**Project Title:** Hash Function Analysis and Data Integrity Verification

**Project Description:** In this project, we explore the use of hash functions for data integrity verification, compare hash values, and understand their significance in ensuring data security. We use a Kali Linux environment to create text files, calculate hash values, and analyze the outcomes of various hash functions.

**Project Steps:**

**Step 1: Directory and File Creation**

1. Create a directory named "Hashes" using the **mkdir** command.
2. Navigate to the "Hashes" directory with the **cd** command.
3. Create the first text file, **text1.txt**, and populate it with content using the **echo** command.
4. Verify the presence and content of **text1.txt** using the **ls** and **cat** commands.
5. Calculate the MD5 hash of **text1.txt** using the **md5sum** command.

**Step 2: Duplicate File Creation** 6. Create a second text file, **text2.txt**, with similar content to **text1.txt** and calculate its MD5 hash.

1. Slightly modify the content of **text2.txt**, recalculate the MD5 hash, and observe how the hash changes.

**Step 3: Using OpenSSL for Hash Functions** 8. Utilize OpenSSL to calculate MD5, SHA-1, and SHA3-512 hash values for **text1.txt**. Analyze the results to understand how different hash functions produce unique hash values.

**Step 4: Verifying New Files** 9. Create a new text file, **text3.txt**, and calculate its MD5 hash.

1. Compare the MD5 hash of **text3.txt** with the previously stored hashes to determine its integrity.

**Step 5: Additional File Verification** 11. Create another text file, **text4.txt**, with the same content as **text3.txt**.

1. Calculate its MD5 hash and compare it to the hash of **text3.txt**.

**Project Conclusion:** This project explores the practical application of hash functions in verifying data integrity and understanding their use in data security. Through hands-on experimentation, we observed how hash values change when the content is altered, thereby indicating even minor data modifications. We also used various hash functions and the OpenSSL tool to compute different types of hash values for the same data, highlighting the uniqueness of each function.

The project additionally demonstrated the importance of hash functions in real-world scenarios, such as ensuring the integrity of downloaded files from the internet through checksums. Furthermore, the use of salted hashes was discussed as a fundamental practice in secure password storage. Lastly, the project provided a glimpse into how blockchain technology relies on hash functions to achieve data security and immutability.

Overall, this project equips learners with a fundamental understanding of hash functions and their crucial role in data verification and security across various applications.

Top of Form

Bottom of Form

┌──(kaliadmin㉿kali)-[~]

└─$ mkdir Hashes

┌──(kaliadmin㉿kali)-[~]

└─$ cd Hashes

┌──(kaliadmin㉿kali)-[~/Hashes]

└─$ echo This is a txt file> text1.txt

┌──(kaliadmin㉿kali)-[~/Hashes]

└─$ ls

text1.txt

┌──(kaliadmin㉿kali)-[~/Hashes]

└─$ cat text1.txt

This is a txt file

┌──(kaliadmin㉿kali)-[~/Hashes]

└─$ md5sum text1.txt

c2b8aa1da9f7f707e231dbb7b0f70e06 text1.txt

┌──(kaliadmin㉿kali)-[~/Hashes]

└─$ echo This is a txt file> text2.txt

┌──(kaliadmin㉿kali)-[~/Hashes]

└─$ cat text2.txt

This is a txt file

┌──(kaliadmin㉿kali)-[~/Hashes]

└─$ md5sum text2.txt

c2b8aa1da9f7f707e231dbb7b0f70e06 text2.txt

┌──(kaliadmin㉿kali)-[~/Hashes]

└─$ echo This is a txt file.> text2.txt

┌──(kaliadmin㉿kali)-[~/Hashes]

└─$ cat text2.txt

This is a txt file.

┌──(kaliadmin㉿kali)-[~/Hashes]

└─$ md5sum text2.txt

6b23e881b56748d1a4cf673723eefccc text2.txt

┌──(kaliadmin㉿kali)-[~/Hashes]

└─$ openssl md5 text1.txt

MD5(text1.txt)= c2b8aa1da9f7f707e231dbb7b0f70e06

┌──(kaliadmin㉿kali)-[~/Hashes]

└─$ openssl sha1 text1.txt

SHA1(text1.txt)= 7c0d7a38233f42b24ddc697f642ccdda07825dc0

┌──(kaliadmin㉿kali)-[~/Hashes]

└─$ openssl sha3-512 text1.txt

SHA3-512(text1.txt)= 69e664586a46359362eb18ec92329b99e5868893d139fe3ff01b883addb826269fcbd84b93868330d371db649a4ca9eb20631cc50c4772714cd2d66c3d5bf720

┌──(kaliadmin㉿kali)-[~/Hashes]

└─$ echo This is a new txt file > text3.txt

┌──(kaliadmin㉿kali)-[~/Hashes]

└─$ cat text3.txt

This is a new txt file

┌──(kaliadmin㉿kali)-[~/Hashes]

└─$ openssl md5 text3.txt

MD5(text3.txt)= 86d273cde4990221a06794762431a814

┌──(kaliadmin㉿kali)-[~/Hashes]

└─$ echo This is a new txt file > text4.txt

┌──(kaliadmin㉿kali)-[~/Hashes]

└─$ md5sum text4.txt

86d273cde4990221a06794762431a814 text4.txt

A screenshot of a computer

Description automatically generated