MÉTODO DE ENCRIPTACIÓN BASADO EN EL ALGORITMO RSA

Ponentes: **Alfredo Gómez Calvache**
Diego Fernando Ruiz Solarte

Abstract

Esta ponencia es de tipo informativo, en la cual se presenta una de las aplicaciones de la matemática como lo es la criptografía. Esta ciencia trata de ocultar un mensaje de modo que sólo pueda ser descifrado por la persona que posea la clave o que conozca el método que permita averiguar su significado.

Existen diferentes tipos encriptación, entre ellos están

1. **Criptografía simétrica:** en este tipo de criptografía se manejan dos claves, una para encriptar y otra para desencriptar, las cuales tanto el emisor como el receptor las conocen. La deficiencia radica en que no existe un medio seguro para enviar las claves que se estén manejando.
2. **Criptografía asimétrica:** soluciona la deficiencia de la cripotografía anterior utilizando funciones conocidas como "funciones de un sentido" en canales abiertos.

Dentro de la Criptografía asimétrica se encuentra el método de encriptación basado en el algoritmo RSA. Su seguridad se fundamenta en la escritura de un número compuesto como producto de dos números primos.

Se deben tener en cuenta las siguientes definiciones.

Definición 1 *El conjunto formado por todas las clases residuales módulo p con p primo forma un grupo que se nota por $\mathbb{Z}_p$.*

Definición 2 ***(Función de Euler).*** *Dado un entero positivo n, la función que se nota por ϕ se conoce como la función de Euler y se define como el número de primos relativos con n menores que n.Facílmente se verifica que si p primo, entonces $\phi(p) = p - 1$.*

Definición 3 ***(Funciones de un sentido).*** *Una función f se dice de un sentido si $y = f(x)$ es de fácil cálculo conociendo x, mientras que el cálculo de $x = f^{-1}(y)$ conociendo y es computacionalmente imposible.*

Un ejemplo de una función de un sentido, es la función exponenciación modular definida como

$$y \equiv a^x \,(\mathrm{mod}\, p)\,,$$

donde $a, x \in \mathbb{Z}$ y p es un número primo con más de 200 digítos. Su función inversa conocida como la función logaritmo discreto se define como

$$x \equiv \log_a y \,(\mathrm{mod}\, p)\,,$$

siendo computacionalmente imposible con las computadoras actuales el cálculo de x para el p dado.

Con el uso de las definiciones anteriores daremos a conocer el algortimo RSA y su aplicación en la encriptación y desencriptación de una frase dada; además se hará el análisis de la complejidad computacional que tiene este algoritmo.