Matemáticas Discretas

Teoría de números y Criptografía

Nicolás Alvarado
nfalvarado@mat.uc.cl

Bernardo Barías
bjbarias@uc.cl

Sebastián Bugedo
bugedo@uc.cl

Gabriel Diéguez
gsdieguez@uc.cl

Departamento de Ciencia de la Computación
Escuela de Ingeniería
Pontificia Universidad Católica de Chile

20 de noviembre de 2023

Objetivos

1. Formular enunciados formales en notación matemática usando lógica, conjuntos, relaciones, funciones, cardinalidad, y otras herramientas, desarrollando definiciones y teoremas al respecto, así como demostrar o refutar estos enunciados, usando variadas técnicas.
2. Aplicar inducción como técnica para demostración de propiedades en conjuntos discretos y como técnica de definición formal de objetos discretos.
3. Aplicar propiedades y resultados de aritmética modular al estudio de números primos, congruencias y criptografía.

Contenidos

Bibliografía

- Apuntes Luis Dissett, capítulo 11.
- Rosen: capítulo 4.

Recordemos. . .

Definición

La relación *divide a*, denotada por $|$, sobre los enteros sin el 0, es una relación tal que a está relacionado con b si y sólo si b es múltiplo de a:

$$a|b \text{ si y sólo si } \exists k \in \mathbb{Z} \text{ tal que } b = ka.$$

$$3|9 \qquad 18|72 \qquad 7 \not| 9 \qquad 2|-4$$

Recordemos. . .

Definición

La relación *equivalencia módulo* n, denotada por $\equiv_n$, sobre los enteros, es una relación tal que a está relacionado con b si y sólo si $n|(b-a)$:

$$a \equiv_n b \text{ si y sólo si } n|(b-a)$$
$$a \equiv_n b \text{ si y sólo si } \exists k \in \mathbb{Z} \text{ tal que } (b-a) = kn.$$

Por ejemplo, dado $n = 7$:

$$2 \equiv_7 23 \qquad 8 \equiv_7 1 \qquad 19 \not\equiv_7 4 \qquad -3 \equiv_7 4$$

Recordemos. . .

- La relación $\equiv_n$ es una relación de equivalencia.
- Podemos tomar el conjunto cuociente generado por ella sobre $\mathbb{Z}$.
- Usando las clases de equivalencia, definimos la suma y la multiplicación.

Definición

Dado $n \in \mathbb{N}$, $n > 0$, definimos

$$\mathbb{Z}_n = \mathbb{Z}/\equiv_n$$

y sus operaciones

$$[i] + [j] = [i + j]$$
$$[i] \cdot [j] = [i \cdot j]$$

Recordemos. . .

Por simplicidad, renombramos las clases de equivalencia como los números que representan.

Ejemplo

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

Calcule $37 + 18$ y $26 \cdot 37$.

Recordemos. . .

Ejemplo

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

Calcule $37 + 18$ y $26 \cdot 37$.

$$37 + 18 = [37] + [18] = [37 + 18] = [55] = [0]$$
$$26 \cdot 37 = [26] \cdot [37] = [26 \cdot 37] = [962] = [2]$$

Aritmética modular

Dados dos enteros a y n, siempre podemos expresar a en términos de n como $a = \alpha \cdot n + \beta$, donde $\alpha = \left\lfloor \frac{a}{n} \right\rfloor$ es la división entera de a por n, y β es el resto de esa división, con $\alpha, \beta \in \mathbb{Z}$ y $\beta \geq 0$.

Ejemplo

Dados $a = 3$ y $n = 2$, podemos escribir

$$a = \left\lfloor \frac{3}{2} \right\rfloor \cdot 2 + 1 = 1 \cdot 2 + 1$$

Definición

La operación **módulo** n entrega el resto de la división por n.
Se escribe a mod n.

Ejemplo

$3 \text{ mod } 2 = 1$

Aritmética modular

Con esta operación podemos redefinir la suma y la multiplicación en $\mathbb{Z}_n$:

$$[i] + [j] = (i + j) \bmod n$$
$$[i] \cdot [j] = (i \cdot j) \bmod n$$

Una observación importante es que siempre se cumple que

$$0 \leq a \bmod n < n$$

- ¿Por qué?

Aritmética modular

Teorema

$a \equiv_n b$ si y sólo si $a \bmod n = b \bmod n$.

Ejercicio

Demuestre el teorema.

Teorema

$a \equiv_n b$ si y sólo si $a \bmod n = b \bmod n$.

En primer lugar, sabemos que podemos escribir a y b en términos de n:

$$a = \alpha \cdot n + a \bmod n \tag{1}$$
$$b = \gamma \cdot n + b \bmod n \tag{2}$$

donde $\alpha, \gamma \in \mathbb{Z}$ son los resultados de las divisiones enteras.

($\Leftarrow$) Suponemos que $a \bmod n = b \bmod n$. Por demostrar: $a \equiv_n b$.

Si restamos $(2) - (1)$ obtenemos $b - a = (\gamma - \alpha) \cdot n$, de donde es claro que $n \mid (b - a)$, pues $(\gamma - \alpha) \in \mathbb{Z}$. Por lo tanto, se cumple que $a \equiv_n b$.

Teorema

$a \equiv_n b$ si y sólo si $a \bmod n = b \bmod n$.

($\Rightarrow$) Por contrapositivo, suponemos que $a \bmod n \neq b \bmod n$ (3). Por demostrar: $a \not\equiv_n b$.

Sin pérdida de generalidad, asumimos que $a \bmod n < b \bmod n$ (4). Si restamos $(2) - (1)$ obtenemos $b - a = (\gamma - \alpha) \cdot n + (b \bmod n - a \bmod n)$. Como

$$0 \leq a \bmod n, b \bmod n < n$$

por (4) se tiene que $1 \leq (b \bmod n - a \bmod n) \leq b \bmod n < n$. Por lo tanto, $n \not| (b - a)$, de donde concluimos que $a \not\equiv_n b$.

Aritmética modular

Corolario

$a \equiv_n a \bmod n$

Ejercicio

Demuestre el corolario.

Corolario

$a \equiv_n a \bmod n$

Como sabemos que $a \bmod n < n$, se tiene que $\left\lfloor \frac{a \bmod n}{n} \right\rfloor = 0$. Luego, si expresamos $a \bmod n$ en términos de n:

$$a \bmod n = 0 \cdot n + (a \bmod n) \bmod n$$
$$a \bmod n = (a \bmod n) \bmod n$$

y por el teorema anterior, $a \equiv_n a \bmod n$.

