Inspira Crea Transforma

UNIVERSIDAD EAFIT®

CRIPTOGRAFÍA

Presentado por:
Juan S. Cárdenas Rodríguez
David Plazas Escudero

Modelación y Simulación II
Ingeniería Matemática
Departamento de Ciencias Matemáticas
Escuela de Ciencias
Universidad EAFIT
2017

CONTENIDO

DEFINICIÓN

1. DEFINICIÓN

Es el cifrado y descifrado de mensajes secretos o encriptados. También referido a encriptado computacional de información [1].

[1] WEBSTER, M., "Definition of cryptography," 2017, https://www.merriam-webster.com/dictionary/cryptography. [Online] consultado en Octubre 29, 2017

[1] BIT4ID, "Cryptography," 2017, https://www.bit4id.com/en/cryptography/. [Online] consultado en Octubre 29, 2017

HISTORIA DE LA CRIPTOGRAFÍA

2. HISTORIA DE LA CRIPTOGRAFÍA

- Khnumhotep II - Egipto, India.
- Cifrado de César, 100 A.C.
- Cifrado de Vigenere, Siglo 16.
- La máquina Enigma.

158,962,555,217,826,360,000

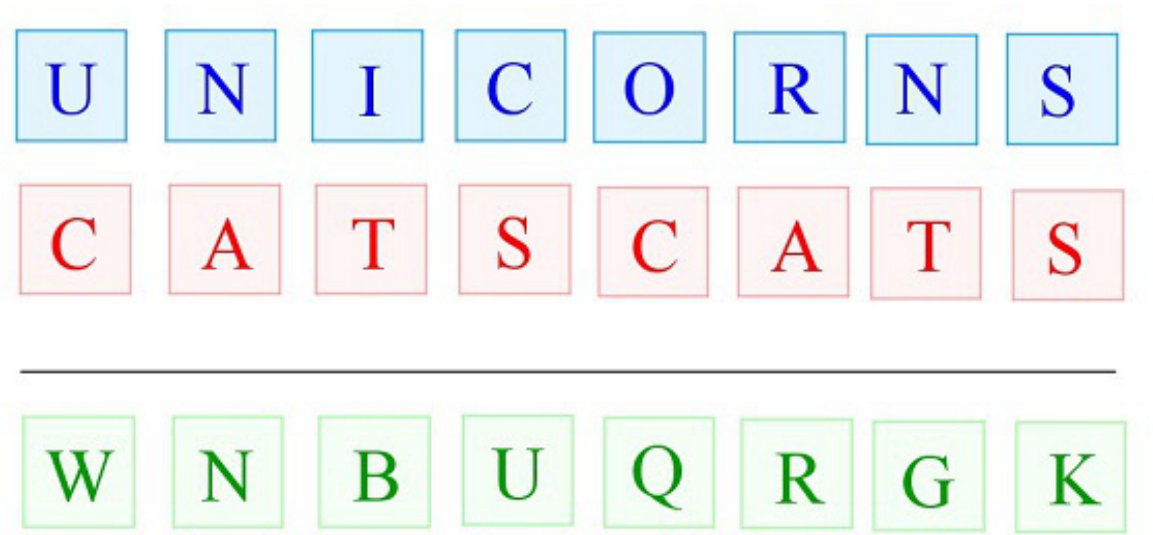

Figura 1. Ejemplo del Cifrado de Vigenere[2]

[2] WORDPRESS, "Cryptography," 2015, https://wafflescrazypeanut.files.wordpress.com/2015/03/untitled1.jpg?w=600&h=300. [Online] consultado en Octubre 29, 2017

TIPOS DE CRIPTOGRAFÍA

3. TIPOS DE CRIPTOGRAFÍA

3.1 Simétrica

Se utiliza la misma llave (privada) para cifrar y descifrar el mensaje.

