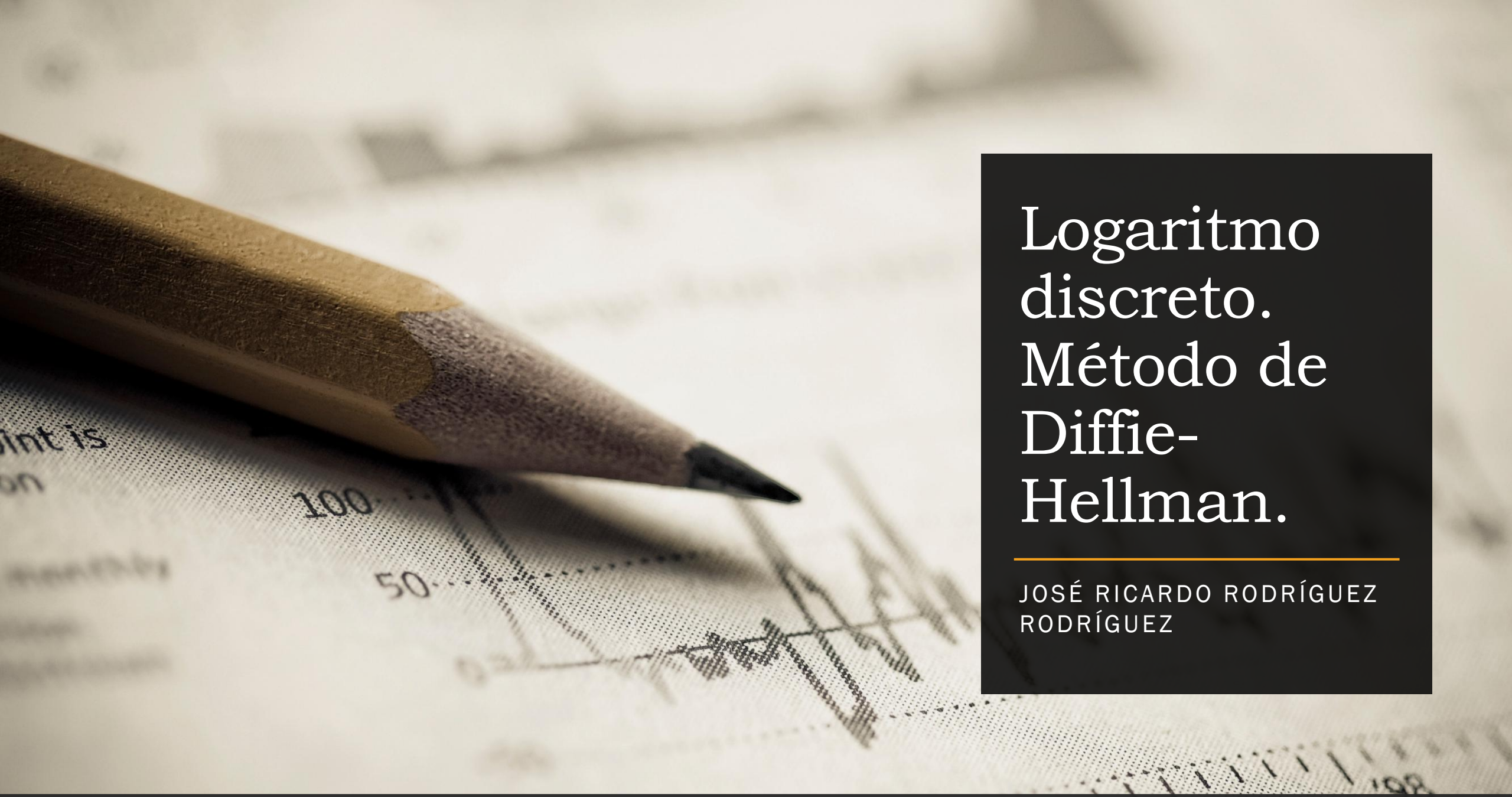


Logaritmo discreto. Método de Diffie-Hellman.