Aritmética modular

Teorema

Si $a \equiv_n b$ y $c \equiv_n d$, entonces

- $(a + c) \equiv_n (b + d)$
- $(a \cdot c) \equiv_n (b \cdot d)$

Ejercicio

Demuestre el teorema.

Teorema

Si $a \equiv_n b$ y $c \equiv_n d$, entonces

- $(a + c) \equiv_n (b + d)$
- $(a \cdot c) \equiv_n (b \cdot d)$

Como $a \equiv_n b$, por definición sabemos que $n \mid (b - a)$, y nuevamente por definición tenemos que $b - a = k_1 \cdot n$. Si despejamos b, y procedemos análogamente desde $c \equiv_n d$:

$$b = a + k_1 \cdot n \tag{1}$$

$$d = c + k_2 \cdot n \tag{2}$$

Aritmética modular

Teorema

Si $a \equiv_n b$ y $c \equiv_n d$, entonces $(a + c) \equiv_n (b + d)$.

$$b = a + k_1 \cdot n \tag{1}$$
$$d = c + k_2 \cdot n \tag{2}$$

Sumamos (1) y (2):

$$\begin{aligned} & b + d = a + c + (k_1 + k_2) \cdot n \\ \Leftrightarrow \quad & (b + d) - (a + c) = k_3 \cdot n \\ \Leftrightarrow \quad & n \mid (b + d) - (a + c) \\ \Leftrightarrow \quad & a + c \equiv_n b + d \end{aligned}$$

Aritmética modular

Teorema

Si $a \equiv_n b$ y $c \equiv_n d$, entonces $(a \cdot c) \equiv_n (b \cdot d)$.

$$b = a + k_1 \cdot n \tag{1}$$
$$d = c + k_2 \cdot n \tag{2}$$

Multiplicamos (1) y (2):

$$\begin{aligned}
& b \cdot d = (a + k_1 \cdot n)(c + k_2 \cdot n) \\
\Leftrightarrow \quad & = a \cdot c + (a \cdot k_2 + c \cdot k_1 + n \cdot k_1 \cdot k_2) \cdot n \\
\Leftrightarrow \quad & b \cdot d - a \cdot c = k_4 \cdot n \\
\Leftrightarrow \quad & n \mid b \cdot d - a \cdot c \\
\Leftrightarrow \quad & a \cdot c \equiv_n b \cdot d
\end{aligned}$$

Aritmética modular

Corolario

$(a + b) \bmod n = ((a \bmod n) + (b \bmod n)) \bmod n$
$a \cdot b \bmod n = ((a \bmod n)(b \bmod n)) \bmod n$

Ejercicio

Demuestre el corolario.

Ejercicio

Calcule $(55 \cdot 26) \bmod 4$.

Ejercicio

Demuestre que un número es divisible por 3 si y sólo si la suma de sus dígitos es divisible por 3.

Aritmética modular

Corolario

$(a + b) \bmod n = ((a \bmod n) + (b \bmod n)) \bmod n$
$a \cdot b \bmod n = ((a \bmod n)(b \bmod n)) \bmod n$

Por teorema anterior sabemos que $a \equiv_n a \bmod n$ y $b \equiv_n b \bmod n$.
Aplicando el teorema de sumas y multiplicaciones:

$$a + b \equiv_n (a \bmod n) + (b \bmod n)$$
$$\Leftrightarrow \quad (a + b) \bmod n = ((a \bmod n) + (b \bmod n)) \bmod n$$

$$a \cdot b \equiv_n (a \bmod n) \cdot (b \bmod n)$$
$$\Leftrightarrow \quad (a \cdot b) \bmod n = ((a \bmod n)(b \bmod n)) \bmod n$$

Ejercicio

Calcule $(55 \cdot 26) \bmod 4$.

$$\begin{aligned}(55 \cdot 26) \bmod 4 &= (55 \bmod 4 \cdot 26 \bmod 4) \bmod 4 \\ &= (3 \cdot 2) \bmod 4 \\ &= 6 \bmod 4 \\ &= 2\end{aligned}$$

Ejercicio

Demuestre que un número es divisible por 3 si y sólo si la suma de sus dígitos es divisible por 3.

Sabemos que un número entero n se puede representar como

$$n = d_k \cdot 10^k + \cdots + d_1 \cdot 10 + d_0 \tag{1}$$

donde d_i es el dígito i-ésimo de n. Por ejemplo:

$$1347 = 1 \cdot 10^3 + 3 \cdot 10^2 + 4 \cdot 10 + 7$$

Ahora, tenemos que n será divisible por 3 si y sólo si $n \bmod 3 = 0$.

Ejercicio

Demuestre que un número es divisible por 3 si y sólo si la suma de sus dígitos es divisible por 3.

Tomamos mod 3 en (1) y usamos el teorema de suma y multiplicación:

$$\begin{aligned} n \bmod 3 =& (d_k \cdot 10^k + \cdots + d_1 \cdot 10 + d_0) \bmod 3 \\ =& ((d_k \cdot 10^k) \bmod 3 + \cdots + (d_1 \cdot 10) \bmod 3 + d_0 \bmod 3) \bmod 3 \\ =& ((d_k \bmod 3 \cdot 10^k \bmod 3) \bmod 3 + \cdots \\ & + (d_1 \bmod 3 \cdot 10 \bmod 3) \bmod 3 + d_0 \bmod 3) \bmod 3 \end{aligned}$$

Ejercicio

Demuestre que un número es divisible por 3 si y sólo si la suma de sus dígitos es divisible por 3.

Notemos que $\forall k \geq 1, 10^k \bmod 3 = 1$. Por lo tanto:

$$\begin{aligned} n \bmod 3 =& ((d_k \bmod 3 \cdot 1) \bmod 3 + \cdots \\ & + (d_1 \bmod 3 \cdot 1) \bmod 3 + d_0 \bmod 3) \bmod 3 \\ =& ((d_k \bmod 3) \bmod 3 + \cdots \\ & + (d_1 \bmod 3) \bmod 3 + d_0 \bmod 3) \bmod 3 \\ =& (d_k \bmod 3 + \cdots + d_1 \bmod 3 + d_0 \bmod 3) \bmod 3 \\ =& (d_k + \cdots + d_1 + d_0) \bmod 3 \end{aligned}$$

Luego, $n \bmod 3 = 0$ si y sólo si $(d_k + \cdots + d_1 + d_0) \bmod 3 = 0$; es decir, si la suma de los dígitos de n es divisible por 3.

