**GUÍA DE LABORATORIO NO. 5**

**HANNA KATHERINE ABRIL GÓNGORA**

**JENNIFER NATALIA BELTRAN**

**FELIPE ARAUJO**

**UNIVERSIDAD MANUELA BELTRÁN**

**ESTRUCTURA DE DATOS**

**DOCENTE**

**HUGO ALFONSO ORTIZ BARRERO**

**BOGOTA DC 7 ABRIL 2025**

**Preguntas Orientadoras**

1. **¿Cuáles fueron los aprendizajes obtenidos al realizar esta guía? Liste como mínimo 3 aprendizajes y relaciónelos con su futuro quehacer profesional.**

* **Pensamiento lógico y estructurado:**  
  Al desarrollar cada ejercicio, fue necesario seguir un orden lógico para llegar a la solución. Este tipo de pensamiento es clave en mi carrera como ingeniera de software, ya que me permitirá escribir código eficiente y resolver problemas complejos de forma ordenada.
* **Interpretación y análisis de problemas:**  
  Comprender qué pedía cada punto de la guía me ayudó a mejorar mi capacidad de análisis. En el ámbito profesional, esto se traduce en una mejor comprensión de requerimientos técnicos y funcionales en proyectos reales.
* **Gestión del tiempo y búsqueda autónoma de soluciones:**  
  Al enfrentarme a retos dentro de la guía, aprendí a organizar mi tiempo y buscar recursos como documentación oficial, foros o ejemplos en línea. Estas habilidades son fundamentales para un entorno laboral donde muchas veces se debe investigar y resolver problemas por cuenta propia.

1. **¿Dónde presenté mayor dificultad resolviendo la guía? ¿Cómo lo resolví y cuáles fueron las estrategias de solución?**

Tuvimos mayor dificultad al momento de interpretar un ejercicio que requería aplicar un concepto nuevo que no habíamos practicado en clase. Inicialmente fue confuso, pero decidimos:

* Volver a leer cuidadosamente el enunciado para entender mejor lo que se pedía.
* Consultar el material de clase y buscar ejemplos similares en internet.
* Preguntar a mis compañeros y comparar nuestras ideas para validar enfoques distintos.
* Finalmente, hice pruebas con el código hasta lograr el resultado correcto.

Estas estrategias me ayudaron a superar el obstáculo y me mostraron que la colaboración, la lectura crítica y la perseverancia son esenciales para el aprendizaje y para mi desarrollo como profesional en el área de tecnología.

1. **Es más que un conjunto de caracteres alfanumérico generado a partir de un texto plano. Suelen tener una longitud finita y se caracterizan por ser irreversibles y determinísticos:**

b. Hash

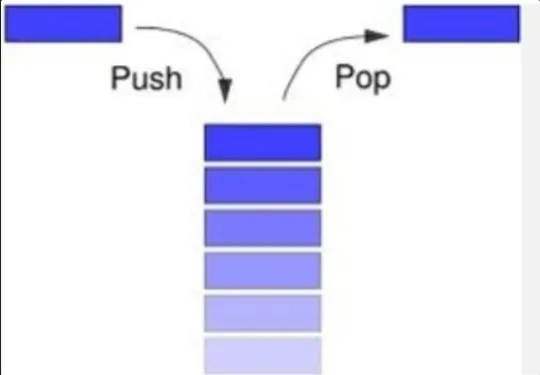
Un hash es una función que transforma datos de entrada (como texto) en una cadena de longitud fija. Es irreversible (no se puede obtener el texto original a partir del hash) y determinístico (el mismo texto siempre da el mismo resultado).

1. **La función de hash más conocida es MD5 y siempre que se aplique sobre un texto se obtendrá el mismo hash, es decir, no importando el tamaño del texto siempre generará una cadena de caracteres de:**

c. 32

El algoritmo MD5 genera una salida de 128 bits, que comúnmente se representa como una cadena hexadecimal de 32 caracteres.

1. **¿A que estructura lineal corresponde la imagen?**



La imagen muestra las operaciones Push y Pop, donde:

Push agrega un elemento en la parte superior.

Pop elimina el último elemento agregado (también desde la parte superior).

Esto corresponde al comportamiento de una estructura de datos tipo Pila (Stack), que funciona con la lógica LIFO (Last In, First Out), es decir, el último que entra es el primero en salir.

* 1. Pila

**Actividad de trabajo Autónomo**

How Bitcoin Encrypts Its Transactions

Bitcoin is a decentralized digital currency that relies on cryptographic techniques to ensure secure, verifiable, and irreversible transactions. One of the most fundamental aspects of Bitcoin’s security is how it encrypts and signs transactions using public key cryptography and hashing algorithms.

1. Public Key Cryptography

Each Bitcoin user has a pair of cryptographic keys: a public key (used as the Bitcoin address) and a private key (used to sign transactions). When someone sends Bitcoin, they create a transaction that includes:

* The recipient’s public key.
* A digital signature, generated using the sender’s private key.
* A reference to the previous transaction (the source of the Bitcoin).

The digital signature proves ownership of the funds and prevents unauthorized spending. Anyone on the network can verify this signature using the sender's public key, ensuring the transaction is legitimate.

2. Hashing with SHA-256

Bitcoin uses the SHA-256 hashing algorithm to create unique digital fingerprints of data. Every block and transaction is hashed to:

* Guarantee data integrity.
* Ensure tamper resistance.
* Link each block securely to the previous one in the blockchain (via the hash of the previous block).

Transactions are grouped into a block and summarized into a Merkle Tree, which compresses all transaction hashes into a single root hash. This root hash is included in the block header and is used during the mining process.

3. Encryption and Mining

Although transaction data is not encrypted in the traditional sense (it's publicly visible), Bitcoin ensures confidentiality and security by:

* Using digital signatures to prevent fraud.
* Hashing data to maintain integrity.
* Performing a proof-of-work (mining) process that secures the blockchain and prevents tampering.

In conclusion, Bitcoin does not encrypt individual transaction contents but ensures secure and verifiable transactions using cryptographic techniques such as public key cryptography, digital signatures, and hashing with SHA-256. These methods form the backbone of Bitcoin's decentralized and tamper-resistant system.