JOSÉ RICARDO RODRÍGUEZ RODRÍGUEZ

Logaritmo discreto

Definición: Sea $m > 1 \in \mathbb{Z}^+$ con raíz primitiva r y sea $a \in \mathbb{Z}^+ \ni \gcd(a, m) = 1$, el único $x \in \mathbb{Z} \ni 1 \leq x \leq \phi(m)$ & $r^x \equiv a \ (mod\ m)$, se llama el índice o logaritmo discreto de a en la base r módulo m. Se denota como:

$ind_r a$

Propiedad: Si a & b son enteros y primos relativos con m, entonces:

$a \equiv b \ (mod\ m) \leftrightarrow ind_r a = ind_r b$

Ejemplo

Sea $m = 7$ y $r = 3$. Nótese que:

$3^1 \equiv 3 \ (mod\ 7)$ $3^2 \equiv 2 \ (mod\ 7)$ $3^3 \equiv 6 \ (mod\ 7)$

$3^4 \equiv 4 \ (mod\ m)$ $3^5 \equiv 5 \ (mod\ 7)$ $3^6 \equiv 1 \ (mod\ 7)$

$ind_3 1 = 6$ $ind_3 2 = 2$ $ind_3 3 = 1$

$ind_3 4 = 4$ $ind_3 5 = 5$ $ind_3 6 = 3$

Teorema

Sea $m > 1 \in \mathbb{Z}^+$ con raíz primitiva $r \in \mathbb{Z}^+$. Además sean $a \,\&\, b \in \mathbb{Z}$ primos relativos con m. Entonces:

$(i)\ ind_r 1 \equiv 0\ (mod\ \phi(m))$

$(ii)\ ind_r(ab) \equiv ind_r a + ind_r b\ \big(mod\ \phi(m)\big)$

$(iii)\ ind_r a^k \equiv k \cdot ind_r a\ \big(mod\ \phi(m)\big)$ con $k \in \mathbb{Z}^+$

Ejemplos

Sea $m = 7$ y $r = 3$. Nótese que:

$ind_3 2 = 2$ $ind_3 3 = 1$ $ind_3 6 = 3$ $\phi(m) = 6$

$ii)\ ind_3 6 \equiv ind_3 (2 \cdot 3) \equiv ind_3 2 + ind_3 3 = 2 + 1 = 3 \pmod 6$

$3^5 \equiv 5\ (mod\ 7)$ $ind_3 3 = 1$ $ind_3 5 = 5$

$iii)\ ind_3 3^5 \equiv 5 \cdot ind_3 3 = 5 \cdot 1 = 5 \pmod 6$

Dificultad del logaritmo discreto

Dado un primo p con raíz primitiva $r \in \mathbb{Z}^+$, el problema de encontrar el logaritmo discreto de $a \in \mathbb{Z}$ en la base r módulo p, se considera que tiene la misma dificultad computacional que la factorización de enteros.

Debido a su dificultad computacional es usado como base de criptosistemas de clave pública como el criptosistema ElGamal, y protocolos como el intercambio de claves de Diffie–Hellman.

Dificultad del logaritmo discreto

El algoritmo más eficiente para calcular logaritmos discretos es el método de cribado en el campo de números (number-field sieve method). Los tiempos aproximados se muestran en la siguiente tabla.

Número de dígitos (del primo p)	Millones de instrucciones por segundo Años requeridos.
150	10^4
225	10^8
300	10^{11}
450	10^{16}
600	10^{20}

Otros algoritmos

1) **Fuerza bruta.**

2) **Baby-step Giant-step (BSGS):** Se reduce el problema en pasos pequeños y en pasos grandes con el fin de reducir las búsquedas.

3) **Pohlig–Hellman:** Aprovecha el caso donde p-1 tiene factores pequeños para resolver por partes.

4) **Pollard’s Rho para logaritmo discreto:** Usa un método probabilístico que busca colisiones

