APLICACIONES DE LA ARITMÉTICA MODULAR

- Funciones de dispersión
- Números pseudoaleatorios
- Computación con números grandes
- Dígitos de control
- Criptografía
- Arte

FUNCIONES DE DISPERSIÓN

Hashing Functions

Se utilizan para asignar lugares de memoria a datos de forma que puedan ser recuperados rápidamente usando una clave.

Una de las más comunes es:

$$H(k) = k \text{ mód } m$$

Donde *m* es el número de posiciones de memoria existentes. El problema se presenta cuando el lugar está ya ocupado (colisión) y se suele resolver asignando la primera posición libre

FUNCIONES DE DISPERSIÓN

Hashing Functions

También se utilizan para garantizar la integridad de un texto en una transmisión:

Se divide el texto en bloques a los que se aplican diversas operaciones mód *m*.

El resultado se envía junto al texto.

El receptor repite los cálculos y la coincidencia en el resultado garantiza la integridad del envío.

La seguridad depende de *m* y de los cálculos efectuados.

NÚMEROS PSEUDOALEATORIOS

Son unos números generados por medio de una función (determinista, no aleatoria) y que aparentan ser aleatorios

NÚMEROS PSEUDOALEATORIOS

GENERADOR BBS

Entrada:

Dos primos grandes p,q congruentes con 3 módulo 4.

Un número e primo con $n=p \cdot q$.

Una semilla inicial $x_0 = e^2 \ mód \ n$.

La longitud de la salida k.

Algoritmo:

Para j = 1 hasta k:

a_1) $x_j=(x_{j-1})^2 \ mód \ n$

a_2) z_j=el bit menos significativo de x_j

Salida:

La sucesión $z_1, z_2, \ldots, z_k$.

COMPUTACIÓN CON NÚMEROS GRANDES

Dados $m_1, m_2, .., m_n$ números primos entre sí dos a dos. Todo entero $a < m = m_1\ m_2\ ..\ m_n$ puede ser representado de forma única por sus restos módulo m_i y recuperado mediante el teorema chino del resto

DÍGITOS DE CONTROL

- NIF
- ISBN
- NÚMERO DE UNA CUENTA CORRIENTE

NIF

El NIF es el resultado de aplicar al número del DNI mód 23 la siguiente tabla:

0 = T	**5 = M**	**10 = X**	**15 = S**	**20 = C**
1 = R	**6 = Y**	**11 = B**	**16 = Q**	**21 = K**
2 = W	**7 = F**	**12 = N**	**17 = V**	**22 = E**
3 = A	**8 = P**	**13 = J**	**18 = H**	
4 = G	**9 = D**	**14 = Z**	**19 = L**	

Sirve para detectar errores cometidos al introducir el número del DNI y para recuperar un dígito perdido

ISBN

El ISBN es un número de 10 cifras que identifica cualquier libro editado en el mundo

Las dos primeras cifras corresponden al país

Las cuatro siguientes a la editorial

Las tres siguientes al libro dentro de la editorial

La décima se obtiene $\sum_{i=1}^{9} i \cdot x_i \pmod{11}$ (X si se trata de 10).

También sirve para detectar errores cometidos al introducir el número o para recuperar un dígito perdido en la transmisión.

NÚMERO DE UNA CUENTA CORRIENTE

El número de una cuenta corriente consta de 20 dígitos.

El primer dígito de control vigila la entidad y la sucursal:

(7A + 3B + 6C + D + 2E + 4F + 8G + 5H) mód 11 (1 si es 10)

El segundo, el número de cuenta:

(10A + 9B + 7C + 3D + 6E + F + 2G + 4H + 8I + 5J) mód 11

SISTEMA DE CIFRADO RSA

Ron **R**ivest

Adi **S**hamir

Len **A**dleman

SISTEMA DE CIFRADO RSA

- Cifrado
- Descifrado
- RSA como sistema de clave pública
- Seguridad del sistema

CIFRADO RSA

El mensaje se cifra asignando a cada letra un entero. Estos enteros se agrupan en bloques que forman enteros más grandes.
Para codificar se usa la función:

$$C = M^{e} \bmod n$$

donde:

M = mensaje original

C = mensaje cifrado

$n = p \times q$ con p y q primos grandes (200 dígitos)

e = número primo con $(p-1)(q-1)$

DESCIFRADO RSA

Para descifrar se usa la función siguiente donde d es un inverso de e módulo $(p-1)(q-1)$:

$$C^{d} = (M^{e})^{d} = M^{ed} = M^{1+k(p-1)(q-1)}$$

Suponiendo que M no es múltiplo de p ni de q, lo que sucede en la mayoría de los casos :

$$M^{(p-1)} = 1 \bmod p$$

$$M^{(q-1)} = 1 \bmod q$$

$$M^{1+k(p-1)(q-1)} = M\,(M^{(p-1)})^{k(q-1)} = M \bmod p$$

$$M^{1+k(p-1)(q-1)} = M\,(M^{(q-1)})^{k(p-1)} = M \bmod q$$

DESCIFRADO RSA

Para descifrar se usa la función siguiente donde d es un inverso de e módulo $(p-1)(q-1)$:

$$C^d = (M^e)^d = M^{ed} = M^{1+k(p-1)(q-1)}$$

$$C^d = M \bmod p$$

$$C^d = M \bmod q$$

Y por el teorema Chino M, es la única solución $\bmod n$

$$C^d = M \bmod pq$$

RSA COMO SISTEMA DE CLAVE PÚBLICA

Clave pública:

$\boldsymbol{n}$ los primos $\boldsymbol{p}$ y $\boldsymbol{q}$ deben permanecer secretos

$\boldsymbol{e}$ primo con $\boldsymbol{(p-1)(q-1)}$

Clave privada:

$$\boldsymbol{d} = \boldsymbol{e}^{-1} \bmod \boldsymbol{(p-1)(q-1)}$$

SEGURIDAD DEL SISTEMA

- Si n es suficientemente grande, el tiempo necesario para factorizarlo es excesivo.
- Sin p y q es imposible encontrar d, necesario para descifrar el mensaje
- Cuando la mejora de los equipos permita factorizar n en un tiempo razonable, bastará aumentar n para recuperar la seguridad.

- MÚSICA
- ARTES VISUALES

http://britton.disted.camosun.bc.ca/modart/jbmodart2.htm