Preliminares matemáticos

Conversión de mensajes
Aritmética modular

Conversión de mensajes

En todo criptosistema tenemos una *función de cifrado*, que debe ser biyectiva:

$$\begin{array}{ccc} \mathcal{M} & \xrightarrow{f} & \mathcal{C} \\ M & \mapsto & C \\ \text{(mensaje en claro)} & & \text{(mensaje cifrado)} \end{array}$$

Como la función es biyectiva, existirá su función inversa, que es la *función de descifrado*:

$$\begin{array}{ccc} \mathcal{C} & \xrightarrow{f^{-1}} & \mathcal{M} \\ C & \mapsto & M \end{array}$$

Criptosistema:

$$\mathcal{M} \xrightarrow{f} \mathcal{C} \xrightarrow{f^{-1}} \mathcal{M}$$

Los conjuntos $\mathcal{M}$ y $\mathcal{C}$ son conjuntos de números, o de cadenas de bits.

Los mensajes (en claro y cifrados) están escritos en un *alfabeto* de N caracteres.

Por ejemplo:

$$\text{alfabeto} = \{A,\, B,\, \ldots,\, Z,\, 0,\, 1,\, 2,\, \text{“ ”}\} \quad N = 26 + 3 + 1 = 30.$$

Paso de mensaje a número

Etiquetamos los caracteres.

$$\begin{array}{cccccccc} A & B & \ldots & Z & 0 & 1 & 2 & \text{“ ”} \\ 0 & 1 & \ldots & 25 & 26 & 27 & 28 & 29 \end{array}$$

A	B	...	Z	0	1	2	" "
0	1	...	25	26	27	28	29

Partimos los mensajes en *unidades de mensaje* o *bloques*. Pueden estar formados por una letra, por dos (*bigramas*), tres (*trigramas*), etc.

Si los bloques son de una letra, simplemente transformamos cada letra en su etiqueta:

"LA PRUEBA 1 ES" $\rightarrow$ 11 0 29 15 17 20 4 1 0 29 27 29 4 18

11 0 29 28 29 4 18 29 4 18 19 0 $\rightarrow$ "LA 2 ES ESTA"

Observación: $0 \leq M \leq N - 1$. Es decir,

$$M \in \mathbb{Z}_N = \{0, 1, \ldots, N - 1\}.$$

Si partimos el mensaje en bigramas:

“LA PRUEBA 1 ES” $\rightarrow$ “LA”, “ P”, “RU”, “EB”, “A ”, “1 ”, “ES”

primero asignamos a cada letra su etiqueta

$$\text{“LA”} \rightarrow (11, 0)$$

y después al par $(11, 0)$ le asignamos el número

$$30 \cdot 11 + 0 = 330.$$

$$\text{“LA”} \to (11, 0) \to 30 \cdot 11 + 0 = 330$$

$$\text{“ P”} \to (29, 15) \to 30 \cdot 29 + 15 = 885$$

$$\text{“LA PRUEBA 1 ES”} \to 330\ 885\ 530\ 121\ 29\ 839\ 138$$

En general, al par (x, y) le asignamos el número $M = Nx + y$.

$$(x, y) \to M = Nx + y.$$

Observaciones:

1. $0 \leq M = Nx + y \leq N^2 - 1$. Es decir,

$$M \in \mathbb{Z}_{N^2} = \{0, 1, \ldots, N^2 - 1\}.$$

2. El par (x, y) es la representación de M en base N.

Para pasar un número M a mensaje deberemos obtener la representación de M en base N:

Si el alfabeto es

$$\begin{array}{cccccccc} A & B & \dots & Z & 0 & 1 & 2 & \text{“ ”} \\ 0 & 1 & \dots & 25 & 26 & 27 & 28 & 29 \end{array} \qquad N = 30$$

y recibimos

$$330\ 898\ 874\ 569\ 138\ 570$$

$$330 = 30 \cdot 11 + 0 \to (11, 0) \to \text{“LA”}$$

$$898 = 30 \cdot 29 + 28 \to (29, 28) \to \text{“ 2”}$$

$$330, 898, 874, 569, 138, 570 \to \text{“LA 2 ES ESTA”}$$

Podemos partir el mensaje en trigramas:

“LA PRUEBA 1 ES” $\rightarrow$ “LA ”, “PRU”, “EBA”, “ 1 ”, “ES ”

