



Actividad de Aprendizaje 1:

Los conceptos básicos de la criptografía

Nombre del Alumno:

Edwin Absalón Martínez Moreno

Matrícula

23410272

Materia cursada

Criptografía

Asesor de la materia:

Dr. Luis Roberto Pérez Macías

Objetivo específico:

Definir los conceptos básicos de la criptografía, a través del análisis de la historia, los tipos y las técnicas criptográficas clásicas, para una mejor aplicación de esta disciplina.

Instrucciones:

Consulta los apuntes y las lecturas correspondientes al bloque; y si es necesario, complementa con investigaciones de fuentes confiables para el desarrollo de la presente actividad. Es importante que anexes las referencias al final del trabajo.

1. Elabora un esquema sobre los conceptos principales de la criptografía que contenga:

- a) Las definiciones básicas
- b) Los tipos de criptografía
- c) Las técnicas criptográficas clásicas

2. Elabora lo que se pide a continuación:

- a) El cálculo del máximo común divisor de 588 y 114 a través del algoritmo de Euclides.
- b) Demuestra si la siguiente expresión es correcta $15 \equiv -9 \pmod{12}$. ¿Cuál es el valor del módulo?
- c) Entrega el procedimiento que se realizó para cada inciso con argumentos que lo sustenten.

3. Tomando como referencia el cifrador de Alberti, en el que se utilizan dos discos concéntricos, realiza la encriptación del texto "INSTITUTO SUIZO".

- a) En el disco externo coloca el alfabeto castellano
- b) Para el disco interno utiliza el alfabeto en griego.

4. Entrega un documento en el que detalles los pasos que realizaste para obtener el texto cifrado y el criptograma resultante, con argumentos que lo sustenten.

Conceptos principales de la criptografía

La criptografía es definida por AWS como “(...) una práctica que consiste en proteger información mediante el uso de algoritmos codificados, hashes y firmas.”

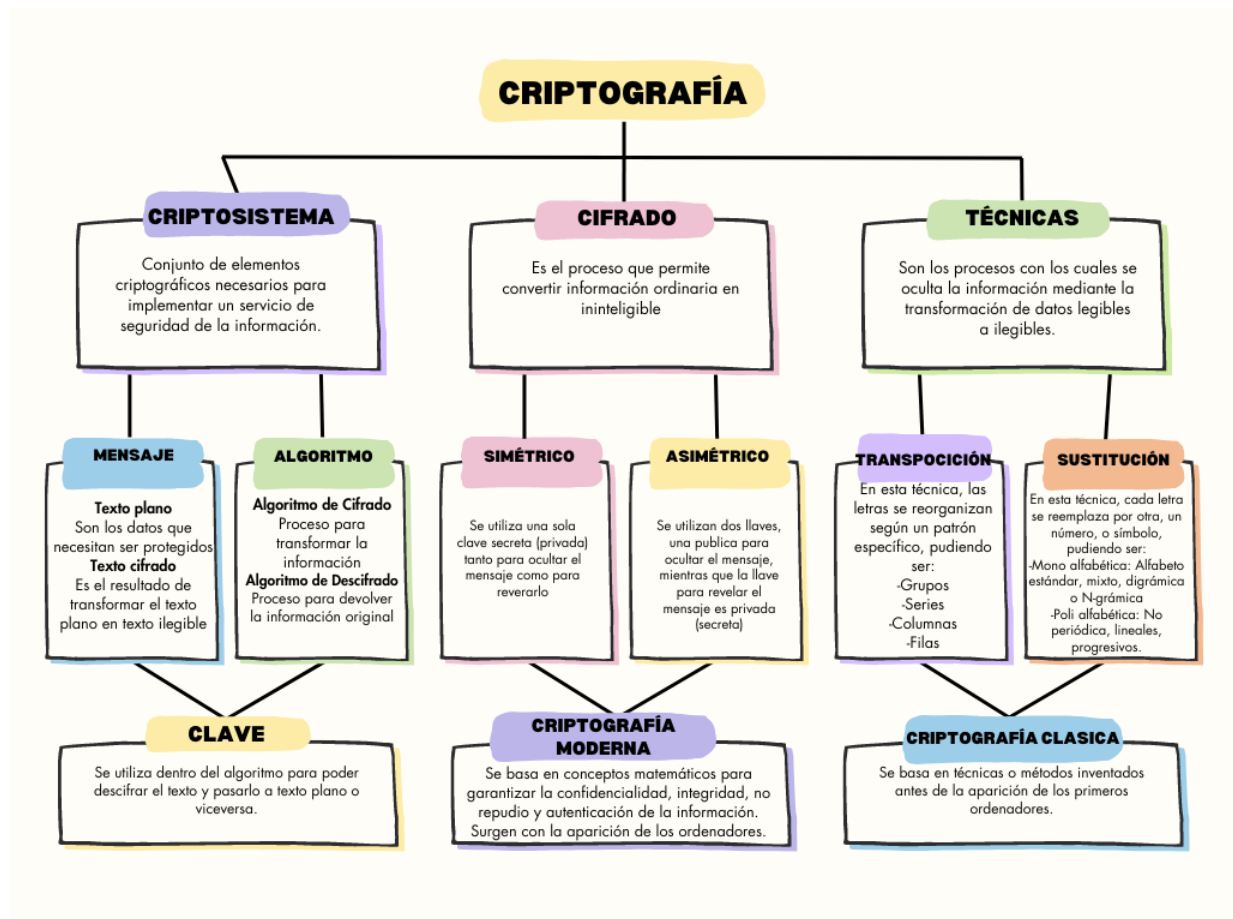
Antes de entrar en profundidad en el tema de la criptografía, es importante entender primero como surge esta misma.

La criptografía surge de la teoría de la información, la cual a su vez viene de las matemáticas. El principal uso que se le ha dado a la criptografía desde sus orígenes es el de proteger la información.

Adicionalmente, para entender la criptografía, se debe tener en mente los conceptos básicos que la forman, los cuales son mostrados en la imagen 1.1. También, cabe destacar que hoy en día, la criptografía se divide en clásica y moderna

Figura 1.1

Definiciones básicas.



Fuentes:

Amazon Web Services, (s.f.). ¿Qué es la criptografía?. Documentación oficial de AWS en línea. Recuperado de: <https://aws.amazon.com/es/what-is/cryptography/#:~:text=La%20criptograf%C3%ADa%20es%20una%20pr%C3%A1ctica,algoritmos%20codificados%2C%20hashes%20y%20firmas>.

IBM, (s.f.). ¿Qué es el cifrado?. Artículo oficial de IBM en línea. Recuperado de: <https://www.ibm.com/mx-es/topics/encryption>

Soler, J. (s.f.). Una introducción a la Criptografía Clásica. Documento en línea. Recuperado de: <https://www.criptohistoria.es/files/cifras.pdf>

Vicent, J. F. (s.f.). Conceptos básicos. En Propuesta y análisis de criptosistemas de clave pública basados en matrices triangulares superiores por bloques [tesis de grado] (pp. 16-22). Universidad de Alicante, España. 16-22. Recuperado de: https://m.isu.edu.mx/pluginfile.php/368606/mod_page/content/14/1%29%20Vicent.pdf

Granados, G. (2006). Introducción a la criptografía. En Revista Digital Universitaria. 7(7), 3-16. https://m.isu.edu.mx/pluginfile.php/368606/mod_page/content/14/4%29%20Granados.pdf