Cifrado Afin

Hernán Gómez

Universidad del Pacifico
EISC(Facultad de Ingeniería)

Agosto, 2025

Contenido

Definición

- El cifrado afin es un tipo de cifrado que emplea expresiones modulares para codificar y decodificar
- Sea la expresion de codificacion $y = (a.c + k)\ mod\ m$ donde a, es un coeficiente multiplicativo; c, el valor del codigo del elemento en el alfabeto ;k, valor de desplazamiento y m, cantidad de elementos del alfabeto
- Sea la expresion de decodificacion $c = a^{-1}(y - k)\ mod\ m$; a^{-1}, es el inverso multiplicativo de $a\ mod\ m$

Codificación

Considere el siguiente alfabeto de 27 elementos

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

Codificación de la palabra humildad, $y = (7.c + 3)\ mod\ 27$ donde $a = 7, k = 3$ y $m = 27$

Elemento	**H**	**U**	**M**	**I**	**L**	**D**	**A**	**D**
Valor(c)	7	21	12	8	11	2	0	3
Y	25	15	6	5	26	17	3	24
Codificación	**Y**	**O**	**G**	**F**	**Z**	**Q**	**D**	**X**

Pasos Decodificación

Para decodificar un mensaje o cadena se emplea la siguiente formula $c = a^{-1}(y - k)\ mod\ m$; para ello hay que encontrar a^{-1}, que es el inverso multiplicativo de $a\ mod\ m$. Acontinuacion se presentan los pasos:

- **Paso 1:** verificar que el $MCD(m, a) = 1$, es decir probar que no haya divisibilidad entre m y a para poder encontrar un expresión de decodificación de lo contrario no existira.
- **Paso 2:** encontrar la variable x, de la siguiente ecuacion diofantica lineal[1] $x.a + m.y = 1$. Para encontrar x, emplee el algoritmo eucledianо como apoyo
- **Paso 3:** una vez encontrado x,calcular el inverso como $a^{-1} = x\ mod\ m$

[1] Ecuación diofantica lineal es una ecuación algebraica con coeficientes enteros en la que se busca soluciones enteras

Ejemplo Decodificación

Sea la expresión general de decodificación $c = a^{-1}(y - k)\ mod\ m$ y la función particular para $m = 27$, $k = 3$ y $a = 7$

Paso 1: Probando $MCD(27, 7)$ es 1

$$27 = 7 * 3 + 6$$

$$7 = 6 * 1 + 1$$

$$6 = 1 * 6 + 0$$

De esta forma se prueba que $MCD(27, 7) = 1$

Ejemplo Decodificación

Paso 2: Dado que el $MCD(27, 7) = 1$; procedemos a utilizar la expresion diofantica lineal $x.a + m.y = 1$ para eso seleccionamos la expresion del **paso 1** con residuo **"1"** , en este caso $7 = 6 * 1 + 1$ despejando tendriamos $7 - 6 * 1 = 1$ que se asemeja a la expresion diofantica lineal, pero no tenemos a m que es "27",en su lugar tenemos un "6"

Para ello despejamos la **expresion 1** del **paso 1** que seria $27 = 7 * 3 + 6$ entonces tendriamos $27 - 7 * 3 = 6$. **Reemplazando** la expresion $27 - 7 * 3 = 6$ en $7 - 6 * 1 = 1$ se tendria $7 - (27 - 7 * 3) * 1 = 1$

Resumiendo: $(4)7 + 27(-1) = 1$. Comparando con la ecuación diofantica lineal $\boxed{\boxed{x.a + m.y = 1}\\ \boxed{(4)7 + 27(-1) = 1}}$ se puede deducir que $x = 4$

Ejemplo Decodificación

Paso 3: como se dedujo que $x = 4$ entonces podremos hallar el inverso multiplicativo del modulo $a^{-1} = x \ mod \ m$

$$a^{-1} = 4 \ mod \ 27 = 4$$

Formula de decodificación:

$$c = 4(y - 3) \ mod \ 27$$

Elemento	**Y**	**O**	**G**	**F**	**Z**	**Q**	**D**	**X**
Valor(y)	25	15	6	5	26	17	3	24
c	7	21	12	8	11	2	0	3
Decodificación	**H**	**U**	**M**	**I**	**L**	**D**	**A**	**D**

Practique

Resuelva el siguiente ejercicio :halle la formula de decodificación. Si el inverso multiplicativo del modulo $a^{-1} = x \ mod \ m$, ademas se sabe que su formula de codificacion es $y = (8.c + 9) \ mod \ 27$