Como la longitud del mensaje es 14, deberemos añadir un carácter para obtener un múltiplo de 3. Se añade una letra que no cree ambigüedad. En este ejemplo hemos añadido la última letra del alfabeto (“ ”).
Ahora la transformación a número será:

$$\text{“LA ”} \rightarrow (11, 0, 29) \rightarrow 30^2 \cdot 11 + 30 \cdot 0 + 29 = 9929$$

$$\text{“LA PRUEBA 1 ES”} \rightarrow 9929\ 14030\ 3630\ 26939\ 4169$$

En general,

$$(x, y, z) \rightarrow M = N^2 x + N y + z.$$

Si partimos el mensaje en k-gramas:

$$(x_{k-1}, \ldots, x_1, x_0) \to M = N^{k-1} x_{k-1} + \cdots + N x_1 + x_0$$

$$M \in \mathbb{Z}_{N^k} = \{0, 1, \ldots, N^k - 1\}$$

Para transformar un número $M \in \mathbb{Z}_{N^k}$ en mensaje deberemos primero obtener su representación en base N.

Paso de mensaje a bits

Si los elementos de los conjuntos $\mathcal{M}$ y $\mathcal{C}$ son cadenas de bits, deberemos transformar los mensajes en cadenas de bits.

Una posibilidad es transformar primero el mensaje en número con la técnica anterior y expresar el número en base 2.

Por ejemplo, si $N = 30$ y dividimos el mensaje en trigramas ($k = 3$):

Paso a números:

$$\text{“LA ”} \to (11, 0, 29) \to M = 30^2 \cdot 11 + 30 \cdot 0 + 29 = 9929 < N^k.$$

Paso a bits:

Como $M \leq N^k - 1 = 30^3 - 1 = 26999 = 2^{14} + 2^{13} + \cdots + 2 + 1$, las cadenas constarán de 15 bits ($\log_2 26999 = 14.72$):

$$M = 9929 = 2^{13} + 2^{10} + 2^9 + 2^7 + 2^6 + 2^3 + 1 \to 010011011001001.$$

Otra alternativa es utilizar, por ejemplo, el código ASCII:

$$\text{“L”} \rightarrow [01001100]$$

$$\text{“A”} \rightarrow [01000001]$$

$$\text{“LA...”} \rightarrow 0100110001000001\ldots$$

Aritmética modular

Definición

Sea n un entero, $n > 1$.

Dados dos números enteros a, b, diremos que a es congruente con b módulo *n si existe un entero k tal que*

$$a = b + kn.$$

Es decir, si

$$n \mid a - b.$$

Se escribe

$$a \equiv b \mod n.$$

Ejemplo

$$17 \equiv 2 \mod 5, \quad 17 \not\equiv 2 \mod 4, \quad -23 \equiv -5 \mod 6,$$

$$-7 \equiv 2 \mod 3, \quad 1500 \equiv 0 \mod 2.$$

$$n \equiv 0 \mod n, \quad 2n \equiv 0 \mod n, \quad 3n \equiv 0 \mod n,$$

$$-n \equiv 0 \mod n, \quad -2n \equiv 0 \mod n, \quad \ldots, \quad kn \equiv 0 \mod n.$$

$$-5 \equiv 2 \mod 7, \quad -3 \equiv 8 \mod 11, \quad -a \equiv n-a \mod n.$$

Dado un entero a, podemos calcular el cociente y resto de la división de a entre n.

$$\begin{array}{c|l} a & \underline{\;n\;} \\ r & \;q \end{array} \qquad a = r + qn, \quad 0 \leq r < n.$$

Entonces,

$$a \equiv r \mod n.$$

Como el resto r satisface $0 \leq r < n$, los posibles restos que podemos encontrar son $0, 1, \ldots, n-1$.

El conjunto de posibles restos se representa por $\mathbb{Z}_n$,

$$\mathbb{Z}_n = \{0, 1, ..., n-1\}$$

y se llama *conjunto de residuos* módulo n.

Ejemplo

- $$\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}.$$

  Cualquier $a \in \mathbb{Z}$ es congruente módulo 5 con algún elemento de $\mathbb{Z}_5$.

  $$8753 \equiv 3 \pmod 5, \quad 35 \equiv 0 \pmod 5, \quad -23 \equiv 2 \pmod 5.$$

- $$\mathbb{Z}_2 = \{0, 1\}.$$

  Si $a \in \mathbb{Z}$ es par, entonces $a \equiv 0 \pmod 2$.
  Si $a \in \mathbb{Z}$ es impar, entonces $a \equiv 1 \pmod 2$.