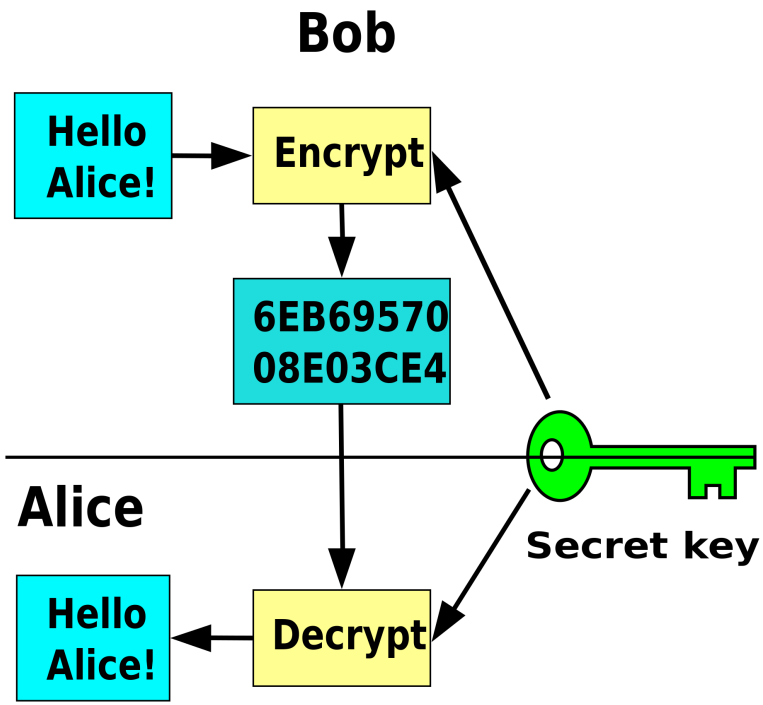

Figura 2. Ilustración de criptografía simétrica[3]

[3] WIKIMEDIACOMMONS, "Symmetric key encryption," 2014, https://commons.wikimedia.org/wiki/File:Symmetric_key_encryption.svg. [Online] consultado en Octubre 29, 2017

3. TIPOS DE CRIPTOGRAFÍA

3.2 Antisimétrica

Hay dos llaves, una privada y otra pública. Se puede utilizar la pública para encriptar la información o la privada para firmarla.

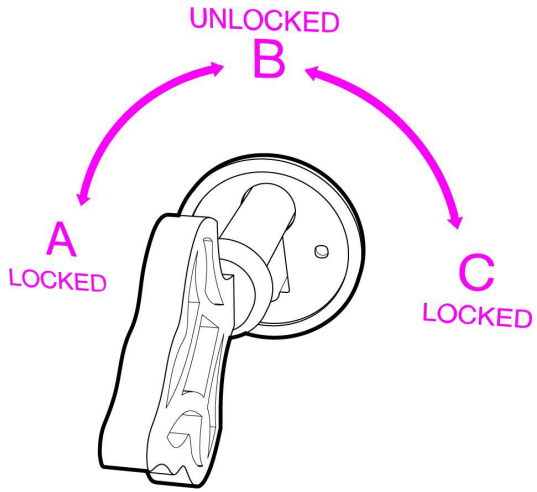

Figura 3. Ilustración de criptografía asimétrica[4]

[4] VRYONIS, P., "Explaining public-key cryptography to non-geeks," 2014, https://commons.wikimedia.org/wiki/File:Symmetric_key_encryption.svg. [Online] consultado en Octubre 29, 2017

NÚMEROS PRIMOS

4. NÚMEROS PRIMOS

4.1 Teoría

- Teorema Fundamental de la aritmética
- ¿Cuántos primos hay en el intervalo (1,x)?
- Teorema de Chebyshev
- Problemas clásicos de los primos

