Unidad V

Criptografía

5.1. Factorización.

En matemáticas, la **factorización** es una técnica que consiste la descomposición de una expresión matemática (que puede ser un número, una suma, una matriz, un polinomio, etc) en forma de producto. Existen diferentes métodos de factorización, dependiendo de los objetos matemáticos estudiados; el objetivo es *simplificar* una expresión o reescribirla en términos de «bloques fundamentales», que recibe el nombre de **factores**, como por ejemplo un número en números primos, o un polinomio en polinomios irreducibles.

El teorema fundamental de la aritmética cubre la factorización de números enteros, y para la factorización de polinomios, el teorema fundamental del álgebra. La factorización de números enteros muy grandes en producto de factores primos requiere de algoritmos sofisticados, el nivel de complejidad de tales algoritmos está a la base de la fiabilidad de algunos sistemas de criptografía asimétrica como el RSA.

Factorizar un polinomio

Una factorización de un polinomio de grado *n* es un producto de como mucho $m \leq n$ factores o polinomios de grado $n_k \leq n$ con $1 \leq k \leq m$. Así por ejemplo el polinomio *P*(*x*) de grado 5 se puede factorizar como producto de un polinomio de grado 3 y un polinomio de grado 2:

$$P(x) = x^5 - x^3 + 69x^2 - 20x + 16 = (x^3 + 4x^2 - x + 1)(x^2 - 4x + 16)$$

5.2. Números primos.

En matemáticas, un **número primo** es un número natural mayor que 1 que tiene únicamente dos divisores distintos: él mismo y el 1. Los números primos se contraponen así a los compuestos, que son aquellos que tienen algún divisor natural aparte de sí mismos y del 1. El número 1, por convenio, no se considera ni primo ni compuesto.

Los números primos menores que cien son los siguientes: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59,61, 67, 71, 73, 79, 83, 89 y 97.[1]

La propiedad de ser primo se denomina **primalidad**. A veces se habla de **número primo impar** para referirse a cualquier número primo mayor que 2, ya que éste es el único número primo par. A veces se denota el conjunto de todos los números primos por $\mathbb{P}$.

El estudio de los números primos es una parte importante de la teoría de números, la rama de las matemáticas que comprende el estudio de los números enteros. Los números primos están presentes en algunas conjeturas centenarias tales como la hipótesis de Riemann y la conjetura de Goldbach. La distribución de los números primos es un tema recurrente de investigación en la teoría de números: si se consideran números individuales, los primos parecen estar distribuidos aleatoriamente, pero la distribución «global» de los números primos sigue leyes bien definidas.

5.3. Criptografía de llave pública.

Se suele definir criptografía como el conjunto de procedimientos (aunque sería más correcto hablar de una disciplina) que permiten transformar una información de manera que quede oculta a observadores no autorizados.

En tiempos remotos se estableció ya la necesidad de ocultar la información a observadores no deseados. Probablemente esta preocupación sea tan antigua como la propia escritura, ya que cualquiera que supiera leer podía tener acceso a una información que podía desearse mantener oculta.

Existen pruebas de que en tiempos del antiguo Egipto, o la Roma clásica ya se usaban métodos criptográficos. Algunos de ellos, como el método César, o el algoritmo de cifrado de Augusto, se siguieron usando durante la edad media, y fueron perfeccionados en el renacimiento (método Vigénere).

Durante un tiempo se tendió a abandonar la criptografía por otros métodos de ocultación (como el uso de una jerga particular), pero en la edad moderna, con la llegada de los nuevos medios de comunicación, como el telégrafo, la criptografía volvió a cobrar importancia, y se empezó abuscar nuevos métodos criptográficos.

Sin embargo, ha sido durante el S. XX cuando la criptografía ha experimentado un mayor crecimiento. Basta recordar la importancia que llegó a tener durante la II Guerra Mundial, cuando numerosos matemáticos trabajaron, tanto en el bando aliado como en el bando del eje, dedicándose casi en exclusiva a tratar de romper los cifrados del enemigo.

Durante todo ese tiempo, se estuvo empleando la criptografía de llave privada como medio de protección de la información. En ella, toda la seguridad depende de la capacidad del método y de la capacidad de cada uno de los

usuarios de mantener su clave privada en secreto. Pero para descifrar la información se necesita dicha llave, y eso vuelve vulnerable todo el sistema.

Así, en la década de los 70 apareció un nuevo concepto en criptografía: la criptografía de llave pública. En este tipo de criptografía, cada uno de los usuarios tiene dos claves, una clave pública y una clave privada, y sólo una de ellas es necesaria para descifrar la información que se cifra con la otra. Así, la seguridad del sistema se ve incrementada.

Así, utilizando lo mejor de la criptografía de llave pública y privada, se consigue dar respuesta a las siguientes necesidades:

a)Garantizar la autenticidad del origen de la información

b)Garantizar la autenticidad del contenido e integridad del mismo

c)Incorporación de protocolos que dificulten en repudio interesado

d)Verificar la identidad de los comunicantes.

En la actualidad, ambos tipos de criptografía se emplean, utilizándose la criptografía de llave pública como complemento de la de llave privada, permitiendo aumentar la seguridad de los métodos criptográficos empleados y cubriendo las lagunas que la criptografía de llave privada deja.