

# **Parallel Project Report**

## **CUDA Parallel Implementation of Brute Force Cracking Password via SHA-1**

**BY**

<b>Miss Kanrawee</b>	<b>Chiamsakul</b>	<b>6188049</b>
<b>Mr. Tharit</b>	<b>Chantanalertvilai</b>	<b>6188068</b>

**Present**

**Assoc. Prof. Dr. Sudsanguan Ngamsuriyaroj**

**ITCS443 Parallel and Distributed Systems**

**Faculty of Information and Communication Technology**

**Mahidol University**

**2020**

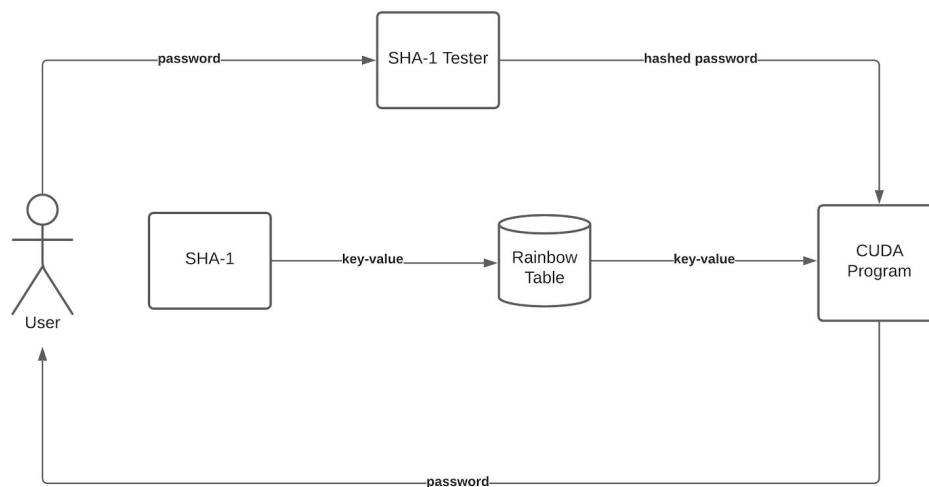
## Objective

The objective of this project is to create a program that applies the SHA-1 algorithm to hash the password number from “00000000” to “99999999” into hexadecimal value and input the hash value into the CUDA program to find the input value of this hash value. Since the SHA-1 is a one-way cryptographic hash function, the output of the function can’t be decode, so we need to create a rainbow table that records the key-value of all the given numbers and their hash value in advance.

