**Cifrado Afin**

En aritmética modular, se considera que **dos enteros relativos son congruentes modulo n** si presentan la misma resta en la división euclidiana por n. Trabajar con modulo n significa trabajar con números enteros comprendidos en el intervalo [0; n-1] incluidos los limites.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **A** | **B** | **C** | **D** | **E** | **F** | **G** | **H** | **I** | **J** | **K** | **L** | **M** | **N** | **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 |

Usar como función de cifrado una función afín del tipo en las que [a] y [b] son constantes, y en las que [x] e [y] son números correspondientes a las letras del alfabeto en base a esta tabla.

**\*\*Nota:** si **[a]=1**, volvemos a encontrar la cifra de Cesar donde **[b] representa el desplazamiento.** Y el valor de [b] es un número comprendido entre el 0 y el 25.

No podemos utilizar cualquier valor para [a]; [a] y 26 **deben ser primos entre sí**, lo que significa que no deben tener divisores comunes que no sean 1. Los valores posibles para [a] son pues *1, 3, 5, 7, 11, 15, 17, 19, 21, 23, y 25*.

**Ejemplo.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Texto en Claro** | **H** | **O** | **L** | **A** |
| **X** | 7 | 14 | 11 | 0 |
| **Y** | 15 | 0 | 25 | 4 |

**H**

**O A**

**L**

**A E**

**Fórmula de descifrado**

Invertir (mod 26) la fórmula de cifrado con el fin de expresar [x] en función de [y]

Si resulta negativo basta con sumarle 26 antes de multiplicarlo por

**Ejemplo.**

**Para romper con este cifrado al igual que con el de Vigenere, 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.**