RESUMEN

Ante el desarrollo de las telecomunicaciones, la información que viaja a través de la red se ha visto afectado por enemigos que intentan quebrantar la seguridad. La criptología es la solución para reducir las amenazas en las redes, mediante algoritmos y protocolos, que permiten cifrar y descifrar sin tomar en cuenta los recursos computacionales. Los algoritmos asimétricos proporcionan una comunicación segura a través del Internet, sin embargo las soluciones matemáticas que estas brindan requieren de un mayor costo computacional. El presente proyecto tiene como objetivo optimizar el algoritmo de encriptación asimétrica RSA para mejorar la seguridad de los mensajes y disminuir el consumo de los recursos. Para llevarlo a cabo se diseñó y desarrolló una solución genérica, en la que el algoritmo permite incrementar la velocidad del cálculo, al disminuir la complejidad matemática. Además se combina tanto el cálculo modular como el probabilístico para mejorar el tiempo de cifrado y descifrado. La información enviada será el mensaje a cifrar y descifrar, junto con los parámetros necesarios para el cálculo del RSA. Estos parámetros consisten en el *p, q, n* y *una serie de índices aleatorios*, que se obtendrán a través de una llamada a procedimiento remoto. Se realizaron pruebas funcionales tanto en el cliente como en el servidor, con los que se obtuvo varios resultados de las variables evaluadas como el consumo de memoria, consumo del procesador, latencia, reporte estadístico de la red, tiempo cifrado y descifrado. Posteriormente se procedió a la interpretación de estos datos mediante el procesamiento estadístico, determinando que el algoritmo RSA propuesto tiende a una mejoría en cuanto al costo de software y a la seguridad de la información.

PALABRAS CLAVES:

- **CRIPTOGRAFIA**
- **ALGORITMO ASIMÉTRICO**
- **RSA**
- **RECURSOS COMPUTACIONALES**
- **SEGURIDAD**