APLICACIONES DE LAS CONGRUENCIAS

Gregorio Hernández

UPM

Matemática Discreta I

Aritmética con números grandes

Por el T. Chino del resto, si $m_1, m_2, \ldots, m_n$ son primos entre sí entonces todo $a < m = m_1 m_2 \ldots m_n$ se representa de modo único

$a \leftrightarrow (a(\mathrm{mod}\ m_1), \ldots, a(\mathrm{mod}\ m_n))$

Ejemplo $m_1 = 3$ $m_2 = 4$ permiten representar de 0 a 11

$0 \leftrightarrow (0,0)$ $1 \leftrightarrow (1,1)$ $2 \leftrightarrow (2,2)$ $3 \leftrightarrow (0,3)$

$4 \leftrightarrow (1,0)$ $5 \leftrightarrow (2,1)$ $6 \leftrightarrow (0,2)$ $7 \leftrightarrow (1,3)$

$8 \leftrightarrow (2,0)$ $9 \leftrightarrow (3,1)$ $10 \leftrightarrow (1,2)$ $11 \leftrightarrow (2,3)$

¿Y si las operaciones con números mayores que 100 fueran lentas?

Se toman $m_1=99$, $m_2=98$, $m_3=97$, $m_4=95$ y se representa cada número menor que $99 \cdot 98 \cdot 97 \cdot 95 = 89403930$ por sus restos

$x = 123684 \quad \rightarrow \quad (33, 8, 9, 89)$

$y = 413456 \quad \rightarrow \quad (32,92,42,16)$

¿Cómo sumar $x + y$? Sumamos sus representaciones

$z = x + y \quad \rightarrow \quad (65, 2, 51, 10)$

Y resolvemos el sistema de congruencias

$$\left.\begin{array}{l} z \equiv 65 \pmod{99} \\ z \equiv 2 \pmod{98} \\ z \equiv 51 \pmod{97} \\ z \equiv 10 \pmod{95} \end{array}\right\} \quad z = 537140$$

Así sólo se trabaja con números mayores que 100 al final

Las computadoras utilizan módulos de la forma $2^k - 1$
Los módulos $2^{35} - 1$, $2^{34} - 1$, $2^{33} - 1$, $2^{31} - 1$, $2^{29} - 1$, $2^{23} - 1$, permiten trabajar con enteros $< 2^{184}$ de modo que sus representaciones no excedan de 2^{35}

Almacenamiento en memoria (Hashing)

2000 alumnos, 5000 posiciones de memoria

h: DNI $\rightarrow$ Memoria

k $\rightarrow$ h(k) h(k)=k(mod m) m=4969

si h(k)=h(k') COLISIÓN

Inspección lineal h(k) = k(mod m)
h(k')= k'+1 (mod m)
h(k')= k'+2 (mod m) ….

PROBLEMA DE ACUMULACIÓN

Doble direccionamiento g(k) = k+1 (mod m-2)

$h_1(k) = h(k) + g(k) \pmod m$

$h_2(k) = h(k) + 2g(k) \pmod m$

……..

$h_j(k) = h(k) + jg(k) \pmod m$

ISBN (International Standard Book Number)

84 - 316 - 3311 - 5 N. Biggs *Matemática Discreta*

84 idioma 316 editorial 3311 libro 5 dígito de control

$$\sum_{k=1}^{10} kx_k = 165 \quad \text{(múltiplo de 11)} \qquad x_{10} \equiv \sum_{k=1}^{9} kx_k \ (\text{mód}\ 11)$$

ISBN-13 compatibilidad con EAN-13

978 - 84 - 316 - 3311 -

Nuevo dígito de control 0

$$3 \sum_{\text{pos impar}} x_{pos} + \sum_{\text{pos par}} x_{pos} = 110$$

Complemento a 10

978 - 0 - 387 - 95584 -

Nuevo dígito de control 1

$$3 \sum_{\text{pos impar}} x_{pos} + \sum_{\text{pos par}} x_{pos} = 139$$

Complemento a 10

Números pseudoaleatorios

simulación de fenómenos en el ordenador

$x_1, x_2, \ldots, x_n, \ldots \qquad 0 \leq x_n < m$

$x_{n+1} = (a\, x_n + c)$ mód m

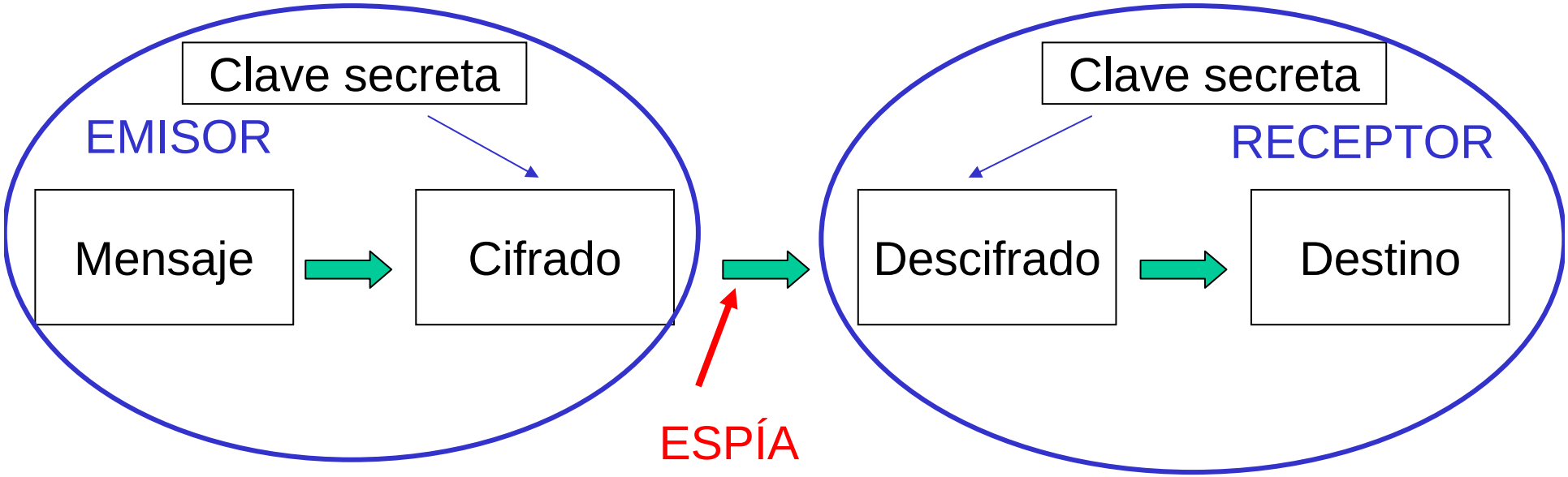
$x_1=2,\ m=9,\ c=0,\ a=4 \qquad 2, 8, 5, 2, 8, 5, \ldots$ repeticiones