En $\mathbb{Z}_n$ se pueden definir las operaciones suma y producto de la siguiente forma

$$((a \mod n) + (b \mod n)) \mod n = (a+b) \mod n.$$

$$((a \mod n) \cdot (b \mod n)) \mod n = (a \cdot b) \mod n.$$

Ejemplo

$\mathbb{Z}_4 = \{0, 1, 2, 3\}$

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$\mathbb{Z}_2 = \{0, 1\}$

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

Propiedades de la suma

- *Asociativa:*
$$\forall a, b, c \in \mathbb{Z}_n \quad (a+b)+c \equiv a+(b+c) \mod n.$$

- *Conmutativa:*
$$\forall a, b \in \mathbb{Z}_n \quad a+b \equiv b+a \mod n.$$

- *Existe elemento neutro* (0)
$$\exists 0 \in \mathbb{Z}_n \text{ tal que } \quad \forall a \in \mathbb{Z}_n \quad a+0 \equiv a \mod n.$$

- *Todo elemento tiene simétrico (opuesto)*
$$\forall a \in \mathbb{Z}_n \quad \exists(-a) \in \mathbb{Z}_n \text{ tal que } \quad a+(-a) \equiv 0 \mod n.$$

Observación: $\quad -a \equiv n-a \mod n.$

Un conjunto dotado de una operación que cumpla esas cuatro propiedades se dice que es un *grupo conmutativo*.

Por tanto, $(\mathbb{Z}_n, +)$ es un grupo conmutativo.

Propiedades del producto

- *Asociativa:*

$$\forall a, b, c \in \mathbb{Z}_n \quad (a \cdot b) \cdot c \equiv a \cdot (b \cdot c) \pmod{n}.$$

- *Conmutativa:*

$$\forall a, b \in \mathbb{Z}_n \quad a \cdot b \equiv b \cdot a \pmod{n}.$$

- *Existe elemento neutro* (1)

$$\exists 1 \in \mathbb{Z}_n \text{ tal que } \quad \forall a \in \mathbb{Z}_n \quad a \cdot 1 \equiv a \pmod{n}.$$

Propiedades del producto con respecto a la suma:

- *Distributiva:*

$$\forall a, b, c \in \mathbb{Z}_n \quad (a + b) \cdot c \equiv (a \cdot c) + (b \cdot c) \pmod{n}.$$

Un conjunto dotado de dos operaciones $(+)$ y $(\cdot)$ que satisfacen todas las propiedades anteriores se dice que es un *anillo conmutativo unitario.*

Por tanto, $(\mathbb{Z}_n, +, \cdot)$ es un anillo conmutativo unitario.

Potenciación modular

Dados dos enteros a, x, $(x \geq 0)$, para calcular a^x, el mecanismo más sencillo sería multiplicar a por sí mismo x veces. Pero para valores muy grandes de x ese algoritmo es poco eficiente.

Utilizaremos la potenciación por cuadrados.
Por ejemplo,

$$a^8 = a^{2^3} = ((a^2)^2)^2.$$

$$a^{13} = a^{2^3+2^2+1} = a^{2^3} \cdot a^{2^2} \cdot a = ((a^2)^2)^2 \cdot (a^2)^2 \cdot a = ((a^2 \cdot a)^2)^2 \cdot a.$$

En general, para calcular a^x, utilizaremos la representación binaria de x. Por ejemplo,

$$x = 27 = 11011_{(2} = 2^4 + 2^3 + 2 + 1.$$

$$a^{27} = a^{2^4+2^3+2+1} = a^{2^4} \cdot a^{2^3} \cdot a^2 \cdot a = (((a^2 \cdot a)^2)^2 \cdot a)^2 \cdot a.$$

Para calcular $a^x \mod n$, basta calcular los productos módulo n.

Ejemplo

$$3^{13} \mod 5.$$

$$13 = 2^3 + 2^2 + 1 = 1101_{(2}.$$

$$3^{13} \equiv 3^{2^3+2^2+1} \equiv ((3^2 \cdot 3)^2)^2 \cdot 3 \equiv ((4 \cdot 3)^2)^2 \cdot 3$$

$$\equiv (2^2)^2 \cdot 3 \equiv 4^2 \cdot 3 \equiv 1 \cdot 3 \equiv 3 \mod 5.$$

Fin de la sección