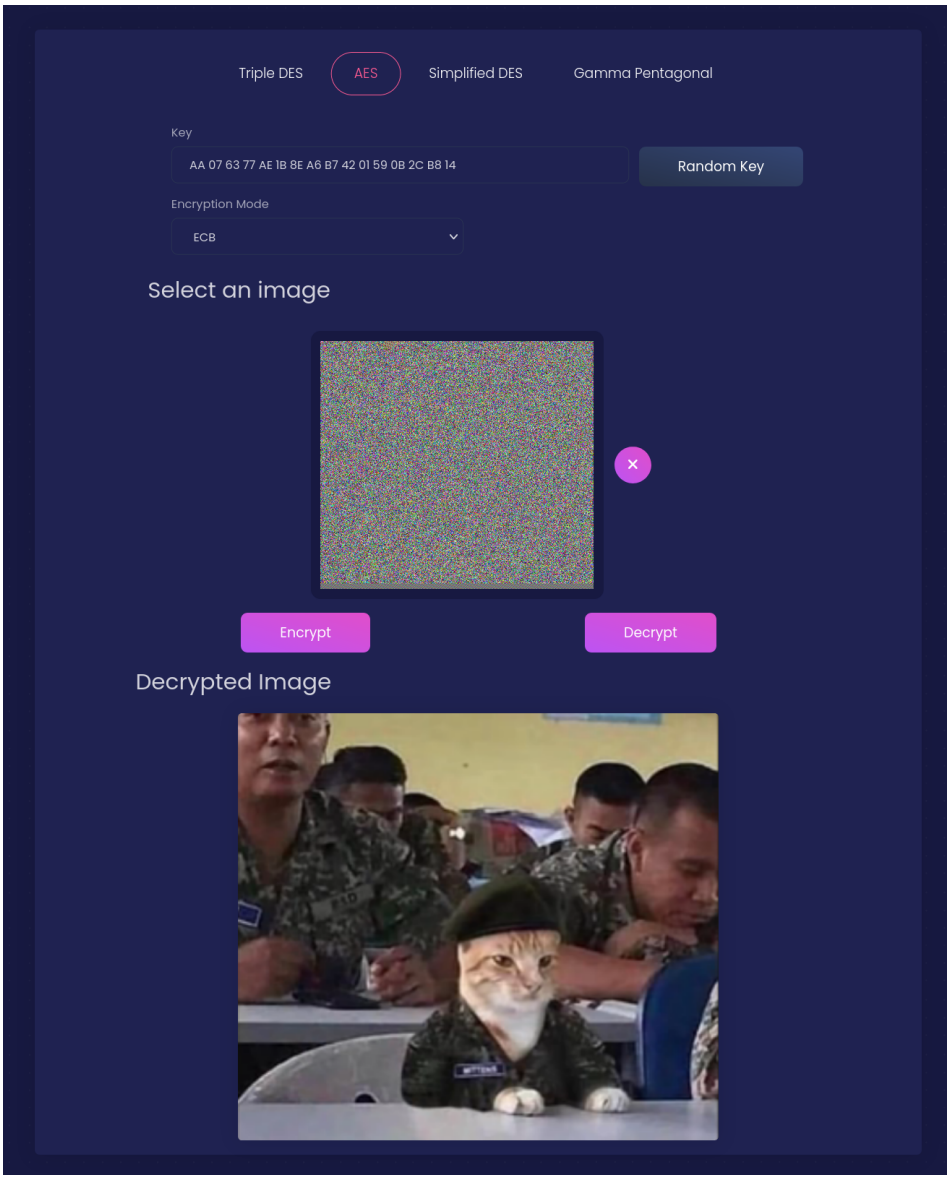

Figure 13: Con la misma clave y la imagen encriptada se decripta a la imagen original

