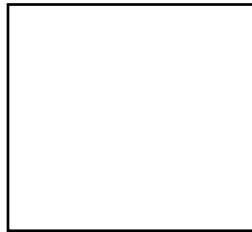


TIP-Quezon City
College of Information Technology Education

IT021 - Usable Security

Laboratory Activity 1.1 - Identifying Basic Cryptography Concepts



Score

Members:

AGUILA, KEVIN

BORRAS, JEFERSON

DOMOGMA, KENNETH DAVID

ELEDA, MARVIN LLOYD

VERGARA, BEATRICE

IT 021-IT31S1

Professor

Engr. Jerry E. Borromeo

Laboratory Activity: Identifying Basic Cryptography Concepts

Data File

Identifying Security Fundamentals\Simple Hasher.exe

Before You Begin

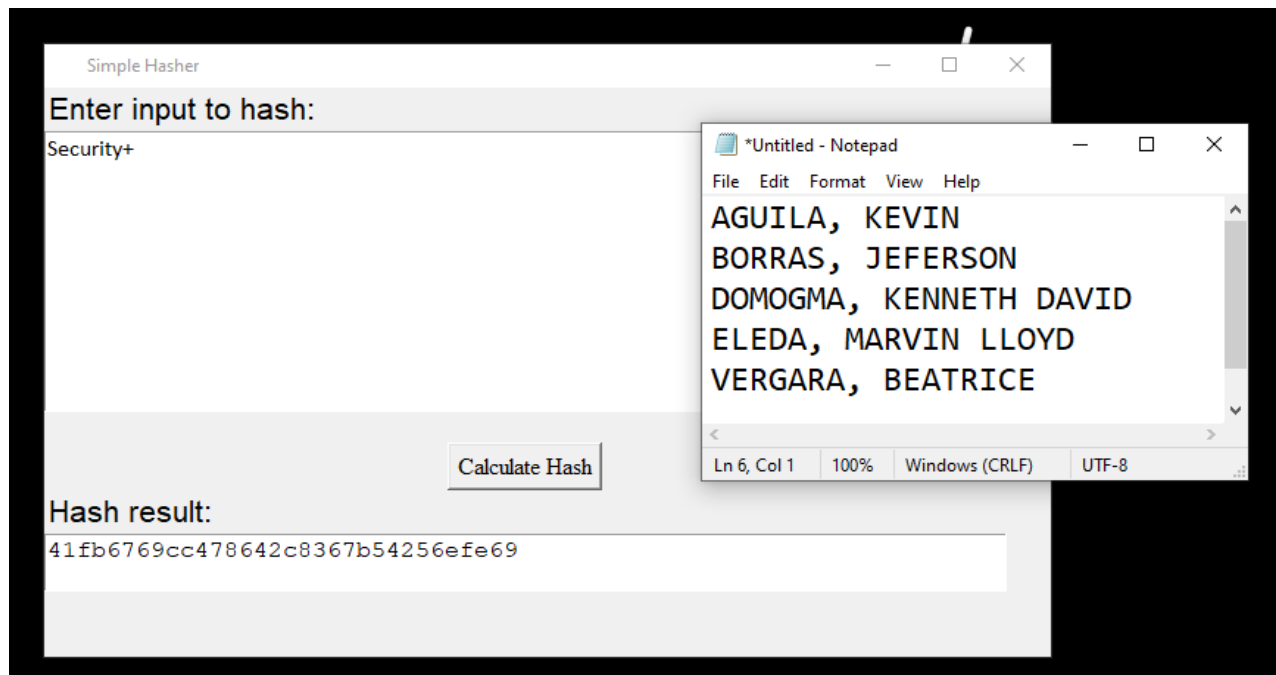
You will be using Simple Hasher, a rudimentary tool that demonstrates the concept of hashing.

Scenario

As a company security administrator, you know that you will need to implement and support cryptographic technologies to help keep company, employee, and customer data secure. To start with, you'll go over some of the fundamentals of cryptography, as well as demonstrate how simple one-way cryptography works.

