Johan Sebastián Sánchez Vargas

Sistema de Encriptado

Problema

Desde los tiempos de la antigua Roma ha sido necesario establecer métodos para proteger los mensajes enviados entre un emisor y un receptor de posibles interceptaciones. Julio César estableció uno de los primeros métodos de cifrado conocidos, el cifrado por desplazamiento, el cual asignaba números a las letras del alfabeto sumándole tres unidades a cada letra y las últimas tres se establecían como las tres primeras para completar el ciclo. Para aquel entonces este método era suficiente. Sin embargo, en la actualidad, con la capacidad de procesamiento de las maquinas existentes es necesario crear un algoritmo de encriptación de alta complejidad capaz de proteger la información enviada, desde mensajes de texto, cuentas bancarias, hasta documentos privados.

Solución

Un algoritmo que se puede implementar es un algoritmo que utilice aritmética modular como lo es el algoritmo RSA. Este algoritmo utiliza números primos, aritmética modular y una combinación de llaves, una pública y una privada, la llave pública puede ser accedida por cualquier individuo, sin embargo, debe conocerse la llave privada para poder desencriptar el mensaje. La confiabilidad de este sistema radica en que se utiliza números primos de al menos cincuenta cifras, esto genera tantas combinaciones que intentar desencriptar el mensaje por fuerza bruta computacional sea inviable. El uso de llaves genera mayor seguridad respecto a un atacante debido a que, a diferencia del método de Julio César que solo necesita conocerse el algoritmo de encriptado, este necesita una pieza más para poder completar el desencriptado. En ese orden de ideas, lo que se propone es crear un algoritmo RSA reducido que sea capaz de encriptar y desencriptar mensajes utilizando aritmética modular y que provea un cierto grado de confiabilidad.

Referencias

https://www.romeandart.eu/es/arte-cifrado-cesar.html

https://www.comparitech.com/blog/information-security/rsa-encryption/