Algebra Abstracta CCOMP 3-1.1

Joan Salas Rondón

3ª:

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **N** | **O** | **F** | **U** | **E** | **I** | **N** | **D** | **E** | **S** |
| **P** | **E** | **R** | **O** | **C** | **A** | **S** | **I** | **P** | **E** |
| **C** | **S** | **W** | **J** | **G** | **I** | **F** | **L** | **T** | **W** |
| **C** | **I** | **F** | **R** | **A** | **B** | **L** | **E** |  |  |
| **R** | **O** | **C** | **A** | **S** | **I** | **P** | **E** |  |  |
| **T** | **W** | **H** | **R** | **S** | **J** | **A** | **I** |  |  |

Cifrado:

**CS WJG IFLTWTWHRSJAI**

4ª:

Fortalezas:

Al ser tan simple, el cifrado César es el cifrado más simple para enseñar a nuevas personas el concepto de criptografía.

Debilidades:

Al ser monoalfabético solo depende de las letras y no de su posición en el mensaje, por lo tanto solo se pueden hacer unas pocas operaciones en un solo alfabeto, en este caso sumar y restar posiciones, una vez se halla la cantidad de la clave, ya se descifro el mensaje.

4b:

Fortaleza:

El cifrado nunca va a ser el mismo porque depende de la posición de las letras del mensaje y de la clave, lo que hace que cada cifrado sea diferente

Debilidade:

La repetición de la clave en el mensaje es fácil de hallar y una vez se halle la longitud de la clave, es cuestión de tiempo en poder descifrarlo