**Práctica Vigenere**

**3. a)**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **0** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **12** | **13** | **14** | **15** | **16** | **17** | **18** | **19** | **20** | **21** | **22** | **23** | **24** | **25** | **26** |
| **A** | **B** | **C** | **D** | **E** | **F** | **G** | **H** | **I** | **J** | **K** | **L** | **M** | **N** | **Ñ** | **O** | **P** | **Q** | **R** | **S** | **T** | **U** | **V** | **W** | **X** | **Y** | **Z** |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **N** | **O** | **F** | **U** | **E** | **I** | **N** | **D** | **E** | **S** | **C** | **I** | **F** | **R** | **A** | **B** | **L** | **E** | **L1** | | |  |  |  |  |  |  |
| **P** | **E** | **R** | **O** | **C** | **A** | **S** | **I** | **P** | **E** | **R** | **O** | **C** | **A** | **S** | **I** | **P** | **E** | **L2** | | |  |  |  |  |  |  |
| **29** | **19** | **23** | **36** | **6** | **8** | **32** | **11** | **20** | **23** | **20** | **23** | **7** | **18** | **19** | **9** | **27** | **8** | **L1+L2** | | |  |  |  |  |  |  |
| **3** | **19** | **23** | **10** | **6** | **8** | **6** | **11** | **20** | **23** | **20** | **23** | **7** | **18** | **19** | **9** | **1** | **8** | **mod 26** | | |  |  |  |  |  |  |
| **D** | **S** | **W** | **K** | **G** | **I** | **G** | **L** | **T** | **W** | **T** | **W** | **H** | **R** | **S** | **J** | **B** | **I** | **CIFRADO** | | |  |  |  |  |  |  |

**4.**

**a)**

¿Cuáles son las debilidades y fortalezas del cifrado de Cesar (cifrado monoalfabetico)?

La fortaleza que tiene es que para su época fue bastante practico y muy ingenioso, pero la simplicidad de su clave secreta hace que con recursos limitados y haciendo uso de un tiempo reducido sería muy fácil llegarlo a romper.

**b)**

¿Cuáles son las debilidades y fortalezas del cifrado de Vigenere (cifrado polialfabetico)?

Su fortaleza radica en la complejidad para llegar a romperlo, al contar con múltiples alfabetos y una clave secreta un poco más compleja que la anterior, es decir en el caso de Cesar la clave es 1 de entre 26 opciones pero con Vigenere la clave es una palabra de entre todas las palabras existentes en ese idioma.  
La debilidad recae justamente en su fortaleza, el polialfabeto hace que el cifrado y descifrado sea un proceso largo y costoso.