## 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 ; $\boldsymbol{y = ax + b}$ 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 |

$\boldsymbol{a = 9; b = 4;\ y = ax + b}$

**H** $\mathrm{y} = 9(7) + 4 = 67 \bmod 26 = 15 \rightarrow \mathbf{P}$

**O** $\mathrm{y} = 9(14) + 4 = 130 \bmod 26 = 0 \rightarrow \mathbf{A}$

**L** $\mathrm{y} = 9(11) + 4 = 103 \bmod 26 = 25 \rightarrow \mathbf{Z}$

**A** $\mathrm{y} = 9(0) + 4 = 4 \bmod 26 = 0 \rightarrow \mathbf{E}$

**Fórmula de descifrado**

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

$$y = ax + b$$
$$y - b = ax$$
$$Sabemos\ que\ [a^{-1}][a] = 1$$
$$[a^{-1}](y - b) = x$$
$$\boldsymbol{x = [a^{-1}](y - b)(mod\ 26)}$$

Si $(y - b)$ resulta negativo basta con sumarle 26 antes de multiplicarlo por $[a^{-1}]$

**Ejemplo.**

$$a = 9\ \therefore [a^{-1}] = 3; \quad b = 4; \quad x = [a^{-1}](y - b)(mod\ 26)$$

$$\boldsymbol{P} \rightarrow x = 3(15 - 4) = 33\ mod\ 26 = 7 \rightarrow \boldsymbol{H}$$
$$\boldsymbol{A} \rightarrow x = 3(0 - 4) = -12\ mod\ 26 = 14 \rightarrow \boldsymbol{O}$$
$$\boldsymbol{Z} \rightarrow x = 3(25 - 4) = 63\ mod\ 26 = 11 \rightarrow \boldsymbol{L}$$
$$\boldsymbol{E} \rightarrow x = 3(0) = 33\ mod\ 26 = 0 \rightarrow \boldsymbol{A}$$

**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.**