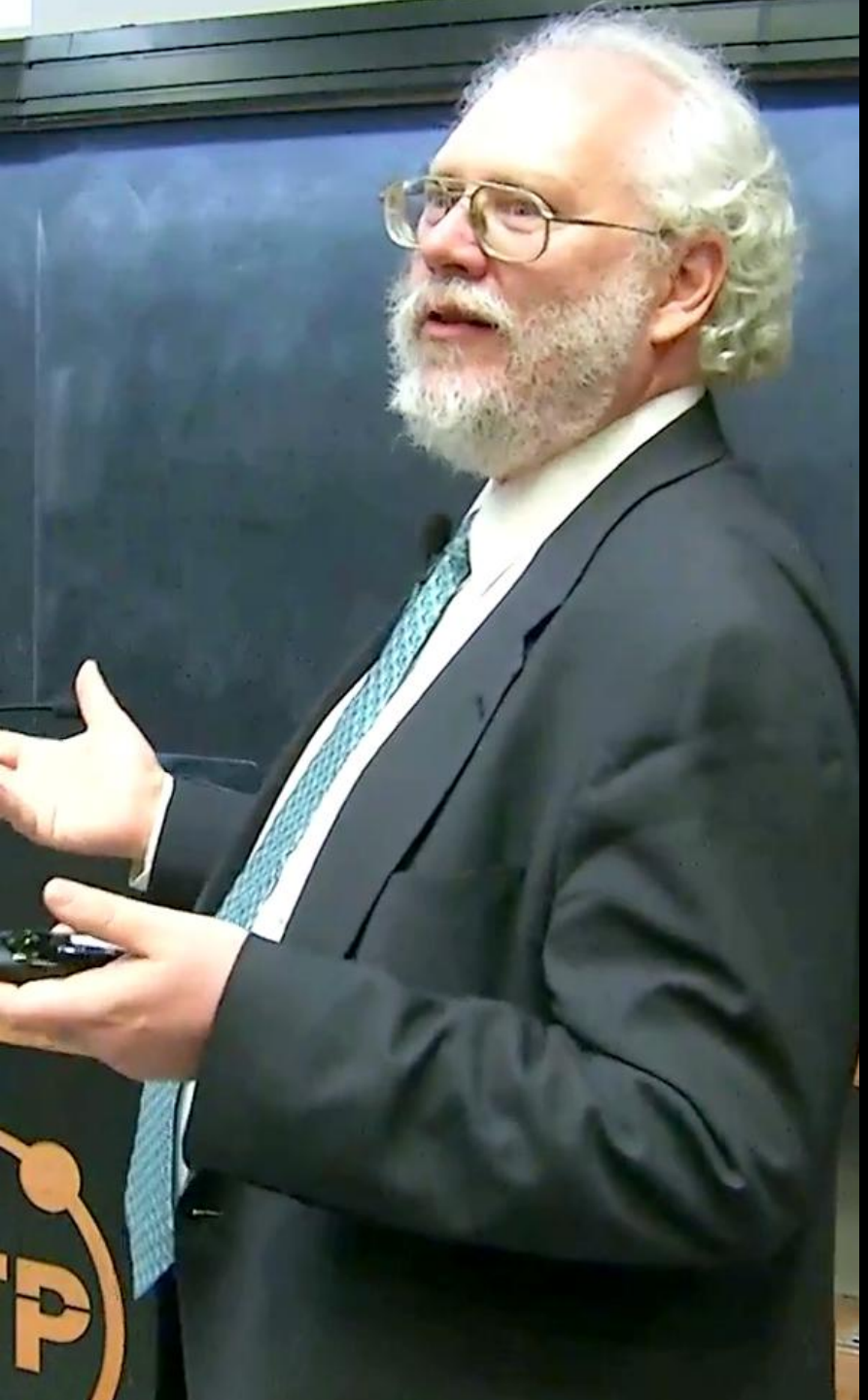
Algoritmo de Shor

Javier Ovalle Chiquin

Seminario 2

Teoría de Números



¿Quién fue su inventor?

- El algoritmo se debe a Peter Shor
- Matemático estadounidense
- Nacido el 14 de agosto de 1959

¿Qué es el Sistema RSA?