Aritmética modular

Teorema (Fermat)

Si p es un número primo, para cualquier entero a se cumple que $a^p \equiv_p a$.

Ejercicio

Demuestre el teorema.

Teorema (Fermat)

Si p es un número primo, para cualquier entero a se cumple que $a^p \equiv_p a$.

Nos pondremos en dos casos.

Caso 1: $a \geq 0$. Se hará la demostración por inducción sobre el valor de a.

BI: $a = 0 \to 0^p = 0 \equiv_p 0$

$a = 1 \to 1^p = 1 \equiv_p 1$

HI: Suponemos que $a^p \equiv_p a$. Notemos que esto implica que $p \mid a^p - a$.

TI: Por demostrar: $(a+1)^p \equiv_p (a+1)$, o equivalentemente, que

$$p \mid (a+1)^p - (a+1), \text{ con } 2 \leq a+1 \tag{1}$$

Teorema (Fermat)

Si p es un número primo, para cualquier entero a se cumple que $a^p \equiv_p a$.

$$\text{PD: } p \mid (a+1)^p - (a+1), \text{ con } 2 \leq a+1 < p. \tag{1}$$

Por el teorema del binomio, sabemos que $(a+1)^p = \sum_{k=0}^{p} \binom{p}{k} a^k$, con $\binom{p}{k} = \frac{p!}{k!(p-k)!}$. Desarrollamos la parte derecha de (1):

$$\begin{aligned}(a+1)^p - (a+1) &= \sum_{k=0}^{p} \binom{p}{k} a^k - (a+1) \\ &= \sum_{k=1}^{p-1} \binom{p}{k} a^k + \binom{p}{0} a^0 + \binom{p}{p} a^p - (a+1)\end{aligned}$$

Teorema (Fermat)

Si p es un número primo, para cualquier entero a se cumple que $a^p \equiv_p a$.

$$
\begin{aligned}
(a+1)^p - (a+1) &= \sum_{k=0}^{p} \binom{p}{k} a^k - (a+1) \\
&= \sum_{k=1}^{p-1} \binom{p}{k} a^k + \binom{p}{0} a^0 + \binom{p}{p} a^p - (a+1) \\
&= \sum_{k=1}^{p-1} \binom{p}{k} a^k + 1 + a^p - a - 1 \\
&= (a^p - a) + \sum_{k=1}^{p-1} \binom{p}{k} a^k
\end{aligned}
$$

Teorema (Fermat)

Si p es un número primo, para cualquier entero a se cumple que $a^p \equiv_p a$.

Tenemos entonces que

$$(a+1)^p - (a+1) = (a^p - a) + \sum_{k=1}^{p-1} \binom{p}{k} a^k$$

Por HI, sabemos que $p \mid a^p - a$. Por demostrar: $p \mid \sum_{k=1}^{p-1} \binom{p}{k} a^k$.

Demostraremos que $\forall k \in \{1, \ldots, p-1\}, p \mid \binom{p}{k}$. Tenemos que

$$\begin{aligned}\binom{p}{k} &= \frac{p!}{k!(p-k)!} = \frac{p(p-1)\cdots(p-k+1)(p-k)!}{k!(p-k)!} \\ &= \frac{p(p-1)\cdots(p-k+1)}{k!}\end{aligned}$$

Teorema (Fermat)

Si p es un número primo, para cualquier entero a se cumple que $a^p \equiv_p a$.

Tenemos entonces que

$$\binom{p}{k} = \frac{p(p-1)\cdots(p-k+1)}{k!}$$

Como los coeficientes binomiales son enteros, el numerador debe ser divisible por el denominador. Como p es primo y $k < p$, sabemos que entre los factores de $k!$ no puede haber divisores de p, por lo que necesariamente

$$\frac{(p-1)\cdots(p-k+1)}{k!} \in \mathbb{Z}, \text{ y entonces}$$

$$\binom{p}{k} = p \cdot \alpha, \text{ con } \alpha \in \mathbb{Z}, \text{ y por lo tanto } p \mid \binom{p}{k}.$$

Teorema (Fermat)

Si p es un número primo, para cualquier entero a se cumple que $a^p \equiv_p a$.

En conclusión, tenemos que

$$p \mid (a+1)^p - (a+1)$$

y por lo tanto

$$(a+1)^p \equiv_p (a+1)$$

como queríamos demostrar.

Se sigue entonces por inducción el teorema planteado para $a \geq 0$.

Teorema (Fermat)

Si p es un número primo, para cualquier entero a se cumple que $a^p \equiv_p a$.

Caso 2: $a < 0$. Sabemos que $a \equiv_p a \bmod p$, y por teorema de multiplicación $a^p \equiv_p (a \bmod p)^p$. Ahora, como $a \bmod p \geq 0$, corresponde al caso 1 recién demostrado, y por lo tanto $(a \bmod p)^p \equiv_p a \bmod p$. Finalmente, tenemos que

$$a^p \equiv_p (a \bmod p)^p \equiv_p a \bmod p \equiv_p a$$

y entonces $a^p \equiv_p a$.

Aritmética modular

Corolario (Fermat)

Si p es un número primo y a es un entero que no es múltiplo de p, entonces $a^{p-1} \equiv_p 1$.

Ejercicio

Demuestre el corolario.

Corolario (Fermat)

Si p es un número primo y a es un entero que no es múltiplo de p, entonces $a^{p-1} \equiv_p 1$.

Por el teorema anterior:

$$a^p \equiv_p a \Rightarrow p \mid a^p - a \Rightarrow a^p - a = k \cdot p \tag{1}$$

Notemos que $a \mid a^p - a$, y por lo tanto $a \mid k \cdot p$. Como p es primo y a no es múltiplo de p, necesariamente $a \mid k$. Dividiendo (1) por a:

$$a^{p-1} - 1 = \frac{k}{a} \cdot p, \text{ con } \frac{k}{a} \in \mathbb{Z}.$$

Por lo tanto:

$$p \mid a^{p-1} - 1 \Rightarrow 1 \equiv_p a^{p-1} \Rightarrow a^{p-1} \equiv_p 1$$

Máximo común divisor

Definición (de colegio)

Dados dos números a y b, su **máximo común divisor**, denotado como $MCD(a, b)$, es el máximo natural n tal que $n|a$ y $n|b$.

