3ª)

Mensaje = NOFUEINDESCIFRABLE

Clave=PEROCASI

Alfabeto = ABCDEFGHIJKLMNÑOPQRSTUVWXYZ

Extensión de la clave: PEROCASIPEROCASIPE

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **N** | **O** | **F** | **U** | **E** | **I** | **N** | **D** | **E** | **S** | **C** | **I** | **F** | **R** | **A** | **B** | **L** | **E** |
| 13 | 15 | 5 | 21 | 4 | 8 | 13 | 3 | 4 | 19 | 2 | 8 | 5 | 18 | 0 | 1 | 11 | 4 |
| **P** | **E** | **R** | **O** | **C** | **A** | **S** | **I** | **P** | **E** | **R** | **O** | **C** | **A** | **S** | **I** | **P** | **E** |
| 16 | 4 | 18 | 15 | 2 | 0 | 19 | 8 | 16 | 4 | 18 | 15 | 2 | 0 | 19 | 8 | 16 | 4 |
| 13+16=29 | 15+4=19 | 5+18=23 | 21+15=36 | 4+2=6 | 8+0=8 | 13+19=32 | 3+8=11 | 4+16=20 | 19+4=23 | 2+18=20 | 8+15=23 | 5+2=7 | 18+0=18 | 0+19=19 | 1+8=9 | 11+16=27 | 4+4=8 |
| mod 27 | mod 27 | mod 27 | mod 27 | mod 27 | mod 27 | mod 27 | mod 27 | mod 27 | mod 27 | mod 27 | mod 27 | mod 27 | mod 27 | mod 27 | mod 27 | mod 27 | mod 27 |
| **2** | **19** | **23** | **9** | **6** | **8** | **5** | **11** | **20** | **23** | **20** | **23** | **7** | **18** | **19** | **9** | **0** | **8** |
| **C** | **S** | **W** | **J** | **G** | **I** | **F** | **L** | **T** | **W** | **T** | **W** | **H** | **R** | **S** | **J** | **A** | **I** |

4. Conclusiones

a. Cuáles son las debilidades y fortalezas del cifrado de Cesar (cifrado monoalfabético)

Cesar al seguir una secuencia mono alfabética, puede ser descifrado con gran facilidad, ofreciendo escasa seguridad, sin embargo, tiene la ventaja de que su alfabeto ocupa posiciones sucesivas en el código ASCII lo que lo hace muy ventajoso para programar.

b. Cuáles son las debilidades y fortalezas del cifrado de Vigenere (cifrado polialfabético)

El cifrado Vigenere, al emplear más de un alfabeto, las estadísticas del lenguaje ya no se manifiestan de manera tan clara en el criptograma. lo que brinda una mayor seguridad a sus usuarios, pero a pesar de esto, sigue manifestando una redundancia al lenguaje, la cual permitio al método Kasiski romperlo.