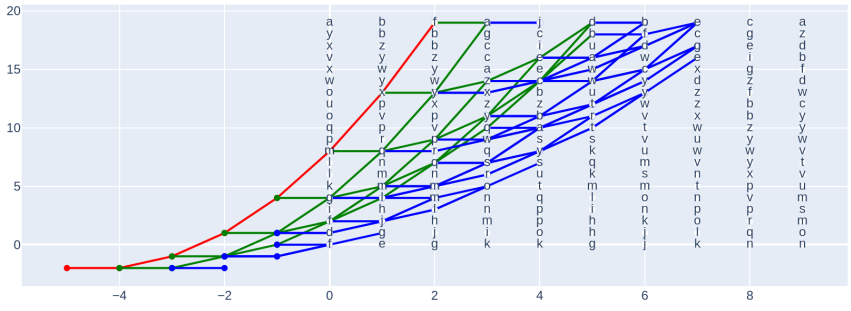

Figure 14: Trayectorias

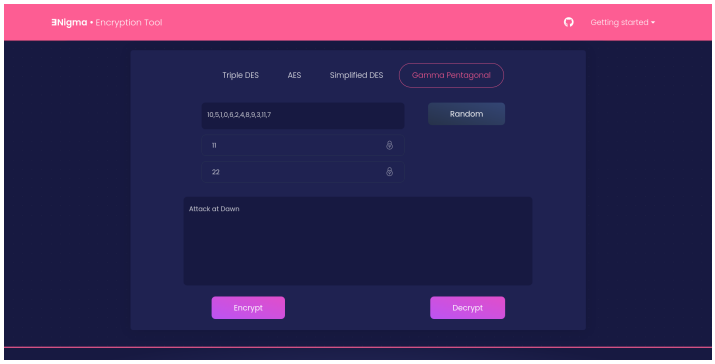

Figure 15: Cifrado gamma-pentagonal: cifra texto. Se puede generar una clave aleatoria.

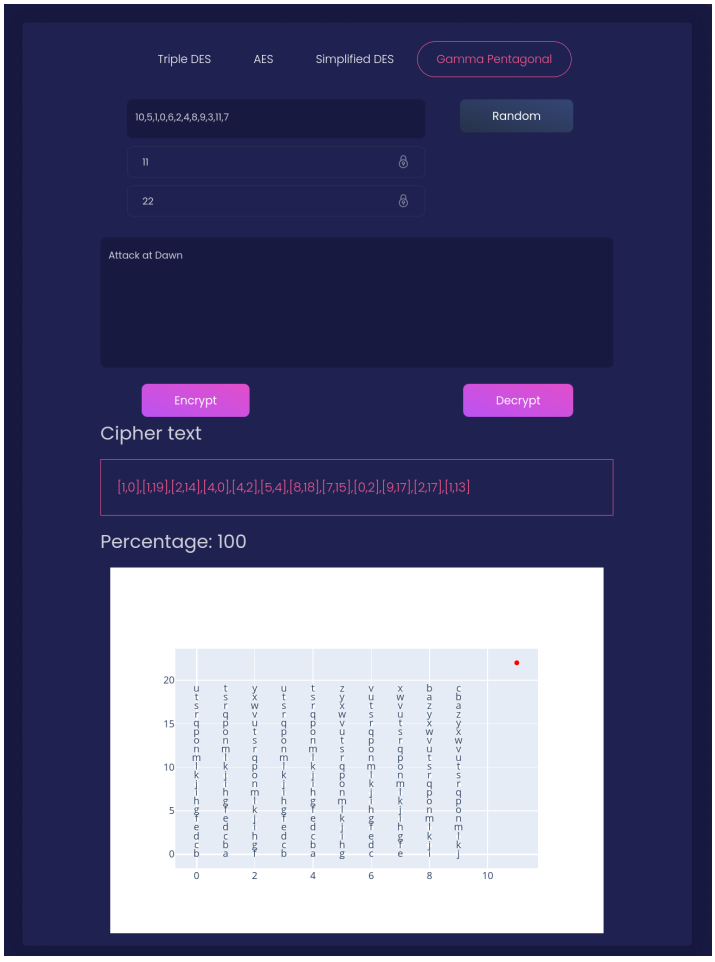

Figure 16: Al encriptar se genera el texto encriptado y se muestra el porcentaje de palabras encriptadas con el grafo

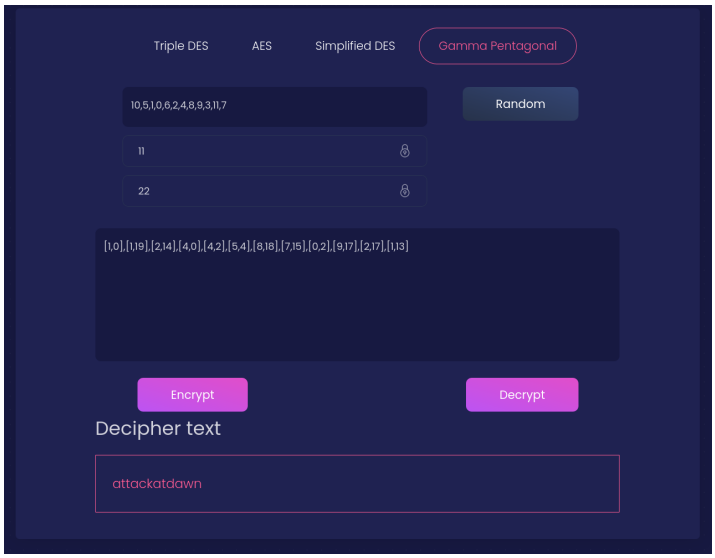

Figure 17: Con la misma clave y el texto encriptado, se decripta la original.