1. Clasifica el cifrador Atbash \_\_\_\_\_\_\_\_
2. Suponga que MCD(a,n)=d con d>1 entonces a⁻¹mod n no existe, explique porque.
3. Find =\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
4. 111 mod 17 =\_\_\_\_ -111 mod 17 \_\_\_\_ 1/111 mod 17 =\_\_\_\_ -1/111 mod 17 =\_\_\_\_
5. Cálcula: 17⁻¹mod 101 utilizando el Algoritmo Extendido de Euclides.
6. The following ciphertext was encrypted by Affine Cipher VMBAON. The plaintext ends with ar. Decrypt the message. Show the Dk
7. The ciphertext XNQV was encrypted using the affine function 15p + 13. Find the plaintext. Show the Dk
8. The ciphertext FRVSEUIW was encrypted using Vigenere cipher with the key *mars*. Find the plaintext Show the decryption key
9. Eve captures Bob´s Hill cipher machine, which uses a 2x2 matrix M mod 26. She tries to find de key, she knows that the plaintext *dont* encrypts to *ELNI*. Find matrix K?
10. Using block cipher with CBC mode. Show that if an error occurs in the transmission of a block Ci, but all the others blocks are transmitted correctly. Show in a diagram which decrypted blocks affects?
11. Betito recibió la siguiente imagen bmp de 24 bits cifrada. Sabe que Alicia utilizó Hill m=3 cuya llave

11.- IV 26, 13, 9

k= y con el modo de operación CBC.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| C1 | | | C2 | | |
| 40 | 171 | 36 | 236 | 184 | 95 |
| C3 | | | C4 | | |
| 47 | 97 | 212 | 194 | 9 | 97 |

Ayuda a Betito a encontrar **P2** (al finalizar utiliza un generador de colores RGB para ilustrarlo).

















