THE UNIVERSITY OF JORDAN

King Abdullah || School of Information Technology

Hashing Techniques

Project Team Member

Monia Waleed Sameh Dahnon

Yara Feras Omer Al-Rbeihat

Aman Abdul Hafiz AlOudat

Heba Ibrahim Sameh Aqel

Contents

1. Introduction:

hashing is the process of converting an input of any length into a fixed side string of text using a mathematical function (hash function). It is widely used in authentication systems to avoid storing plain text passwords in databases, but is also used to validate files, documents, and other types of data.

Data is stored in hash tables as key and value pairs. Each hash table has 3 basic operations it can do: Insert, Delete and Search.

Hashing has many characteristics such as deterministic, quick computation, pre-image resistance, small changes in the input changes the hash, and collision resistant.

Some may think that encryption and hashing are the same, but the difference between them that hashing is a one-way process and there is no key that will convert the input to its original value and encryption is a two-way process that uses keys to change text into ciphertext and back.

2. Problem Statement:

Deterministic

The cryptography of hashing must be deterministic this means that any data you input into the hash function the hash output will be the same, as you can see in the figure below, we are giving an example of two users entering the same password for their accounts and the hash methodology was hashing word cat to the same hash output.

(see figure1).

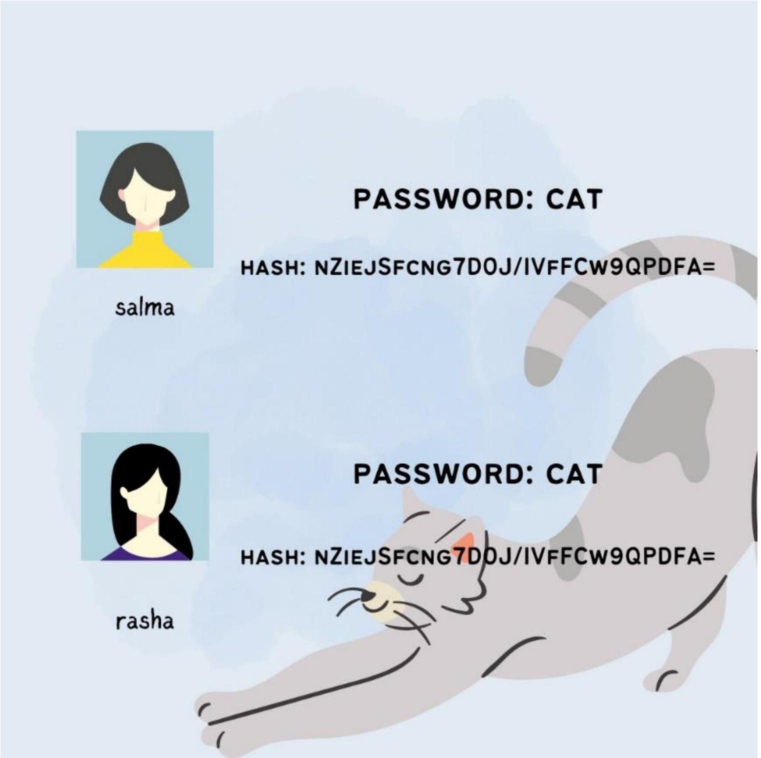
PASSWORD: CAT
HASH: NZIEJSFCNG7D0J/IVFFCW9QPDFA=
salma
PASSWORD: CAT
HASH: NZIEJSFCNG7D0J/IVFFCW9QPDFA=
rasha

Figure 1 : example

3. Problem Challenges:

Many attacks have occurred and one of them is Dictionary attack, this attack started when some systems save their users passwords in the database as a plain text without doing hashing, and it was easy to crake this plain password after that attackers have listed these passwords into a dictionary, and as much we have information in this Dictionary as much the attack will accomplish successfully. Dictionary attack is an automated and scripted attack and it mechanism based on trial-and-error tactics to decode passwords form the dictionary.

4. Problem solution:

We have found 5 solutions that can help standing against dictionary attack, some of these solutions are procedures that the user can follow to avoid Dictionary Attack without any need to a certain algorithm or code.

1.We can add what’s called a Salt (Salted hash), is a random data that is added to the beginning or the end of a password to make it unique to each user.

2.Enable multi-factor authentication.

3. Limit log-in attempts to a lower number and for false attempts make temporary log-in disable for a certain period of time.

4.Adding Web Application Firewall (WAF).

5. Conclusion and Future Recommendations:

In **Conclusion, hashing is really effective way to protect a lot of important information for businesses and individual, and if we did not use it, it could put our information in risk.**

We recommend that spreading awareness between different users about the importance of putting different passwords on the platforms that they use could help avoiding many information losing that could happen.

References

- https://www.youtube.com/watch?v=cczlpiiu42M
- **https://ctemplar.com/hashing-algorithm/**