Pohlig–Hellman

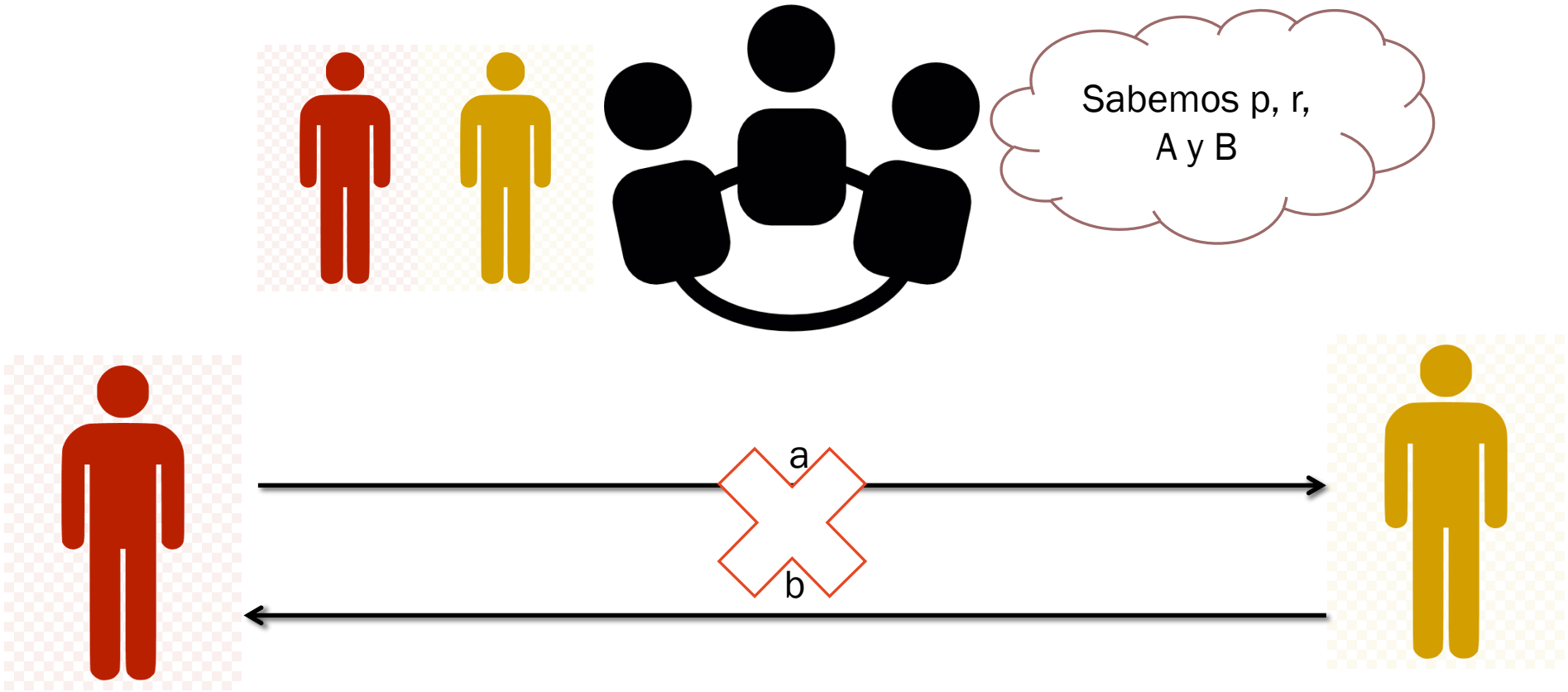
- Factoriza $p-1$ en primos. $p-1=\prod q_i^{e_i}$.
- Para cada factor $q_i^{e_i}$, se resuelve el logaritmo discreto reducido módulo $q_i^{e_i}$.
- Combina todas las soluciones usando el Teorema Chino del Resto para obtener la solución final módulo $p-1$.

Intercambio de Claves Diffie–Hellman

Es un protocolo que permite a dos partes intercambiar una clave secreta en un canal de comunicaciones inseguro sin la necesidad de compartir información previamente.

Inventado en 1976 por Whitfield Diffie y Martin Hellman. Este protocolo tiene la propiedad de que partes no autorizadas no pueden descubrir la clave en un tiempo de cómputo factible.

¿Cómo funciona?



¿Cómo funciona?

p es un número primo, que se recomiendan sean primos proporcionados en el estándar RFC 7919, que tiene números primos de 2048 bits en adelante.

r Es un generador del grupo Z_p^*.

$a \in \{1,2,\dots,p-2\}$ Es la clave elegida por el emisor.

$b \in \{1,2,\dots,p-2\}$ Es la clave elegida por el receptor.