- Es un sistema de cifrado
- Algunos usos:
  - Envier mensajes secretos
  - Firmar digitalmente
  - Autenticar Identidad

Ej:
P = 140,737
Q = 209,759
N = P x Q = 29,528,333,083

Pero si solo tengo **n = 29528333083**

Ejemplo del sistema RSA

Multiplicar 2 primos muy grandes

Calcular la “clave pública”

$$N = p * q$$
$$\theta = (p-1)(q-1)$$
$$e = \ comprimo\ con\ \theta$$
$$d = inv\ de\ E\ mod\theta$$

Quiere decir…

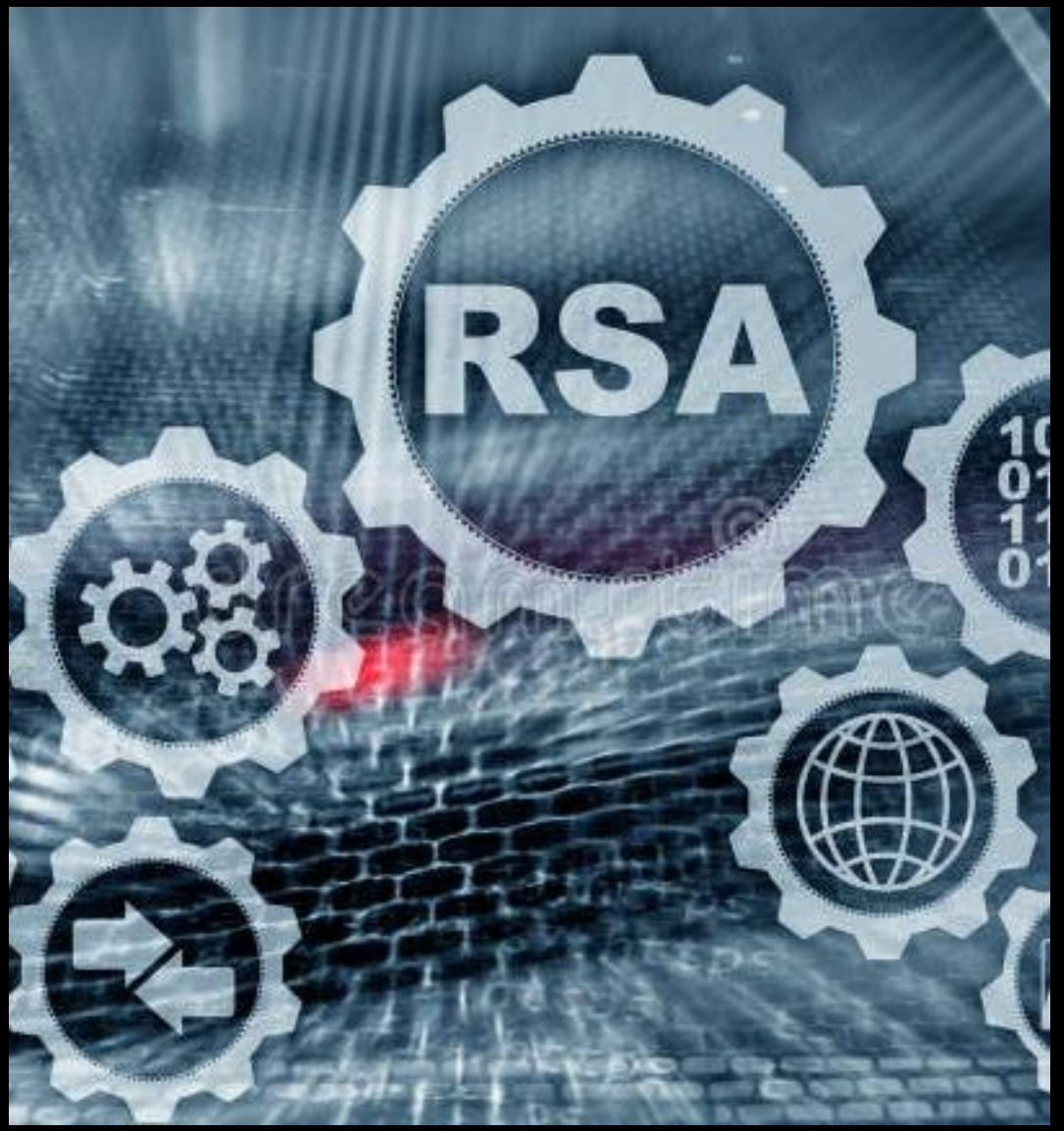
$$d \cdot e = 1\ mod\ 5$$

Ejemplo:

$$7 \cdot 3 = 1\ mod\ 5$$

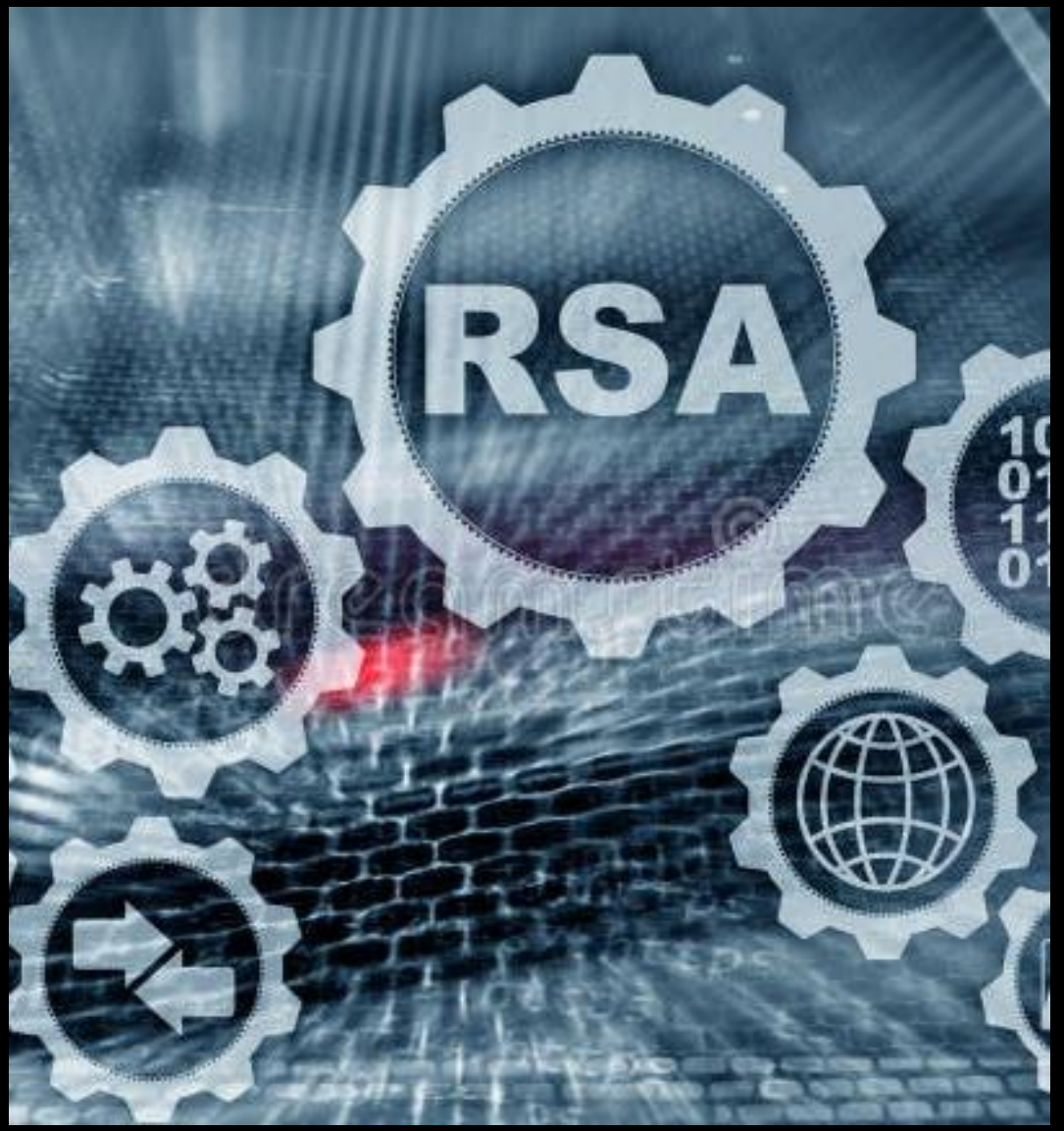
Clave pública será (e, n), donde código = $(mensaje)^e$ mod N

