Importancia de los números primos en la Criptografía Asimétrica.

Desde que el hombre ha podido comunicarse con otros por medio de mensajes escritos se ha visto en la necesidad de ocultar del resto de la población algunos textos que podrían ser considerados como privados. Para ocultar este tipo de mensajes se utiliza la criptografía. Los sistemas de cifrado fueron creados debido a la necesidad de mandar mensajes que solo pudiesen ser vistos por los ciertos destinatarios escogidos. Cifrar un escrito significa transformar el mensaje original de modo que nadie, excepto aquellos a quienes va dirigido, pueda comprender el texto resultante de este proceso. El mensaje cifrado no puede ser comprendido a menos que el destinatario lleve a cabo un proceso de descifrado, o sea, el proceso inverso al cifrado. Los procesos criptográficos han existido desde las civilizaciones más antiguas. Las antiguas civilizaciones como los egipcios y los chinos, ya tenían sus propios códigos para ocultar escritos. Sin embargo, debido al transcurso del tiempo, el incremento de los conocimientos matemáticos y al uso militar que se le ha dado, la complejidad de los cifrados ha aumentado.

La criptografía está basada en un proceso simple de transmisión de mensajes. El proceso empieza cuando un emisor, con ayuda de una clave, cifra un escrito original, es decir, lo convierte en un texto cifrado. Posteriormente, utilizando un canal de comunicación, el texto cifrado llega a un receptor. El receptor lleva a cabo un proceso de descifración. La descifración utiliza otra clave (o la misma) para hallar el mensaje original en un texto cifrado. Entonces, se tiene que, en el proceso de cifrado intervienen dos tipos de clave, las cuales pueden ser o no iguales, dependiendo del sistema de cifrado que se utilice.

Ahora bien, hay dos tipos de sistemas de cifrado. Uno es el sistema simétrico o sistema de clave secreta. El sistema de clave secreta utiliza dos claves idénticas. También puede utilizar claves diferentes *siempre y cuando sea posible deducir la clave de descifrado a partir de la clave de cifrado* (Caballero, 2003: p.51). Por otro lado, el sistema asimétrico o sistema de clave pública maneja dos claves diferentes, pero, a diferencia del sistema de cifrado simétrico, en el cifrado público existe una imposibilidad de obtener la clave de descifrado aún teniendo la clave de cifrado. El propósito de este ensayo es explicar por qué resulta imposible calcular la clave de descifrado en un sistema de clave pública.

La razón por la cual resulta imposible hallar la clave de descifrado en un sistema asimétrico es porque este sistema está basado en funciones trampa. Una función trampa es, por así decirlo, una función matemática cuyo cálculo directo resulta sencillo. Sin embargo, calcular la inversa de dicha función implica desarrollar un gran número de operaciones. La función trampa que utilizan los sistemas de criptografía asimétrica es la multiplicación de números primos. Un número primo es aquél que tiene únicamente dos divisores: él mismo y 1.

En forma general, la ecuación sería:

Donde p y q son números primos.

Esta operación resulta muy sencilla si se conocen los valores de p y q. No obstante, el proceso inverso implica un gran número de operaciones.

Dado m, hallar p y q

La complejidad radica en que para hallar p y q, m tiene que ser factorizado. Por ejemplo:

En este caso fue sencillo hallar los primos factores de m, porque m es un número relativamente pequeño. Fue una tarea fácil encontrar dos primos cuyo producto fuese 77. Al ser 77 una m pequeña, se sabe que sus factores primos deben ser números más pequeños. No fue difícil hallar los componentes de 77 porque se

encontraban en los lugares 4 y 5 de la lista de los primos más pequeños. No hubo necesidad de probar con muchos números primos. Pero, entre más grande sea *m*, mayor será el grado de dificultad para hallar *p* y *q*. Por ejemplo, si *m* tuviera un valor de 12307663 y se quisiera sacar los dos factores primos de este número se tendría que probar con un gran número de números primos y en distintas combinaciones.