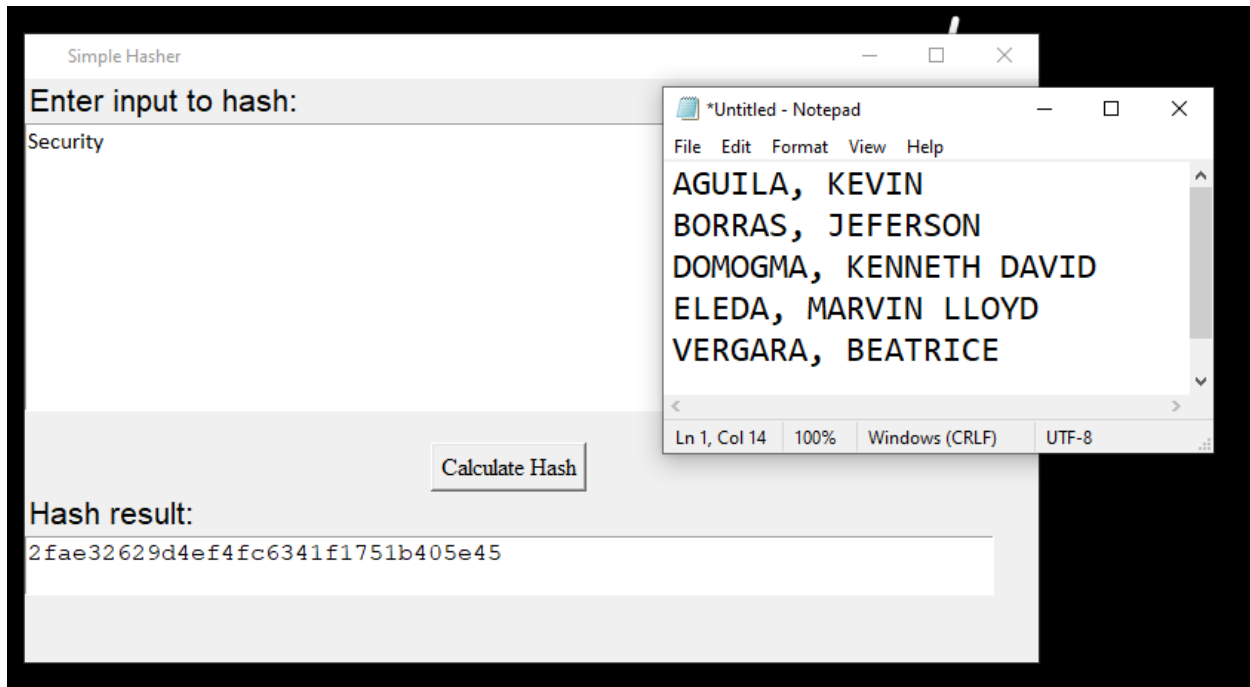
1. Examine hashing functionality.

- a) From the course data files, double-click **Simple Hasher.exe** to open it.
- b) In the **Enter input to hash** text box, type *Security+*
- c) Select **Calculate Hash**.
- d) Verify the hash result.