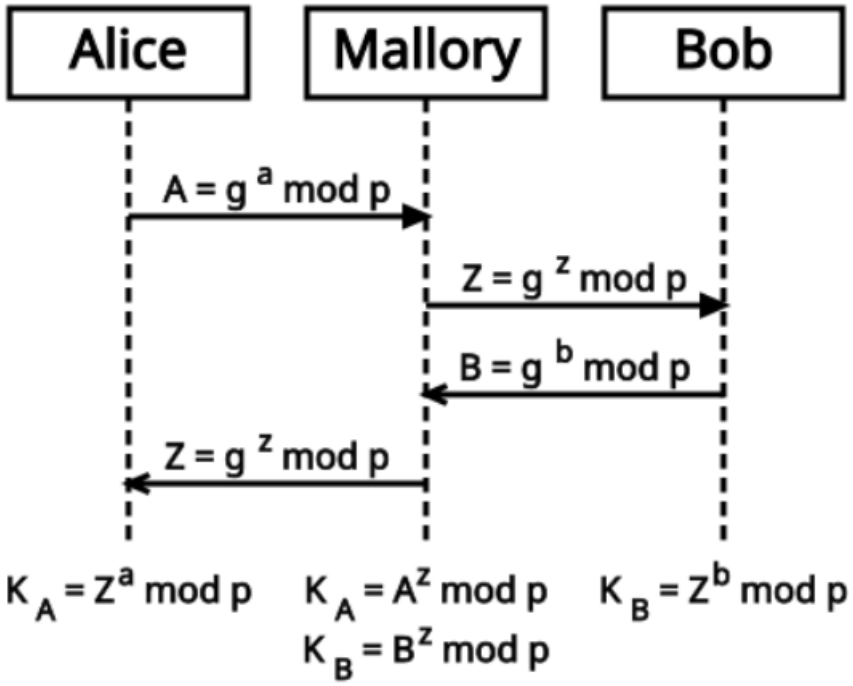
$A = r^a$

$B = r^{\mathrm{b}}$

$K = A^b = B^a = r^{ab}$

Ataque Man-in-the-middle

- Control de tiempos.
- Protocolo de autenticación previa, como TLS.
- Autenticación del contenido, como MAC.
- Cifrando las claves públicas con algún algoritmo asimétrico.
- Usar un tercero para la verificación.



Complejidad

Para el algoritmo de number-field sieve method la complejidad temporal es de:

$$\exp\left(\left((64/9)^{1/3} + o(1)\right)(\log n)^{1/3}(\log\log n)^{2/3}\right)$$

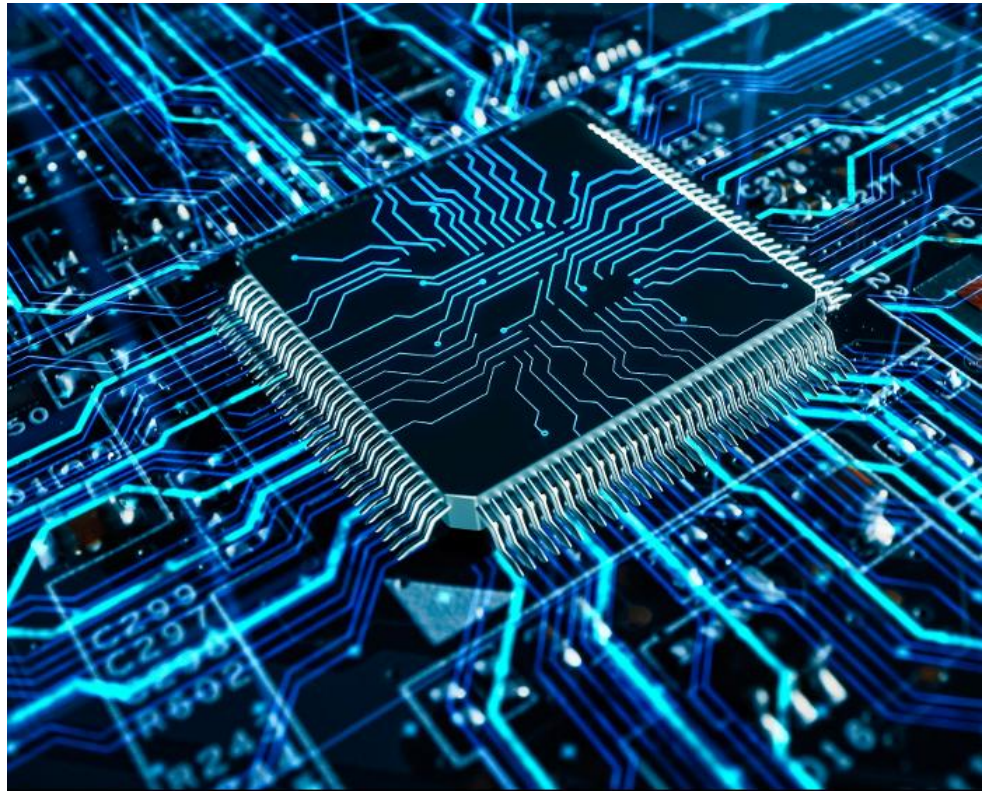
Para 2,048 bits es aproximadamente $4.52 * 10^{75}$

Problemas del algoritmo

El ataque Logjam.

Ataque de denegación de servicio.

Computación y algoritmos cuánticos.



Referencias

- Diffie, W; Hellman, M. (1976). New Directions in Cryptography. *IEEE TRANSACTIONS ON INFORMATION THEORY 22*(6). 644-654. https://web.archive.org/web/20141129035850/https://ee.stanford.edu/~hellman/publications/24.pdf

- Rosen, K. (2011). *Elementary Number Theory, 6ta ed.* Pearson.

- Wong, D. (2021). "Key exchange standards". Real World Cryptography. https://archive.ph/20200921005545/https://freecontent.manning.com/key-exchange-standards