Entonces, no es que sea imposible encontrar la clave de descifrado en un sistema de criptografía de clave pública. La cuestión es que entre más grandes sean los primos factores de *m*, mayor será el tiempo que se tomará para encontrar los factores de *m*. Por ejemplo, si *m* tiene 100 cifras, el número medio de operaciones necesarias para factorizar *m* es de 10^50. O sea que hay un 10^−48% de posibilidades de encontrar en el primer cálculo los factores primos de una *m* de 100 dígitos. Incluso teniendo una computadora que realice un millón de operaciones por segundo, el tiempo que tardaría la máquina en terminar las 10^50 posibles operaciones es de 3.17^37 años, aproximadamente.

10^5 1 segundo

10^50 x

X = 10^45 segundos

Por lo cual resulta inútil tratar de encontrar el par de primos probando de operación en operación.

Además hay que agregar que, en este ejemplo se usa una *m* de 100 cifras. Pero puede haber *m*'s todavía más grandes. Siempre habrá *m*'s mayores hasta que se utilicen los primos más grandes del sistema numérico. Cabe destacar que nunca se llegará a un primo más grande que todos los primos ya que los números primos son infinitos. Por lo tanto, las *m*'s posibles también son infinitas.

La criptografía asimétrica utiliza el principio de las funciones trampa con números primos para elaborar claves más seguras. El valor de m, representa la clave pública, es decir, aquella que puede ser compartida con infinidad de individuos o usuarios sin poner en riesgo el desciframiento del mensaje. La clave secreta, o sea, aquella que permite descifrar el mensaje es la que conocen los destinatarios autorizados para leer el texto codificado. Los usuarios legítimos utilizan la clave secreta para llevar a cabo el descifrado convirtiendo un problema difícil en un problema fácil, mientras que, por el contrario, el criptoanalista debe enfrentarse forzosamente a la resolución del problema difícil. (Caballero, 2002: p.63)

Si un usuario conoce la clave secreta (p), puede conocer q fácilmente.

Por otro lado, un individuo ajeno a la clave secreta se enfrenta al reto de encontrar los factores de m.

Donde p y q son incógnitas.

Como se ha visto, los números primos y las propiedades de los mismos desempeñan un papel fundamental en la elaboración de claves de codificaciones asimétricas. Actualmente, las agencias de seguridad de los principales países del mundo enrolan matemáticos expertos en teoría de números para trabajar en el campo de la criptografía. La criptografía, como ciencia, empezó a tener importancia al término de la Segunda Guerra Mundial, cuando el conocimiento de los códigos japoneses y alemanes por los aliados fue determinante para el resultado de la conflagración.

Una de las aplicaciones más importantes de los números primos radica en la ciencia de los mensajes, la criptografía ya que la seguridad de un texto radica en la forma en la que la criptografía asimétrica utilice los números primos. Las agencias de seguridad de los principales países del mundo enrolan matemáticos expertos en teoría de números para trabajar en el campo de la criptografía. De hecho, el cifrado y descifrado de mensajes ha tenido gran importancia a partir del término de la Segunda Guerra Mundial ya que el

conocimiento de los códigos japoneses y alemanes por los aliados fue determinante para el resultado de la conflagración. Durante la década de los 80 y los 90, y principios del siglo XIX, la Criptografía de clave pública empezó a aplicarse en el área de las comunicaciones y los sistemas computacionales. Ya no se emplea tanto en los ámbitos militares, pues el intercambio de claves secretas también representaba un riesgo. Ahora, las firmas digitales, la autenticación de mensajes (métodos que aseguran que alguna parte de un mensaje, o todo un escrito, no ha sido modificado) y el acceso a redes mediante el manejo de nombres de usuario y password, dependen de la correcta aplicación de los números primos en los sistemas de criptografía pública.

Caballero Gil Pino. (2003). Introducción a la Criptografía. México: Alfaomega.

Fúster, A. & de la Guía, D. & Hernández, L. & Montoya, F. & Muñoz, J. (2001). Técnicas Criptográficas de protección de datos. México: Alfaomega.

José Ramón Esteban Marti. Criptografía. [Online]. http://www.seguridadenlared.org/es/index25esp.html.

Función Trampa. [Online]. Wikipedia la enciclopedia libre. http://es.wikipedia.org/wiki/Funci%C3%B3n_trampa.

Eladio Pascual Foronda. El Pequeño Larousse ilustrado. (2005). México.

Joaquín Navarro. Enciclopedia Autodidáctica Interactiva Océano. (vo.l #3). Barcelona, España. (1999). Océano.