¿Cómo podemos calcularlo?

Máximo común divisor

Teorema (Algoritmo de Euclides)

Si $b > 0$, entonces $MCD(a, b) = MCD(b, a \bmod b)$.

Ejercicio

Demuestre el teorema.

Máximo común divisor

Teorema (Algoritmo de Euclides)

Si $b > 0$, entonces $MCD(a, b) = MCD(b, a \bmod b)$.

Demostraremos que un entero c divide a a y a b si y sólo si divide a b y $a \bmod b$. De esto se concluye el teorema.

Sabemos que $a = k \cdot b + a \bmod b$ (1).

$(\Rightarrow)$ Suponemos que $c \mid a$ y $c \mid b$. Si despejamos $a \bmod b$ desde (1), obtenemos que $a \bmod b = a - k \cdot b$, de donde se concluye que $c \mid a \bmod b$.

$(\Leftarrow)$ Suponemos que $c \mid b$ y $c \mid a \bmod b$. De (1) se concluye que $c \mid a$.

Máximo común divisor

Entonces:

$$MCD(a,b) = \begin{cases} a & b = 0 \\ MCD(b, a \bmod b) & b > 0 \end{cases}$$

Ejercicio

Calcule $MCD(403, 156)$.

Máximo común divisor

Entonces:

$$MCD(a,b) = \begin{cases} a & b = 0 \\ MCD(b, a \bmod b) & b > 0 \end{cases}$$

Ejercicio

Calcule $MCD(403, 156)$.

$$\begin{aligned} MCD(403,156) &= MCD(156, 403 \bmod 156) = MCD(156,91) \\ &= MCD(91, 156 \bmod 91) = MCD(91,65) \\ &= MCD(65, 91 \bmod 65) = MCD(65,26) \\ &= MCD(26, 65 \bmod 26) = MCD(26,13) \\ &= MCD(13, 26 \bmod 13) = MCD(13,0) \\ &= 13 \end{aligned}$$

Máximo común divisor

Un resultado importante relacionado al MCD:

Teorema (Identidad de Bézout)

Si $a, b \in \mathbb{Z}$, entonces existen $s, t \in \mathbb{Z}$ tales que

$$MCD(a, b) = s \cdot a + t \cdot b$$

- El máximo común divisor de a, b se puede escribir como una **combinación lineal** de a y b.
- s y t se conocen como los **coeficientes de Bézout** de a y b.
  - No necesariamente son únicos.
- Para demostrar el teorema, vamos a extender el algoritmo de Euclides para que, además del MCD de a y b, nos entregue algún par de coeficientes de Bézout.

Máximo común divisor

Algoritmo de Euclides extendido

Sea $a \geq b$.

1. Definimos una sucesión $\{r_i\}$ como:

$$r_0 = a,\ r_1 = b,\ r_{i+1} = r_{i-1} \bmod r_i$$

2. Definimos sucesiones $\{s_i\}$, $\{t_i\}$ tales que:

$$s_0 = 1, t_0 = 0$$
$$s_1 = 0, t_1 = 1$$
$$r_i = s_i \cdot a + t_i \cdot b$$

3. Calculamos estas sucesiones hasta un k tal que $r_k = 0$.
4. Entonces, $MCD(a, b) = r_{k-1} = s_{k-1} \cdot a + t_{k-1} \cdot b$.

Máximo común divisor

Ejercicio

Demuestre que

$$s_{i+1} = s_{i-1} - \left\lfloor \frac{r_{i-1}}{r_i} \right\rfloor \cdot s_i$$

$$t_{i+1} = t_{i-1} - \left\lfloor \frac{r_{i-1}}{r_i} \right\rfloor \cdot t_i$$

Máximo común divisor

En la sucesión definimos que $r_{i+1} = r_{i-1} \bmod r_i$. Escribimos r_{i-1} como división de r_i:

$$r_{i-1} = \left\lfloor \frac{r_{i-1}}{r_i} \right\rfloor \cdot r_i + r_{i-1} \bmod r_i \tag{1}$$

$$r_{i-1} = \left\lfloor \frac{r_{i-1}}{r_i} \right\rfloor \cdot r_i + r_{i+1} \tag{2}$$

En la sucesión también definimos que $r_{i-1} = s_{i-1} \cdot a + t_{i-1} \cdot b$ (3). Reemplazamos (3) en la parte izquierda de (2) y despejamos r_{i+1}:

$$s_{i-1} \cdot a + t_{i-1} \cdot b = \left\lfloor \frac{r_{i-1}}{r_i} \right\rfloor \cdot r_i + r_{i+1}$$

$$r_{i+1} = s_{i-1} \cdot a + t_{i-1} \cdot b - \left\lfloor \frac{r_{i-1}}{r_i} \right\rfloor \cdot r_i$$

Máximo común divisor

$$r_{i+1} = s_{i-1} \cdot a + t_{i-1} \cdot b - \left\lfloor \frac{r_{i-1}}{r_i} \right\rfloor \cdot r_i$$

Como $r_i = s_i \cdot a + t_i \cdot b$:

$$r_{i+1} = s_{i-1} \cdot a + t_{i-1} \cdot b - \left\lfloor \frac{r_{i-1}}{r_i} \right\rfloor \cdot (s_i \cdot a + t_i \cdot b)$$

$$r_{i+1} = \left(s_{i-1} - \left\lfloor \frac{r_{i-1}}{r_i} \right\rfloor \cdot s_i \right) \cdot a + \left(t_{i-1} - \left\lfloor \frac{r_{i-1}}{r_i} \right\rfloor \cdot t_i \right) \cdot b$$

Y como $r_{i+1} = s_{i+1} \cdot a + t_{i+1} \cdot b$:

$$s_{i+1} = s_{i-1} - \left\lfloor \frac{r_{i-1}}{r_i} \right\rfloor \cdot s_i \qquad t_{i+1} = t_{i-1} - \left\lfloor \frac{r_{i-1}}{r_i} \right\rfloor \cdot t_i$$

Máximo común divisor

Algoritmo de Euclides extendido

Sea $a \geq b$.