Con los valores $m=2^{31}-1,\ a=7^5,\ c=0$
se garantizan $2^{31} - 2$ términos sin repeticiones

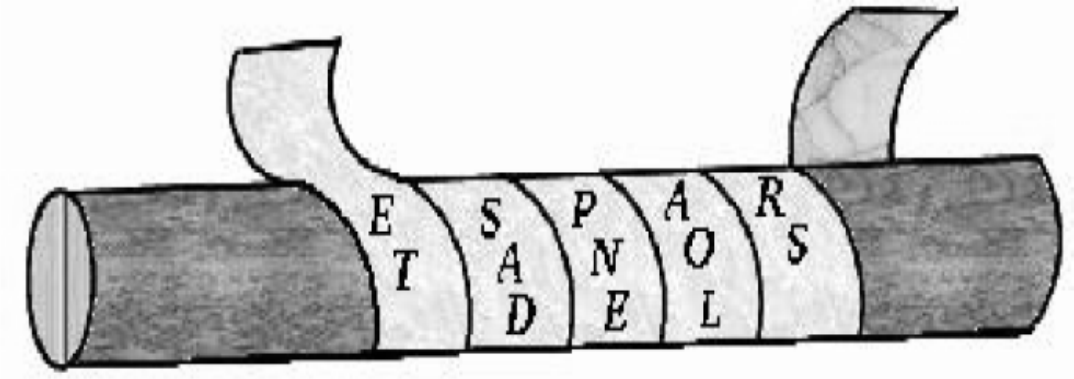
Criptografía

Criptoanálisis

El arte de enviar mensajes secretos …… y de descifrarlos



Escítalo espartano



Criptografía

Sustitución

J. César a b c d …. z → 01 02 03 … 27
d e f g … c → 04 05 06 … 03

Clave de cifrado $f(x)=ax+b(\text{mod } 27)$ $\text{mcd}(a,27)=1$ $(a=1, b=3)$

Descifrado $f^{-1}(q)= a^{-1}(q-b)$ (mód 27)

FÁCIL por medio de análisis de frecuencias

Sustitución polialfabética

Vigenère, 1586
Indescifrable hasta finales del siglo XIX
Babbage y Kasiski

Criptografía clásica (simétrica)

Número de claves
Intercambio seguro de claves

1976, Diffie, Hellman | Intercambio público de claves privadas

Alicia y Benito eligen (de forma pública) p primo y s<p

Alicia escoge a calcula $\alpha = s^a \pmod p$
Benito elige b calcula $\beta = s^b \pmod p$

Cada uno envía su cálculo

Alicia calcula $\beta^a = s^{ba} \pmod p$ Benito calcula $\alpha^b = s^{ab} \pmod p$

La **clave secreta** es $k = s^{ab}$

Un espía puede conocer p, s (son públicos) y detectar α
Para conocer a, necesita resolver un logaritmo discreto **MUY DÍFÍCIL**

Criptografía de clave pública

1978 sistema RSA (Rivest, Shamir, Adleman MIT)

p, q primos grandes $N=pq$
e primo con $(p-1)(q-1)$ } clave pública de A (N,e)

(1) Mensaje de B a A

$M \Rightarrow M(\text{numérico}) \Rightarrow (M_1, M_2, ..., M_r)$ (mensaje en bloques)

$C_k \equiv M_k^e \pmod N$ $C = (C_1, ..., C_r)$ mensaje cifrado

(2) ¿Cómo descifra A el mensaje?

mcd(e,(p-1)(q-1))=1, luego existe d tal que $ed = 1 + k(p-1)(q-1)$

$C^d = M^{ed} = M^{1+(k(p-1)(q-1)} = M(M^{p-1})^{k(q-1)} \equiv M \cdot 1 \pmod p$

análogamente $C^d \equiv M \cdot 1 \pmod q$, luego $C^d \equiv M \pmod N$

La clave privada de A es (N,d)

Un ejemplo con texto del mensaje ALTO

p=43, q=59 N=pq=2537
e=13 primo con (p-1)(q-1) clave pública de A (N,e)

Mensaje de B a A

ALTO $\Rightarrow$ 01122116 $\Rightarrow$ (0112, 2116)

$C_1 \equiv 0112^{13} \pmod N$ $C_2 \equiv 2116^{13} \pmod N$

mensaje cifrado C= (0933, 0316)

Para descifrar A utiliza d=937 pues $de \equiv 1 \pmod{42 \cdot 58}$

$0933^{937} \equiv 0112 \pmod N$ $0316^{937} \equiv 2116 \pmod N$

¿Cómo sabe A que el mensaje se lo envía B?

FIRMA DIGITAL