**Cifrado de Vigenére.**

Este cifrado consiste en realizar la suma (módulo el número de caracteres en el alfabeto) de la clave y el texto en claro, una vez que se ha asignado un valor entero a cada carácter del alfabeto.

**Ejemplo:**

Sea:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **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** |
| 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 |

**Clave**

|  |  |  |
| --- | --- | --- |
| **E** | **R** | **A** |
| 4 | 18 | 0 |

**Mensaje**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **E** | **N** | **T** | **O** | **N** | **C** | **E** | **S** | **U** | **N** | **A** | **A** | **L** | **D** | **E** | **A** |
| 4 | 13 | 20 | 15 | 13 | 2 | 4 | 19 | 21 | 13 | 0 | 0 | 11 | 3 | 4 | 0 |

**Clave + Mensaje mod #Caracteres del Alfabeto**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **E** | **N** | **T** | **O** | **N** | **C** | **E** | **S** | **U** | **N** | **A** | **A** | **L** | **D** | **E** | **A** |
| **E** | **R** | **A** | **E** | **R** | **A** | **E** | **R** | **A** | **E** | **R** | **A** | **E** | **R** | **A** | **E** |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **4** | **13** | **20** | **15** | **13** | **2** | **4** | **19** | **21** | **13** | **0** | **0** | **11** | **3** | **4** | **0** |
| **4** | **18** | **0** | **4** | **18** | **0** | **4** | **18** | **0** | **4** | **18** | **0** | **4** | **18** | **0** | **4** |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 4 | 20 | 19 | 4 | 2 | 8 | 10 | 21 | 17 | 18 | 0 | 15 | 21 | 4 | 4 |
| **I** | **E** | **T** | **S** | **E** | **C** | **I** | **K** | **U** | **Q** | **R** | **A** | **O** | **U** | **E** | **E** |

***Criptograma***

**IETSECIKUQRAOUEE**

El mensaje se recupera realizando la resta (módulo el número de caracteres en el alfabeto de la clave y el criptograma.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 4 | 20 | 19 | 4 | 2 | 8 | 10 | 21 | 17 | 18 | 0 | 15 | 21 | 4 | 4 |
| **I** | **E** | **T** | **S** | **E** | **C** | **I** | **K** | **U** | **Q** | **R** | **A** | **O** | **U** | **E** | **E** |
| **E** | **R** | **A** | **E** | **R** | **A** | **E** | **R** | **A** | **E** | **R** | **A** | **E** | **R** | **A** | **E** |
| 4 | 18 | 0 | 4 | 18 | 0 | 4 | 18 | 0 | 4 | 18 | 0 | 4 | 18 | 0 | 4 |

**Clave - Mensaje mod #Caracteres del Alfabeto**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 4 | 13 | 20 | 15 | 13 | 2 | 4 | 19 | 21 | 13 | 0 | 0 | 11 | 3 | 4 | 0 |
| **E** | **N** | **T** | **O** | **N** | **C** | **E** | **S** | **U** | **N** | **A** | **A** | **L** | **D** | **E** | **A** |

***Mensaje***

**ENTONCESUNAALDEA**

**Ejemplo 2.**

Clave: **COM** Mensaje: **HARRY JAMES POTTER**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **H** | **A** | **R** | **R** | **Y** | **J** | **A** | **M** | **E** | **S** | **P** | **O** | **T** | **T** | **E** | **R** |
| 7 | 0 | 18 | 18 | 25 | 9 | 0 | 12 | 4 | 19 | 16 | 15 | 20 | 20 | 4 | 18 |
| **C** | **O** | **M** | **C** | **O** | **M** | **C** | **O** | **M** | **C** | **O** | **M** | **C** | **O** | **M** | **C** |
| 2 | 15 | 12 | 2 | 15 | 12 | 2 | 15 | 12 | 2 | 15 | 12 | 2 | 15 | 12 | 2 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 9 | 15 | 3 | 20 | 13 | 21 | 2 | 0 | 16 | 21 | 4 | 0 | 22 | 8 | 16 | 20 |
| **J** | **O** | **D** | **T** | **N** | **U** | **C** | **A** | **P** | **U** | **E** | **A** | **V** | **I** | **P** | **T** |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **J** | **O** | **D** | **T** | **N** | **U** | **C** | **A** | **P** | **U** | **E** | **A** | **V** | **I** | **P** | **T** |
| 9 | 15 | 3 | 20 | 13 | 21 | 2 | 0 | 16 | 21 | 4 | 0 | 22 | 8 | 16 | 20 |
| **C** | **O** | **M** | **C** | **O** | **M** | **C** | **O** | **M** | **C** | **O** | **M** | **C** | **O** | **M** | **C** |
| 2 | 15 | 12 | 2 | 15 | 12 | 2 | 15 | 12 | 2 | 15 | 12 | 2 | 15 | 12 | 2 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 7 | 0 | 18 | 18 | 25 | 9 | 0 | 12 | 4 | 19 | 16 | 15 | 20 | 20 | 4 | 18 |
| **H** | **A** | **R** | **R** | **Y** | **J** | **A** | **M** | **E** | **S** | **P** | **O** | **T** | **T** | **E** | **R** |

**Para romper con este cifrado, hay que observar y cuantificar la frecuencia de aparición de cada letra en determinado idioma. Teniendo esto observamos que símbolos se repiten más y suponer que es una de las letras con más frecuencia. Y también es común que antes o después de una vocal exista una consonante. Con estos criterios podemos ir descartando y proponer candidatos para descifrar el mensaje.**