1. Definimos una sucesión $\{r_i\}$ como:

$$r_0 = a,\ r_1 = b,\ r_{i+1} = r_{i-1} \bmod r_i$$

2. Definimos sucesiones $\{s_i\}$, $\{t_i\}$ tales que:

$$s_0 = 1, \quad t_0 = 0$$
$$s_1 = 0, \quad t_1 = 1$$
$$s_{i+1} = s_{i-1} - \left\lfloor \frac{r_{i-1}}{r_i} \right\rfloor \cdot s_i, \quad t_{i+1} = t_{i-1} - \left\lfloor \frac{r_{i-1}}{r_i} \right\rfloor \cdot t_i$$

3. Calculamos estas sucesiones hasta un k tal que $r_k = 0$.
4. Entonces, $MCD(a, b) = r_{k-1} = s_{k-1} \cdot a + t_{k-1} \cdot b$.

Máximo común divisor

Ejercicio

Dados $a = 60$ y $b = 13$, use el algoritmo para calcular $MCD(a, b)$ y $s, t \in \mathbb{Z}$ tales que $MCD(a, b) = s \cdot a + t \cdot b$.

Máximo común divisor

Ejercicio

Dados $a = 60$ y $b = 13$, use el algoritmo para calcular $MCD(a, b)$ y $s, t \in \mathbb{Z}$ tales que $MCD(a, b) = s \cdot a + t \cdot b$.

Inicialmente: $r_0 = a = 60 \quad s_0 = 1 \quad t_0 = 0$

$r_1 = b = 13 \quad s_1 = 0 \quad t_1 = 1$

Entonces:

$$r_2 = r_0 \bmod r_1 = 60 \bmod 13 = 8$$

$$s_2 = s_0 - \left\lfloor \frac{r_0}{r_1} \right\rfloor \cdot s_1 = 1 - 4 \cdot 0 = 1$$

$$t_2 = t_0 - \left\lfloor \frac{r_0}{r_1} \right\rfloor \cdot t_1 = 0 - 4 \cdot 1 = -4$$

$$r_3 = r_1 \bmod r_2 = 13 \bmod 8 = 5$$

$$s_3 = s_1 - \left\lfloor \frac{r_1}{r_2} \right\rfloor \cdot s_2 = 0 - 1 \cdot 1 = -1$$

$$t_3 = t_1 - \left\lfloor \frac{r_1}{r_2} \right\rfloor \cdot t_2 = 1 - 1 \cdot -4 = 5$$

Máximo común divisor

Ejercicio

Dados $a = 60$ y $b = 13$, use el algoritmo para calcular $MCD(a, b)$ y $s, t \in \mathbb{Z}$ tales que $MCD(a, b) = s \cdot a + t \cdot b$.

$$
\begin{array}{lll}
r_0 = 60 & s_0 = 1 & t_0 = 0 \\
r_1 = 13 & s_1 = 0 & t_1 = 1 \\
r_2 = 8 & s_2 = 1 & t_2 = -4 \\
r_3 = 5 & s_3 = -1 & t_3 = 5 \\
r_4 = 3 & s_4 = 2 & t_4 = -9 \\
r_5 = 2 & s_5 = -3 & t_5 = 14 \\
r_6 = 1 & s_6 = 5 & t_6 = -23 \\
r_7 = r_5 \bmod r_6 = 2 \bmod 1 = 0 &&
\end{array}
$$

Por lo tanto:

$$
\begin{aligned}
MCD(60, 13) &= r_6 = 1 \\
&= s_6 \cdot a + t_6 \cdot b = 5 \cdot 60 + (-23) \cdot 13
\end{aligned}
$$

Inversos modulares

Definición

b es **inverso** de a en módulo n si $a \cdot b \equiv_n 1$.

Podemos denotarlo como a^{-1}. Ojo: no es lo mismo que $\frac{1}{a}$.

Ejemplo

1337 es inverso de 3 en módulo 4010.

- ¿Siempre existe el inverso modular?
  - No. Por ejemplo, 2 no tiene inverso en módulo 4.
- ¿Bajo qué condiciones a tiene inverso en módulo n?
- ¿Cómo podemos calcularlo?

Inversos modulares

Teorema

a tiene inverso en módulo n si y sólo si $MCD(a, n) = 1$.

Ejercicio

Demuestre el teorema.

En este caso, diremos que a y n son *primos relativos* (o coprimos o primos entre sí).

Inversos modulares

Teorema

a tiene inverso en módulo n si y sólo si $MCD(a, n) = 1$.

($\Rightarrow$) Supongamos que a tiene inverso en módulo n, digamos b. Por demostrar: $MCD(a, n) = 1$.

Como b es el inverso de a en módulo n, se cumple que $a \cdot b \equiv_n 1$, y por lo tanto $(a \cdot b) \bmod n = 1$. Entonces, tenemos que $a \cdot b = k \cdot n + 1$, y despejando 1 obtenemos que $1 = a \cdot b - k \cdot n$. Luego, necesariamente cualquier entero c tal que $c \mid a$ y $c \mid n$ debe cumplir que $c \mid 1$, por lo que la única posibilidad es que c sea 1, y por lo tanto necesariamente $MCD(a, n) = 1$.

Inversos modulares

Teorema

a tiene inverso en módulo n si y sólo si $MCD(a, n) = 1$.

($\Leftarrow$) Supongamos que $MCD(a, n) = 1$. Por demostrar: a tiene inverso en módulo n.

Si ejecutamos el algoritmo de Euclides extendido obtenemos s, t tales que

$$\begin{aligned} & 1 = s \cdot a + t \cdot n \\ \Leftrightarrow \quad & a \cdot s = (-t) \cdot n + 1 \\ \Leftrightarrow \quad & a \cdot s \bmod n = 1 \\ \Leftrightarrow \quad & a \cdot s \equiv_n 1 \end{aligned}$$

Y entonces a tiene inverso en módulo 1, s.

Inversos modulares

Notemos que la demostración nos da un método para calcular el inverso:

- Usamos el algoritmo de Euclides extendido para encontrar s y t tales que $1 = s \cdot a + t \cdot n$.
- s será el inverso de a en módulo n.

Notación

Dados $a, b, n \in \mathbb{Z}$, si $a \equiv_n b$ también podemos escribir:

$$a \equiv b \pmod{n}$$

Esta es la notación más usada en la literatura.

Ecuaciones de congruencia

Definición

Una **congruencia lineal** es una ecuación de la forma

$$ax \equiv b \pmod{n}$$

donde $n \in \mathbb{N} - \{0\}$, $a, b \in \mathbb{Z}$ y x es una variable.

