CS 5158/6058 Data Security and Privacy, Fall 2022
Project 2: Proof of work
Margi Amin M15219371

Software: Python 3.6.3 is required to run this if you're using Windows 10

Program Location: ..\pow_m15219371\source

File and Structure:

Data

-input.txt

-runstats.txt

-solution.txt

-target.txt

Source

-pow.py

-SolutionGeneration.py

-TargetGeneration.py

-TestRuns.py

-VerifySolution.py

Description:

1. GENERATING A TARGET VALUE

This program will take in a difficulty value from the command line and will generate a target based on this difficulty.
The target will be saved in "../data/target.txt" file in binary format.
It computes the time taken to perform this target generation function.
Replace the value <d> with a numerical value to set the difficulty

Command:
    python pow.py target <d>
Example:
    python pow.py target 20

2. GENERATING THE SOLUTION

This program will take the target value from the target.txt file, take the message from the input.txt file and then hash the message with different nonces - numbers used only once - to find a hash value that is less than the target value.

The program makes use of the hashlib library and computes the hash function using SHA-256.

The values are compared by transforming the hexadecimal hash value and the binary target value into decimal values.

When the required hash value is found, the nonce is saved as a solution in the solution.txt file.

Command:
    python pow.py sol

3. VERIFYING THE SOLUTION

This program takes the target from the target.txt file, the solution from the solution.txt file and the message from the input.txt file. A hash value of the message and the solution is performed and then compared with the target value.

The values are compared by transforming the hexadecimal hash value and the binary target value into decimal values.

If the hash value is less than the target, the solution is valid and the system outputs the value '1'.

If the hash value is more than the target, the solution is invalid and the system outputs the value '0'.

Command:
python pow.py verify

4. RUNNING FOR MULTIPLE DIFFICULTIES FROM 18-26
5.

This program will generate target values for difficulties 18, 19, 20, 21, 22, 23, 24, 25 and 26.

It will take the message from input.txt and loop through different nonces and hash with the message to find solutions
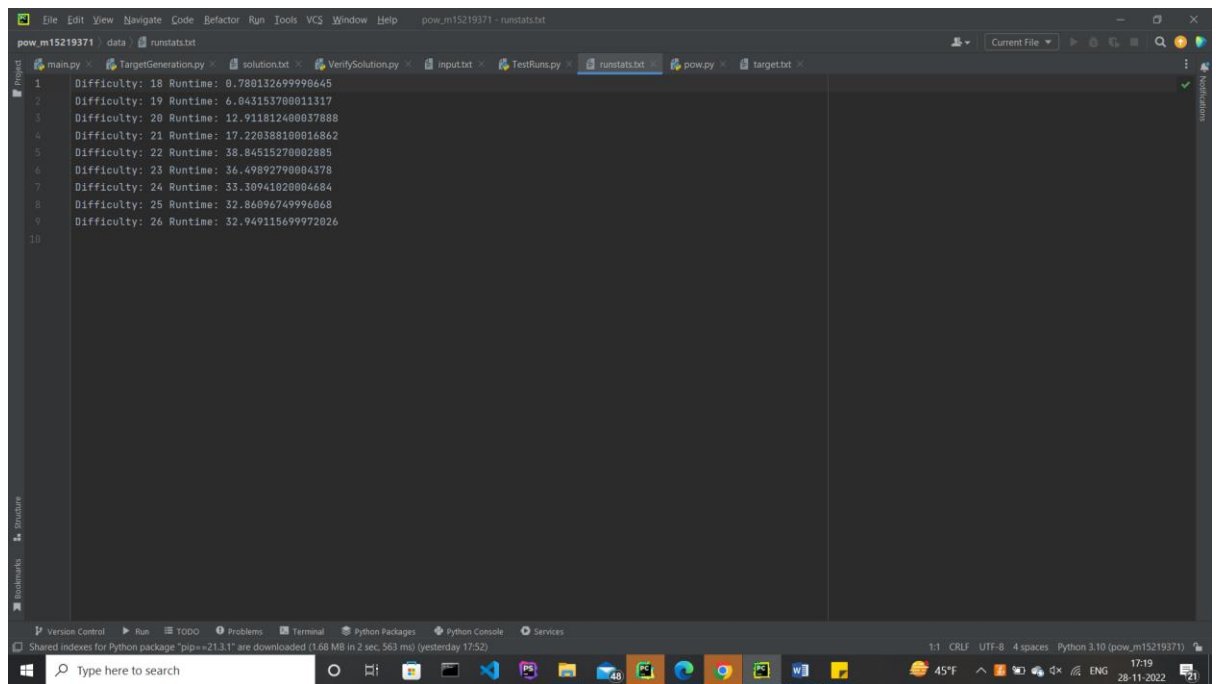
whose hash values when computed with the messages are less than their respective targets.