Clave privada será (d, n), donde mensaje = $(código)^d$ mod N



Ejemplo del sistema RSA

- $p = 5, q = 11$
- $N = p \cdot q = 55$
- $\theta = (5-1) \cdot (11-1) = 40$
- $e = 3$
- $3 \cdot \mathrm{d} = 1 \bmod (40)$
- $\mathrm{d} = 27$
- $c = 2^3(55) = 8(55)$
- $\mathrm{m} = 8\text{^}27\ (55) = 2\ (55)$



¿Qué es QFT?

- Es la versión cuántica de la transformada de Fourier clásica
- Convierte información escondida en las *fases* de los qubits en *probabilidades medibles*.
- Permite descubrir patrones o periodos dentro de estados cuánticos.

Rol en el algoritmo:

- El algoritmo de Shor prepara una superposición cuántica con un patrón periódico.
- La QFT transforma ese patrón en picos de probabilidad.
- Al medir, esos picos permiten encontrar el período r, clave para factorizar el número

Idea principal del algoritmo de Shor

- El algoritmo de Shor **factoriza números grandes rápidamente** encontrando el **período** de una función matemática que depende del número que queremos factorizar.
- Factorizar un número grande N(encontrar sus primos) es difícil para una computadora clásica.
- Pero existe una función $f(a) = x^a \mod N$ que tiene un **período** r
- Si se encuentra ese período r, entonces se podrá obtener los factores de N usando matemáticas clásicas.

¿Cómo se realiza el algoritmo?

Parte Cuántica

- Se encuentra el periodo de la función
- Se utiliza un ordenador cuántico al trabajar con qubits

Parte Clásica

- Utiliza el periodo encontrado
- Se quiere encontrar un número x tal que $x^2 \equiv 1\ mod(N)$
- Tal que $x \in (2, N-2)$

Parte clásica del algoritmo

Recordemos que $N = p \cdot q$

$$\mathrm{x}^2 \equiv 1 \bmod (\mathrm{N})$$
$$\mathrm{x}^2 - 1 \equiv 0 \bmod \mathrm{N}$$
$$(x-1)(x+1) \equiv 0\ mod\ N$$
$$(x-1)(x+1) = kN$$
$$(x-1) = x_1,\ x_2, \cdots\ \mathrm{x}_n$$
$$(x+1) = y_1, y_2, \cdots y_n$$

Entonces: $p \in x_1, x_2, \cdots x_n$ y $q \in y_1, y_2, \cdots y_n$

p = mcd(x-1, N)

q = mcd(x+1, N)

Parte clásica del algoritmo

Necesitamos encontrar lo siguiente: $m^r \equiv 1$

Lo cual es equivalente a encontrar el periodo de la siguiente función:

$$f(a) = x^a \; mod \; N$$

Solo nos vale con encontrar el periodo par

Ejemplo

Objetivo descomponer el 15

- Escogemos un número al azar entre 2 y 13
- Por este ejemplo escojamos 2
- 2^2 es una raíz cuadrada
- Entonces:
  - $p = mcd(4 - 1{,}15) = mcd(3{,}15) = 3$
  - $q = mcd(4 + 1{,}15) = mcd(3{,}15) = 5$

Referencias

- https://www.researchgate.net/publication/386824682_Polynomial-Time_Algorithms_for_Prime_Factorization_and_Discrete_Logarithms_on_a_Quantum_Computer
- https://en.wikipedia.org/wiki/Shor%27s_algorithm
- https://www.semanticscholar.org/paper/Computing-prime-factors-with-a-Josephson-phase-Lucero-Barends/9055b3c0eff725648b70b9b864b59d0c3a8a7f4e
- https://www.youtube.com/watch?v=6SIX_FR4wOM


Gracias