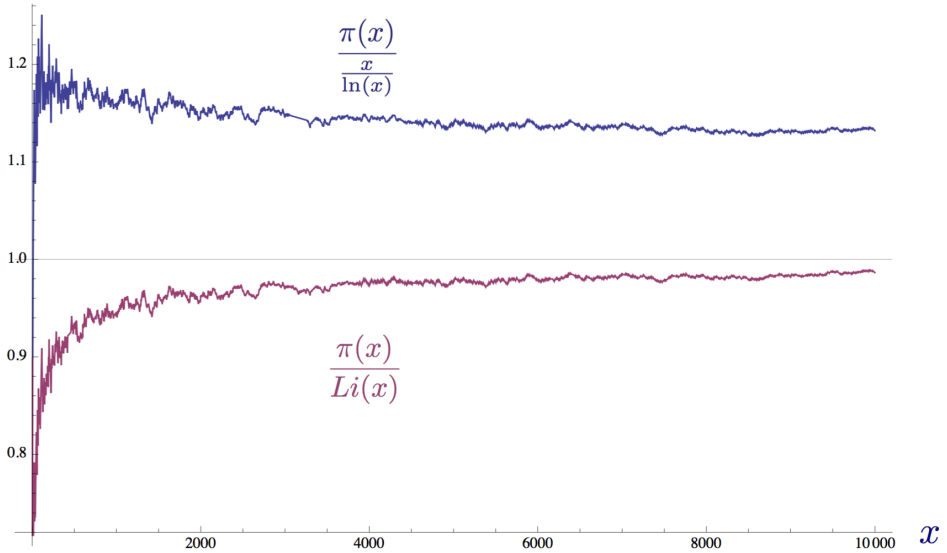

Figura 4. Convergencia de la función contadora de primos a 1 por dos aproximaciones[5].

[5] https://cdn-images-1.medium.com/max/2000/1*P4Vq1b1qIr_21zJTuSIgYw.png. [Online] consultado en Octubre 29, 2017

4.2 Adicional

- Función Zeta de Riemann

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \tag{1}$$

- Identidad de Euler

$$\zeta(s) = \prod_{p} \frac{1}{1 - p^{-s}} \tag{2}$$

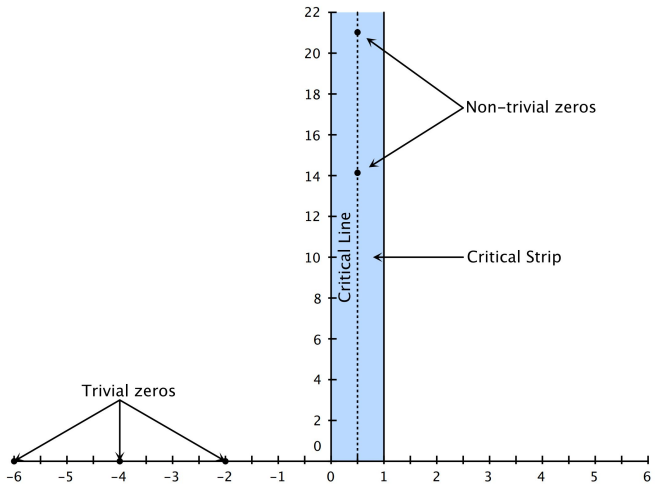

Figura 5. Hipótesis de Riemann[6].

[6] DIGNMAN, R., "The riemann hypothesis," 2010, http://wstein.org/edu/2010/414/projects/dingman.pdf. [Online] consultado en Octubre 29, 2017

CRIPTOGRAFÍA MODERNA

5. CRIPTOGRAFÍA MODERNA

5.1 Generalidades

- No se intercambian el mensaje clave, doble candado.
- Primos grandes
- Eficiencia computacional

$$O((\log n)^{c \log\log\log n})$$

$$O(e^{\sqrt{c \log n (\log\log n)^2}})$$

- Atkin, Sundaram, Eratosthenes [7]

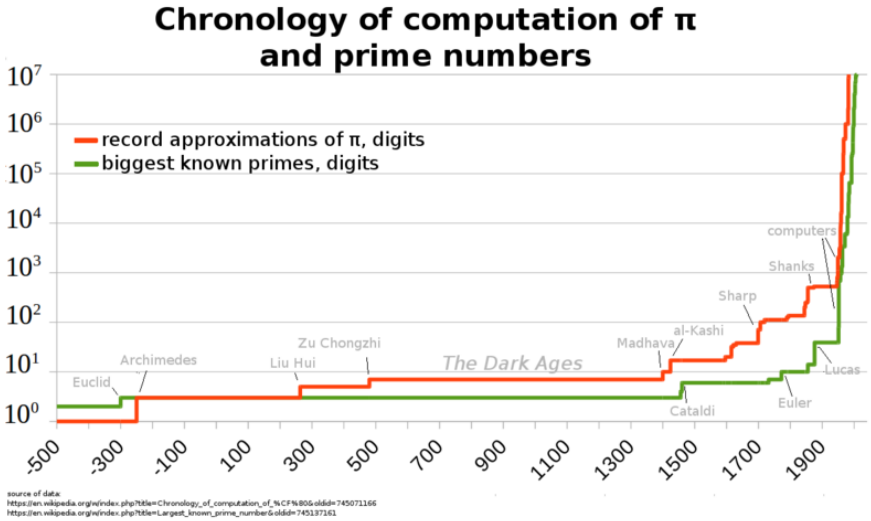

Figura 6. Cronología de pi y los primos a través de los años[8].