Ejemplos

$$3x \equiv 2 \pmod{7}$$
$$4x \equiv 3 \pmod{6}$$

¿Cómo resolvemos estas ecuaciones? ¡Con inversos!

Ecuaciones de congruencia

Corolario (del teorema de los inversos)

Si a y n son primos relativos, entonces $ax \equiv b \pmod{n}$ tiene solución en $\mathbb{Z}_n$.

Ejercicio

Demuestre el corolario.

Ejercicio

Resuelva las ecuaciones anteriores.

Ecuaciones de congruencia

Corolario (del teorema de los inversos)

Si a y n son primos relativos, entonces $ax \equiv b \pmod{n}$ tiene solución en $\mathbb{Z}_n$.

Como a y n son primos relativos, a tiene inverso en módulo n. Entonces:

$$\begin{aligned} & ax \equiv b \pmod{n} \text{ multiplicamos por } a^{-1} \\ \Leftrightarrow \quad & (a^{-1} \cdot a)x \equiv (a^{-1} \cdot b) \pmod{n} \\ \Leftrightarrow \quad & x \equiv (a^{-1} \cdot b) \pmod{n} \end{aligned}$$

Ecuaciones de congruencia

Ejercicio

Resuelva $3x \equiv 2 \pmod{7}$.

El inverso de 3 en módulo 7 es 5: $3 \cdot 5 = 15 \equiv 1 \pmod{7}$.

$$\begin{aligned} x &\equiv 5 \cdot 2 \pmod{7} \\ &\equiv 10 \pmod{7} \\ &\equiv 3 \pmod{7} \end{aligned}$$

$x = 3$ es solución en $\mathbb{Z}_7$.

Criptografía

- La criptografía es el estudio de métodos para enviar y recibir mensajes en privado.
- El interés en el área viene desde la antigüedad...

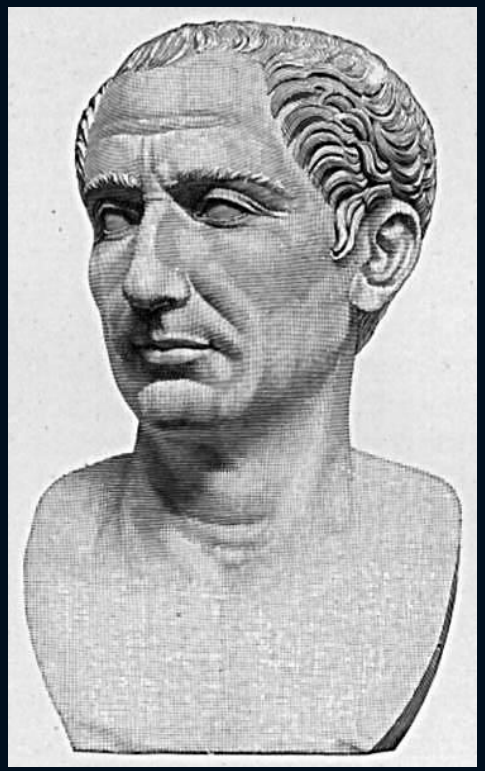

Figura: Julio César

Criptografía

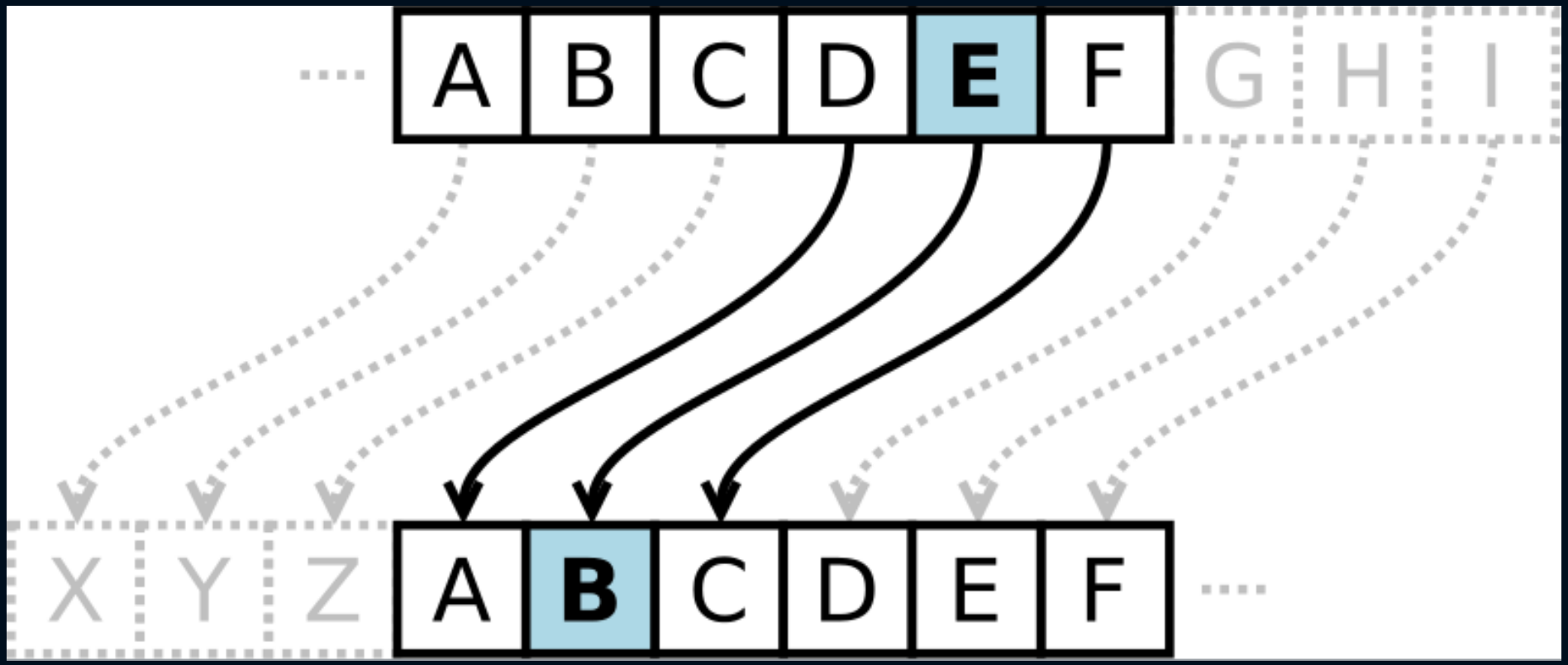

Figura: Julio César usaba este método para su correspondencia privada

Criptografía

Con lo que sabemos, podemos formalizar esto...