It will also output the runtimes for finding the program for each run.

The program will save the run stats in the runstats.txt file

Command:

python pow.py multirun

File Edit View Navigate Code Refactor Run Tools VCS Window Help

pow_m15219371 > data > runstats.txt

main.py   TargetGeneration.py   solution.txt   VerifySolution.py   input.txt   TestRuns.py   runstats.txt   pow.py   target.txt

Terminal: Local + ∨

```
Message:  m15219371
Solution:   00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000001000111101010101000110111
Output:  1

The run Time of the Solution Verification Function is:  0.02643309999257326
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

The run Time of the Function for checking difficulty  4  is:  17.220388100016862
----------------------------------------
End of RUN  4
----------------------------------------



----------------------------------------
RUN  5
----------------------------------------

Difficulty:  22

Target value =  0000000000000000000000011111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111
1111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111

The run Time of the Target Generation Function is:  0.0007809000089764595
Target:   0000000000000000000000011111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111
1111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111
Message:  m15219371
The Hash Value is:  0000022f81a1165be22ca52005cc77770f7cee7582abdb73eaf596c893964bbb
Solution value:  10451384
```

Version Control   Run   TODO   Problems   Terminal   Python Packages   Python Console   Services

Shared indexes for Python package "pip==21.3.1" are downloaded (1.68 MB in 2 sec, 563 ms) (yesterday 17:52)

1:1 CRLF UTF-8 4 spaces Python 3.10 (pow_m15219371)

Type here to search

17:20 28-11-2022

File Edit View Navigate Code Refactor Run Tools VCS Window Help

pow_m15219371 > data > runstats.txt

main.py   TargetGeneration.py   solution.txt   VerifySolution.py   input.txt   TestRuns.py   runstats.txt   pow.py   target.txt

Terminal: Local + ∨

```
Solution value:  10451384

The run Time of the Solution Generation Function is:  38.811664000037126
Target:   0000000000000000000000011111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111
1111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111
Message:  m15219371
Solution:   00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000001001111101011110011011000
Output:  1

The run Time of the Solution Verification Function is:  0.03170429996680468
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

The run Time of the Function for checking difficulty  5  is:  38.84515270002885
----------------------------------------
End of RUN  5
----------------------------------------



----------------------------------------
RUN  6
----------------------------------------

Difficulty:  23

Target value =  0000000000000000000000001111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111
1111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111

The run Time of the Target Generation Function is:  0.0008869000012055039
```

Version Control   Run   TODO   Problems   Terminal   Python Packages   Python Console   Services

Shared indexes for Python package "pip==21.3.1" are downloaded (1.68 MB in 2 sec, 563 ms) (yesterday 17:52)

1:1 CRLF UTF-8 4 spaces Python 3.10 (pow_m15219371)

Type here to search

17:20 28-11-2022

File Edit View Navigate Code Refactor Run Tools VCS Window Help   pow_m15219371 - runstats.txt

pow_m15219371 > data > runstats.txt

main.py   TargetGeneration.py   solution.txt   VerifySolution.py   input.txt   TestRuns.py   runstats.txt   pow.py   target.txt