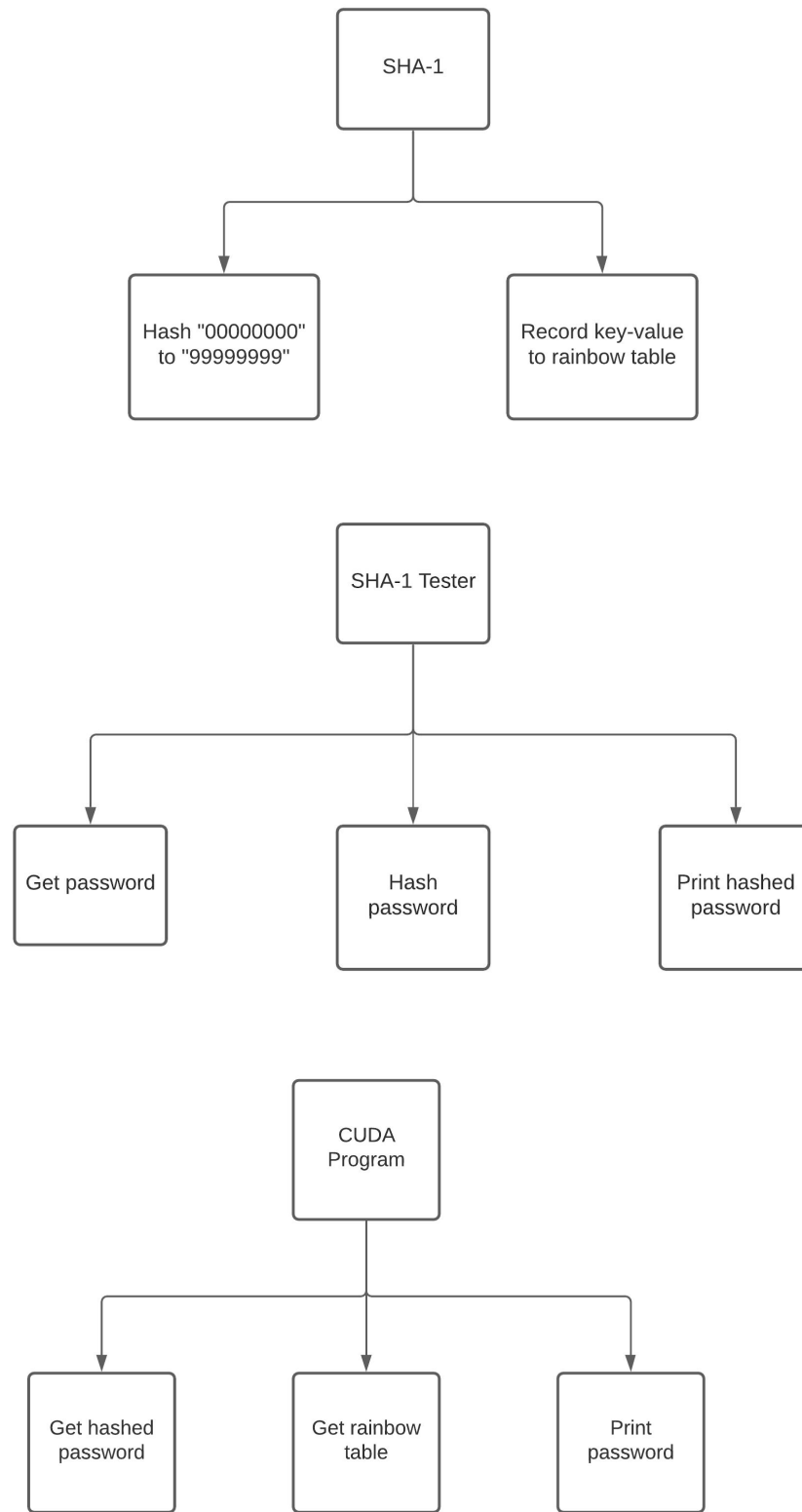
## The System Overview

SHA-1, or Secure Hash Algorithm 1, is a cryptographic hash function designed by the United States National Security Agency. The function takes an input and returns a 20-byte hash value known as a message digest.

In our project, SHA-1 is a c program that hashes the password from “00000000” to “99999999” and records it to the database as a rainbow table, which is a text file that keeps the key-value of passwords and hash values, separated by a comma. This code is referenced from <https://www.ipa.go.jp/security/rfc/RFC3174EN.html#71>. SHA-1 Tester is another c program that receives the user input password and prints the hash value to the user. Then, the hash value (hashed password) will be the input of our CUDA program, which will look up the hash value in the rainbow table and prints the corresponding password back to the user. The system overview diagram is shown below.



## The Structure Chart Showing All Functions



# The Sample Inputs and Outputs of the Project

Correct input:

```
Password (00000000 - 99999999): 00000000
70352f4161eda4ff3c32294af068ba70c3b38b
```

```
Password (00000000 - 99999999): 12345678
7c222fb2927d828af22f592134e8932480637cd
```

```
Password (00000000 - 99999999): 99999999
d528fca3b163c0573e88b528544bec28ecf185
```

Incorrect input (the program will ask the user to input again):

```
Password (00000000 - 99999999): 1234567890123
Password (00000000 - 99999999): 02587
Password (00000000 - 99999999): 0000000
Password (00000000 - 99999999): 55555555
19dd466e43cdb3833abc0609eba6d8786f9b342
```

Rainbow Table:

```
data.txt - Notepad
File Edit Format View Help
00000029,e56d22a5eb9a19a1a55d84332f577542a898ffa
00000030,7c1314ecb28efec830cb593837810d1e8a1b4c
00000031,ce8ffdbead949f16d44cd189ab85619638db4f
00000032,24ad84864cdfef751ec8d33f89ac93e018f76e55
00000033,e17cdb45c0c4855294f091e664f89f48872666
00000034,4e2ec1d33c34e7a39d3be6333cad178cde355ab
00000035,eeab409792338948b5735e106e46a420cc20e9
00000036,7d9f13e8e2275fef658ce75eb78ba69880f03e
00000037,3c428ae0ed73629b34bfd9f3ff2b6180e5d7ac6d
00000038,d7b373b0b1369b7c1f9776c3482fb7fb95a2751
00000039,71d95254836435499e14072ebcafbaf9a80ecb0
00000040,ca6377485444629f1ea4c3cdc3381ffdcc588a
00000041,7e6ca5fedaaf41bd8e67cab67603d61911a26b3
00000042,9c3a60b3d05dd27173b76f12e3837f5e739f4d9a
00000043,ae9627f7ba9e3f4d6135df2d54157f868fa11
00000044,445e49fc9ef177f0446ff5836675e15e9ff77
00000045,d0b99b5493ebcb9e4016167ba92847db4347e1
00000046,96322b35ba75f094284529bb96c893cf9bc8193b
00000047,11a717269b5777629c8cb1790588134d57e1ac1
00000048,332c85cdd89762db703fe690c8e51797271b7adc
00000049,f5ebf260ee65efa77d356941d4cbafc97dbfa5
00000050,2cf1b7f1e28221a2b1d4dd54b3dc70162d732c73
00000051,14634e2eb89165d825c0d2b2bd7c6a6875d6fa56
00000052,42ad264cd3283acaebd2142c794060e843d8764a
00000053,d2a75af6ba7044502fb9cd401a2d521b9d862f12
00000054,8dce1d6fa87cd4d964fe5b5353dc5ef19cf9f8e
00000055,787a7c398e17455e644c811d3942a62dba05153
00000056,28764aed6ebc302da9ddadeb637ec50cf2f9ab
00000057,439ec15d08cba59c343973f5b63678f9ea121a
00000058,9dd78e7eacd28210fc5ce8743fb047ca8be3d0f7
00000059,d85e84314d479dcd8b9ec978f691179b61391d
```