Cifrado del César

Input: letra $M \in \{0, \ldots, 26\}$

Output: letra cifrada $C = (M + 3) \bmod 27$

Ejercicio

Cifre el mensaje "holamundo".

Criptografía

Podemos generalizar el cifrado del César:

Cifrado del César generalizado

Dado un número d:

Input: letra $M \in \{0, \ldots, 26\}$

Output: letra cifrada $C = (M + d) \bmod 27$

Criptografía

En criptografía y teoría de la comunicación, se habla de dos agentes A y B (Alice y Bob) que desean comunicarse.

- Alice desea enviar el mensaje $M =$ "holamundo" a Bob privadamente.
- Elige un número d y envía $C = (M + d) \bmod 27$.
- Bob obtiene el mensaje C.

A M se le conoce como el **texto plano**, a C como el **texto cifrado** y a d como la **llave**.

Criptografía

¿Como recupera Bob el mensaje original?

- Necesita la llave d.
- Con ella: $M = (C - d) \bmod 27$.

Ejercicio

Demuestre que para todo d y M, si $C = (M + d) \bmod 27$ y $M' = (C - d) \bmod 27$, entonces $M = M'$.

Criptografía

Bob necesita la llave...

- ¿Cómo puede obtenerla?
- Alice se la envía.
- ¿Cómo se puede hacer esto de manera segura?
- Suponiendo que se puede, ¿es suficiente protección?

Criptografía asimétrica de clave pública

Vimos que tener sólo una clave es muy inseguro. Estudiaremos ahora sistemas criptográficos que tienen las siguientes características:

- Se tienen dos funciones E y D.
- E sirve para encriptar y D para desencriptar: $D(E(M)) = M$.
- E no puede usarse para desencriptar: $E(E(M)) \neq M$.
- E y D están relacionadas, pero es difícil descubrir D a partir de E.

Uno de estos sistemas es RSA, y es el que estudiaremos.

El sistema criptográfico RSA

Algoritmo RSA

1. Adivinar dos números primos distintos P y Q.
2. Calcular $N = P \cdot Q$ y $\phi(N) = (P-1) \cdot (Q-1)$.
3. Sean e y d dos números tales que $(e \cdot d)$ mod $\phi(N) = 1$.
4. Entonces:

$$E(M) = M^e \text{ mod } N$$
$$D(M) = M^d \text{ mod } N$$

Diremos que (e, N) es la **clave pública** y (d, N) es la **clave privada**.

El sistema criptográfico RSA

Algunas observaciones importantes:

- La clave pública se calcula sólo una vez y se publica.
- Esto permite comunicarse de manera segura con varios clientes.

Ejercicio

Aplique el algoritmo RSA para $P = 7$, $Q = 11$, $e = 13$ y $d = 37$, y encripte y desencripte un mensaje $M = 5$.

El sistema criptográfico RSA

Ejemplo

Sean $P = 7$ y $Q = 11$

- Se tiene que $N = 77$ y $\phi(N) = 60$

Sean $e = 13$ y $d = 37$

- Se tiene que $(13 \cdot 37) \bmod 60 = 1$

Entonces: $E(M) = M^{13} \bmod 77$ y $D(M) = M^{37} \bmod 77$

Para $M = 5$:

$$\begin{array}{lcll} E(5) & = & 5^{13} \bmod 77 & = & 26 \\ D(E(5)) & = & 26^{37} \bmod 77 & = & 5 \end{array}$$

Créditos: Profesor Marcelo Arenas.

El sistema criptográfico RSA

Lo primero que debemos probar es que RSA funciona correctamente.

Teorema (Rivest-Shamir-Adleman)

Para cada $M \in \{0, \ldots, N-1\}$, se tiene que $D(E(M)) = M$.

Ejercicio

Demuestre el teorema.

RSA funciona correctamente

Sean E y D construidas como fue mencionado en las transparencias anteriores.

- $N = P \cdot Q$, $E(M) = M^e \bmod N$ y $D(M) = M^d \bmod N$

Teorema (Rivest-Shamir-Adleman)

Para cada $M \in \{0, \ldots, N-1\}$, se tiene que $D(E(M)) = M$.

Demostración: Sabemos que

$$\begin{aligned} D(E(M)) &= (M^e \bmod N)^d \bmod N \\ &= (M^e)^d \bmod N \\ &= M^{e \cdot d} \bmod N \end{aligned}$$

Por lo tanto, tenemos que demostrar que $M^{e \cdot d} \equiv M \bmod N$

Créditos: Profesor Marcelo Arenas.

RSA funciona correctamente: Demostración

Sabemos que $e \cdot d \equiv 1 \bmod \phi(N)$

- Por lo tanto: $e \cdot d = k \cdot \phi(N) + 1$

Tenemos que demostrar que $M^{k \cdot \phi(N)+1} \equiv M \bmod N$

- El siguiente lema es fundamental para la demostración

Lema

$M^{k \cdot \phi(N)+1} \equiv M \bmod P$ y $M^{k \cdot \phi(N)+1} \equiv M \bmod Q$

Demostración: Primero suponemos que $P|M$.

Créditos: Profesor Marcelo Arenas.

RSA funciona correctamente: Demostración

Entonces: $M^{k\cdot\phi(N)+1} \bmod P = (M \bmod P)^{k\cdot\phi(N)+1} \bmod P$

$= 0^{k\cdot\phi(N)+1} \bmod P$

$= 0$

Por lo tanto: $M^{k\cdot\phi(N)+1} \equiv M \bmod P$

En segundo lugar, suponemos que $P \not| M$.

- Sea $R = M \bmod P$

Dado que $R \in \{1, \ldots, P-1\}$, por teorema de Fermat:

$$R^{P-1} \equiv 1 \bmod P$$

Por lo tanto, dado que $R \equiv M \bmod P$:

$$M^{P-1} \equiv 1 \bmod P$$

Créditos: Profesor Marcelo Arenas.