Terminal: Local   +

```
Target value =  0000000000000000000000001111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111
11111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111

The run Time of the Target Generation Function is:  0.0008869000012055039
Target:  00000000000000000000000011111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111
11111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111
Message:  m15219371
The Hash Value is:  000000117f854402c9fa2e9f13b6b1dc7997f9f8581139013bb4d446b3f7292d
Solution value:  9295122

The run Time of the Solution Generation Function is:  36.49463630001992
Target:  00000000000000000000000011111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111
11111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111
Message:  m15219371
Solution:  000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000001000110111010101000010010
Output:  1

The run Time of the Solution Verification Function is:  0.0024066000478342175
----------------------------------------

The run Time of the Function for checking difficulty  6  is:  36.49892790004378
----------------------------------------
End of RUN  6
----------------------------------------
```

Version Control   Run   TODO   Problems   Terminal   Python Packages   Python Console   Services
Shared indexes for Python package "pip==21.3.1" are downloaded (1.68 MB in 2 sec, 563 ms) (yesterday 17:52)   1:1 CRLF UTF-8 4 spaces Python 3.10 (pow_m15219371)

Type here to search   17:20 28-11-2022

File Edit View Navigate Code Refactor Run Tools VCS Window Help   pow_m15219371 - runstats.txt

pow_m15219371 > data > runstats.txt

main.py   TargetGeneration.py   solution.txt   VerifySolution.py   input.txt   TestRuns.py   runstats.txt   pow.py   target.txt

Terminal: Local   +

```
----------------------------------------

----------------------------------------
RUN  7
----------------------------------------
Difficulty:  24

Target value =  0000000000000000000000001111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111
11111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111

The run Time of the Target Generation Function is:  0.0009076999849639833
Target:  00000000000000000000000011111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111
1111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111
Message:  m15219371
The Hash Value is:  000000117f854402c9fa2e9f13b6b1dc7997f9f8581139013bb4d446b3f7292d
Solution value:  9295122

The run Time of the Solution Generation Function is:  33.305320299987216
Target:  00000000000000000000000011111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111
11111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111
Message:  m15219371
Solution:  000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000001000110111010101000010010
Output:  1

The run Time of the Solution Verification Function is:  0.0021760999807156622
----------------------------------------
```

Version Control   Run   TODO   Problems   Terminal   Python Packages   Python Console   Services
Shared indexes for Python package "pip==21.3.1" are downloaded (1.68 MB in 2 sec, 563 ms) (yesterday 17:52)   1:1 CRLF UTF-8 4 spaces Python 3.10 (pow_m15219371)

Type here to search   17:20 28-11-2022

```
------------------------------------------------



------------------------------------------------
RUN  8
------------------------------------------------

Difficulty:  25

Target value =  00000000000000000000000001111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111
111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111

The run Time of the Target Generation Function is:  0.000784000032581389
Target:   00000000000000000000000001111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111
1111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111
Message:  m15219371
The Hash Value is:  000000117f854402c9fa2e9f13b6b1dc7997f9f8581139013bb4d446b3f7292d
Solution value:  9295122

The run Time of the Solution Generation Function is:  32.85581989999628
Target:   00000000000000000000000001111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111
1111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111
Message:  m15219371
Solution:   00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000001000110111010101000010010
Output:  1

The run Time of the Solution Verification Function is:  0.003223799983970821
------------------------------------------------
```



```
------------------------------------------------
RUN  9
------------------------------------------------

Difficulty:  26

Target value =  00000000000000000000000001111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111
111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111

The run Time of the Target Generation Function is:  0.0008844000403769314
Target:   00000000000000000000000001111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111
1111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111
Message:  m15219371
The Hash Value is:  000000117f854402c9fa2e9f13b6b1dc7997f9f8581139013bb4d446b3f7292d
Solution value:  9295122

The run Time of the Solution Generation Function is:  32.94484720000764
Target:   00000000000000000000000001111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111
1111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111
Message:  m15219371
Solution:   00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000001000110111010101000010010
Output:  1

The run Time of the Solution Verification Function is:  0.0023942000116221607
------------------------------------------------

The run Time of the Function for checking difficulty  9  is:  32.949115699972026
```