[7] WIKIPEDIA, "Sieve atking, sieve sundaram, sieve eratosthenes," 2017, https://en.wikipedia.org/wiki/Sieve_of_Atkin,https://en.wikipedia.org/wiki/Sieve_of_Sundaram,https://en.wikipedia.org/wiki/Sieve_of_Eratosthenes. [Online] consultado en Octubre 29, 2017

[8] WIKIMEDIACOMMONS, "Chronology of pi and primes," 2017, https://upload.wikimedia.org/wikipedia/commons/thumb/f/f0/

5.2 Algoritmo RSA

- 1978, **R**ivest, **S**hamir & **A**dleman.
- Asimétrico.
- Multiplicar números es sencillo, factorizarlos es difícil

Algoritmo: $K_U = (e, n)$, $K_R = (d, n)$

1. p, q primos
2. $n = pq$
3. $z = (p-1)(q-1)$
4. e tal que e primo, $1 < e < z$ y $\texttt{GCD}(n, e) = 1$
5. d tal que $(d \cdot e) \equiv 1 \pmod{z}$

Si m es el mensaje original y c el mensaje encriptado, entonces

$$c = m^e \bmod n$$

$$m = c^d \bmod n$$

5.3 Ejemplo RSA

- $p = 61$
- $q = 53$
- $n = pq = 3233$
- $z = (p-1)(q-1)$
- $e = 17$
- $d = 2753$

Tenemos $R_U = (e, n) = (17, 3233)$, $R_K = (d, n) = (2753, 3233)$ Si tenemos $m = 123$, entonces

$$c = (123)^{17} \bmod 3233 = 855$$

Y si se quiere descifrar,

$$m = (855)^{2753} \bmod 3233 = 123$$

REFERENCIAS BIBLIOGRÁFICAS I

[1] https://cdn-images-1.medium.com/max/2000/1*P4Vq1b1qIr_21zJTuSIgYw.png. [Online] consultado en Octubre 29, 2017.

[2] BIT4ID, "Cryptography," 2017, https://www.bit4id.com/en/cryptography/. [Online] consultado en Octubre 29, 2017.

[3] DIGNMAN, R., "The riemann hypothesis," 2010, http://wstein.org/edu/2010/414/projects/dingman.pdf. [Online] consultado en Octubre 29, 2017.

[4] VRYONIS, P., "Explaining public-key cryptography to non-geeks," 2014, https://commons.wikimedia.org/wiki/File:Symmetric_key_encryption.svg. [Online] consultado en Octubre 29, 2017.

[5] WEBSTER, M., "Definition of cryptography," 2017, https://www.merriam-webster.com/dictionary/cryptography. [Online] consultado en Octubre 29, 2017.

[6] WIKIMEDIACOMMONS, "Symmetric key encryption," 2014, https://commons.wikimedia.org/wiki/File:Symmetric_key_encryption.svg. [Online] consultado en Octubre 29, 2017.

[7] WIKIMEDIACOMMONS, "Chronology of pi and primes," 2017, https://upload.wikimedia.org/wikipedia/commons/thumb/f/f0/Chronology_of_pi_and_primes.png/800px-Chronology_of_pi_and_primes.png. [Online] consultado en Octubre 29, 2017.

[8] WIKIPEDIA, "Sieve atking, sieve sundaram, sieve eratosthenes," 2017, https://en.wikipedia.org/wiki/Sieve_of_Atkin,https://en.wikipedia.org/wiki/Sieve_of_Sundaram,https://en.wikipedia.org/wiki/Sieve_of_Eratosthenes. [Online] consultado en Octubre 29, 2017.

REFERENCIAS BIBLIOGRÁFICAS II

[9] WORDPRESS, “Cryptography,” 2015, https://wafflescrazypeanut.files.wordpress.com/2015/03/untitled1.jpg?w=600&h=300. [Online] consultado en Octubre 29, 2017.

Gracias