RSA funciona correctamente: Demostración

De esto concluimos que:

$$\begin{aligned} M^{k\cdot\phi(N)+1} \bmod N &= ((M^{P-1})^{k\cdot(Q-1)} \cdot M) \bmod P \\ &= ((M^{P-1} \bmod P)^{k\cdot(Q-1)} \cdot M) \bmod P \\ &= (1^{k\cdot(Q-1)} \cdot M) \bmod P \\ &= M \bmod P \end{aligned}$$

Concluimos que $M^{k\cdot\phi(N)+1} \equiv M \bmod P$

- De la misma forma se demuestra que $M^{k\cdot\phi(N)+1} \equiv M \bmod Q$ □

RSA funciona correctamente: Demostración

Del lema concluimos que:

$$M^{k\cdot\phi(N)+1} - M = \alpha \cdot P$$
$$M^{k\cdot\phi(N)+1} - M = \beta \cdot Q$$

Por lo tanto: $\alpha \cdot P = \beta \cdot Q$

Entonces, dado que P y Q son primos distintos tenemos que $P|\beta$

- $\beta = \gamma \cdot P$

Concluimos que $M^{k\cdot\phi(N)+1} - M = \gamma \cdot P \cdot Q$

- Vale decir: $M^{k\cdot\phi(N)+1} \equiv M \bmod N$ □

Créditos: Profesor Marcelo Arenas.

RSA: implementación

Ya vimos que RSA funciona correctamente. Para poder implementarlo, necesitamos resolver los siguientes problemas de manera eficiente:

1. Generar primos P y Q: verificar si un número es primo.
2. Generar números e y d tales que $(e \cdot d)$ mod $\phi(N) = 1$.
3. Calcular funciones E y D.

Dados P, Q, e, d ya vimos como resolver 3. Ahora resolveremos 2.

Recordando...

Algoritmo de Euclides extendido

Sea $a \geq b$.

1. Definimos una sucesión $\{r_i\}$ como:

$$r_0 = a,\ r_1 = b,\ r_{i+1} = r_{i-1} \bmod r_i$$

2. Definimos sucesiones $\{s_i\}$, $\{t_i\}$ tales que:

$$s_0 = 1, \quad t_0 = 0$$
$$s_1 = 0, \quad t_1 = 1$$
$$s_{i+1} = s_{i-1} - \left\lfloor \frac{r_{i-1}}{r_i} \right\rfloor \cdot s_i, \quad t_{i+1} = t_{i-1} - \left\lfloor \frac{r_{i-1}}{r_i} \right\rfloor \cdot t_i$$

3. Calculamos estas sucesiones hasta un k tal que $r_k = 0$.
4. Entonces, $MCD(a, b) = r_{k-1} = s_{k-1} \cdot a + t_{k-1} \cdot b$.

Recordando...

Teorema

a tiene inverso en módulo n si y sólo si $MCD(a, n) = 1$.

RSA: implementación

Tenemos entonces que $N = P \cdot Q$ y $\phi(N) = (P-1) \cdot (Q-1)$, y debemos generar e y d tales que $(e \cdot d) \equiv_{\phi(N)} 1$.

Ejercicio

Encuentre un algoritmo para generar e y d.

Hint: empiece con un número aleatorio.

Cálculo de exponentes e y d en RSA

Recuerde que en RSA: $N = P \cdot Q$ y $\phi(N) = (P-1) \cdot (Q-1)$

- Tenemos que generar e y d tales que $e \cdot d \equiv 1 \bmod \phi(N)$

Tenemos los ingredientes necesarios para generar e y d:

genere al azar un número e
while $\text{MCD}(e, \phi(N)) > 1$ **do**
    genere al azar un número e
calcule s y t tales que $1 = s \cdot \phi(N) + t \cdot e$
sea $d \in \{0, \ldots, \phi(N) - 1\}$ tal que $d \equiv t \bmod \phi(N)$
return (e, d)

Créditos: Profesor Marcelo Arenas.

RSA: implementación

Recapitulando, necesitamos resolver eficientemente los siguientes problemas:

1. Generar primos P y Q: verificar si un número es primo.
2. Generar números e y d tales que $(e \cdot d)$ mod $\phi(N) = 1$.
3. Calcular funciones E y D.

Lamentablemente, resolver 1 está fuera del alcance de este curso :(.

RSA en la vida real

- En la actualidad RSA es el método de encriptación más usado en la práctica.
- RSA es seguro, pues factorizar $N = P \cdot Q$ es un problema difícil. Hasta el momento[1] nadie ha logrado hacerlo en tiempo polinomial...
- Muchas empresas necesitan enviar y guardar mensajes de sus clientes de forma segura y eficaz.
- Para autentificar sus firmas y llaves públicas están compañías como Verisign y Digicert (especie de notario público).
- Hace algunos años, los certificados entregados por Let's Encrypt comenzaron a ser aceptados por los principales browsers. La gracia: Let's Encrypt es gratis!
- Facebook, Twitter y Gmail usan claves de 2048-bits, son del orden de 600 dígitos.

[1] 20 de Noviembre de 2023

Llave pública de Facebook

$N =$
15 585 352 828 848 349 856 166 485 283 177 966 421 839 795 946 170
777 142 906 490 005 519 208 671 120 899 899 262 624 211 155 018 963
971 149 091 443 609 485 368 759 496 111 237 537 449 707 311 848 134
373 181 995 199 147 493 452 694 003 500 368 011 547 715 117 173 524
344 682 017 000 591 316 495 883 475 735 773 018 093 817 594 895 866
056 314 350 877 860 912 538 574 834 472 261 127 066 627 480 222 084
560 839 269 816 445 602 628 601 581 895 334 632 745 344 191 517 226
140 490 360 921 741 751 939 558 168 295 980 724 044 307 482 559 952
209 322 025 555 003 487 849 962 968 543 380 943 480 454 078 536 534
564 950 012 916 335 726 434 409 781 845 853 383 357 876 198 148 575
972 979 783 587 061 381 625 532 779 677 764 226 990 978 580 238 389
348 019 608 813 319 553 602 560 294 192 317 728 580 669 275 227 894
025 650
$e = 65537 = 2^{16} + 1.$

Matemáticas Discretas

Teoría de números y Criptografía

Nicolás Alvarado
nfalvarado@mat.uc.cl

Bernardo Barías
bjbarias@uc.cl

Sebastián Bugedo
bugedo@uc.cl

Gabriel Diéguez
gsdieguez@uc.cl

Departamento de Ciencia de la Computación
Escuela de Ingeniería
Pontificia Universidad Católica de Chile

20 de noviembre de 2023