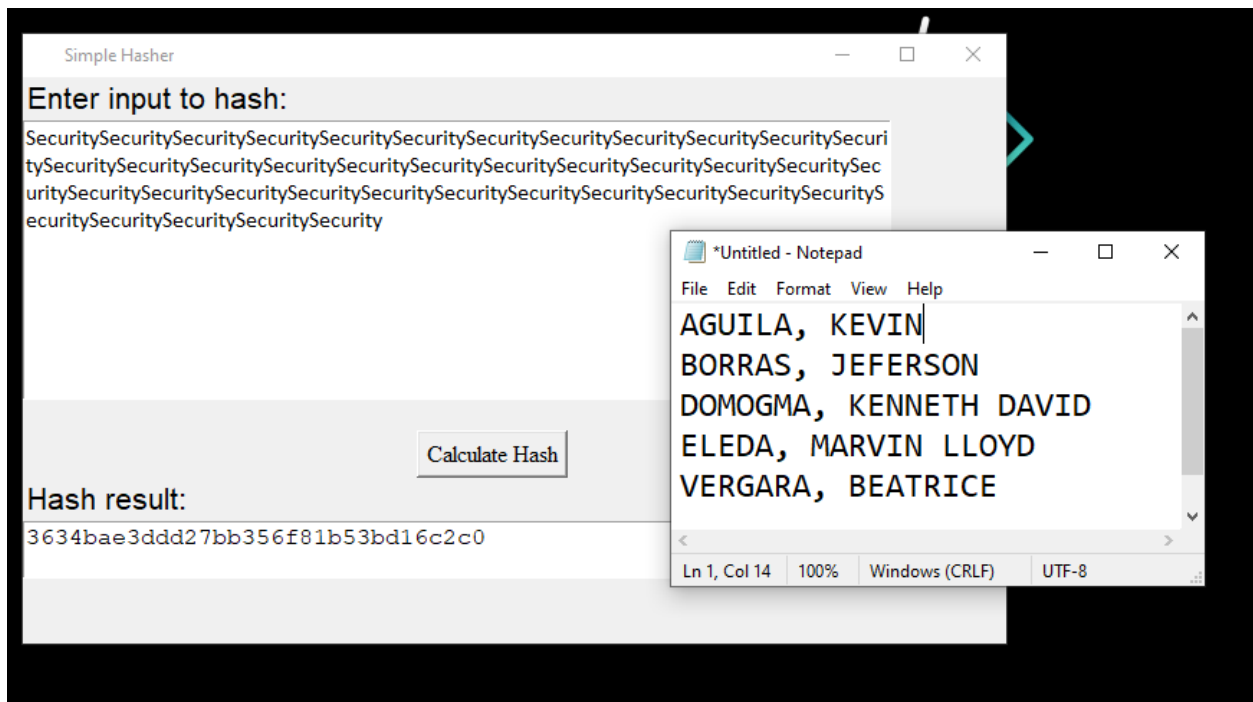
The hashing algorithm transformed your input into a fixed-length result (also known as a message digest). It is infeasible to reverse this result in order to identify your plaintext input.

- e) Remove the + from the input and select **Calculate Hash**.
- f) Verify that a minor change has produced a significantly different result.



If similar input produced similar hash results, the hashing operation would be predictable. Therefore, hashing algorithms are designed so that even a minor change in input will lead to a major change in the result.

- g) Copy the **Security** text and paste it in the **Enter input to hash** text box several times.
- h) Select **Calculate Hash**.
- i) Verify that the hash result is the same length, despite the input being significantly longer.



If the length of the input influenced the hash result, the hashing operation would be predictable. Therefore, hashing algorithms are designed to produce fixed-length message digests.

i) Close the **Simple Hasher** window.

End of activity follow-up questions:

1. Considering that hashing is one-way, and the hash is never reversed, what makes hashing a useful security technique?

Hashing is a cryptographic method for verifying the validity and integrity of various inputs. It's often used in authentication systems to keep plaintext passwords out of databases, but it's also used to verify files, documents, and other types of data. It's used to prevent unauthorized users from reading data from a file by converting it to an unreadable format, which means attackers won't be able to gain or access the contents.

- 2.** Can you describe some real-world situations where you used basic security techniques such as authentication, access control, and encryption?

The process of validating a person's or device's identity is known as authentication. When you log into a website, for example, you normally provide a username and password. When you use the correct login credentials, the website knows that you are who you say you are and that you are the one who is using it. Encryption may be used by individuals and organizations to secure sensitive information from hackers.

- To avoid identity theft and fraud, websites that send credit card and bank account numbers should always encrypt sensitive information.

Honor Pledge

"We affirm that we have not given or received any unauthorized help on this activity and that this work is our own."