VASYL ONUFRIYEV

\*\* Part 1 START \*\*

................

For size: 1 SHA-256-> 17667 MD5-> 76393 DIFF(MD5-SHA256)-> 58726 COLL TIME IN SECS (SHA256, MD5)-> (9223372036854775807, 241471654126812)

For size: 16 SHA-256-> 23329 MD5-> 79996 DIFF(MD5-SHA256)-> 56667 COLL TIME IN SECS (SHA256, MD5)-> (9223372036854775807, 230595830712905)

For size: 64 SHA-256-> 20817 MD5-> 87354 DIFF(MD5-SHA256)-> 66537 COLL TIME IN SECS (SHA256, MD5)-> (9223372036854775807, 211172288317759)

For size: 257 SHA-256-> 22584 MD5-> 86780 DIFF(MD5-SHA256)-> 64196 COLL TIME IN SECS (SHA256, MD5)-> (9223372036854775807, 212569072063949)

For size: 400 SHA-256-> 23396 MD5-> 86951 DIFF(MD5-SHA256)-> 63555 COLL TIME IN SECS (SHA256, MD5)-> (9223372036854775807, 212151028437965)

For size: 512 SHA-256-> 23599 MD5-> 86095 DIFF(MD5-SHA256)-> 62496 COLL TIME IN SECS (SHA256, MD5)-> (9223372036854775807, 214260341177879)

For size: 1024 SHA-256-> 23430 MD5-> 81645 DIFF(MD5-SHA256)-> 58215 COLL TIME IN SECS (SHA256, MD5)-> (9223372036854775807, 225938441713632)

For size: 4096 SHA-256-> 22985 MD5-> 87495 DIFF(MD5-SHA256)-> 64510 COLL TIME IN SECS (SHA256, MD5)-> (9223372036854775807, 210831979812669)

CPU-related specs: Z7 MOBO, i7 4790k CPU, 16GB 1333Hz RAM

\*\* Part 1 END \*\*

\*\* Part 2 START \*\*

Working on generating hashes...please wait

Results tally:

...

100101110 produces-> 07�ݛ�ʅ5�cJ<��� QY��1�D�'p��}�e (after 302 hashes, 8851251 ns) 29308.778146 ns/hash

111011001110111 produces-> 02(`�x�t�7�+��[bj�}���-�o (after 30327 hashes, 84832990 ns) 2797.276025 ns/hash

101000000010100000010101 produces-> 021�q?�^�x�|��B)�/`

���C�: �u (after 10496021 hashes, 25601933818 ns) 2439.203753 ns/hash

\*\* Part 2 END \*\*

\*\* Part 3 START \*\*

Starting iteration 0 of 10 of length 10 seconds

Starting iteration 1 of 10 of length 10 seconds

Starting iteration 2 of 10 of length 10 seconds

Starting iteration 3 of 10 of length 10 seconds

Starting iteration 4 of 10 of length 10 seconds

Starting iteration 5 of 10 of length 10 seconds

Starting iteration 6 of 10 of length 10 seconds

Starting iteration 7 of 10 of length 10 seconds

Starting iteration 8 of 10 of length 10 seconds

Starting iteration 9 of 10 of length 10 seconds

Starting iteration 0 of 10 of length 20 seconds

Starting iteration 1 of 10 of length 20 seconds

Starting iteration 2 of 10 of length 20 seconds

Starting iteration 3 of 10 of length 20 seconds

Starting iteration 4 of 10 of length 20 seconds

Starting iteration 5 of 10 of length 20 seconds

Starting iteration 6 of 10 of length 20 seconds

Starting iteration 7 of 10 of length 20 seconds

Starting iteration 8 of 10 of length 20 seconds

Starting iteration 9 of 10 of length 20 seconds

Starting iteration 0 of 10 of length 30 seconds

Starting iteration 1 of 10 of length 30 seconds

Starting iteration 2 of 10 of length 30 seconds

Starting iteration 3 of 10 of length 30 seconds

Starting iteration 4 of 10 of length 30 seconds

Starting iteration 5 of 10 of length 30 seconds

Starting iteration 6 of 10 of length 30 seconds

Starting iteration 7 of 10 of length 30 seconds

Starting iteration 8 of 10 of length 30 seconds

Starting iteration 9 of 10 of length 30 seconds

10 seconds: Input String: LHCHCIAFTWLAVHPQHHVFBBJSMHGACBHJRNBJVJKWECKUUYSQCBPMRKGJWSTDLNAR-> Hash String: L,=[ ‑�3譇W&r\*gm\_   
  
MuņzmcY-> Weight: 10314

20 seconds: Input String: MOLGOXMOVRDCFFXQDBYLNGXBCMDGTLRLNKNQHIGNJPJBTDMIFEUDJLVOQYSQEDLU-> Hash String: �<SA7�JK\_M^h0UΰOaJc,mW-> Weight: 13373

~Y0�x"L-> Weight: 13449

\*\* Part 3 END \*\*

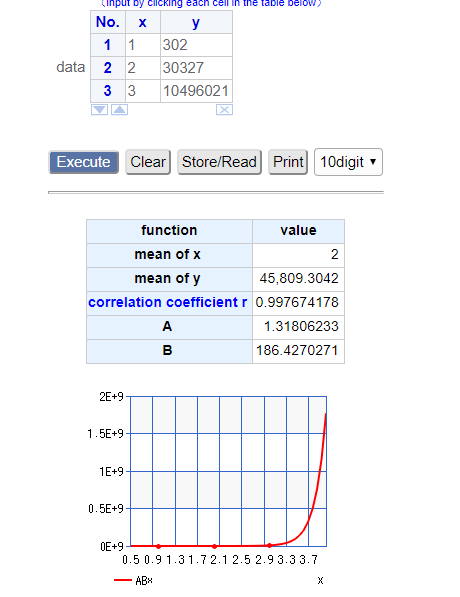
VASYL ONUFRIYEV

Part 1: CPU-related specs: Z7 MOBO, i7 4790k CPU, 16GB 1333Hz RAM

Collision times are in seconds and are displayed in (SHA256, MD5) format above in part 1.

Part 2:

Hash equation:



It will take THIS many hashes to get my full birthdate



Assuming the fastest hash time I had,

2439.203753/hash

This means that it will take (1923122462678049502.5723 \* 24309.203753)/10^9

Seconds to get my full birthday…which approximately is

46749.57578721 seconds

Which is approximately .54 of a day, or just over 12 hours.

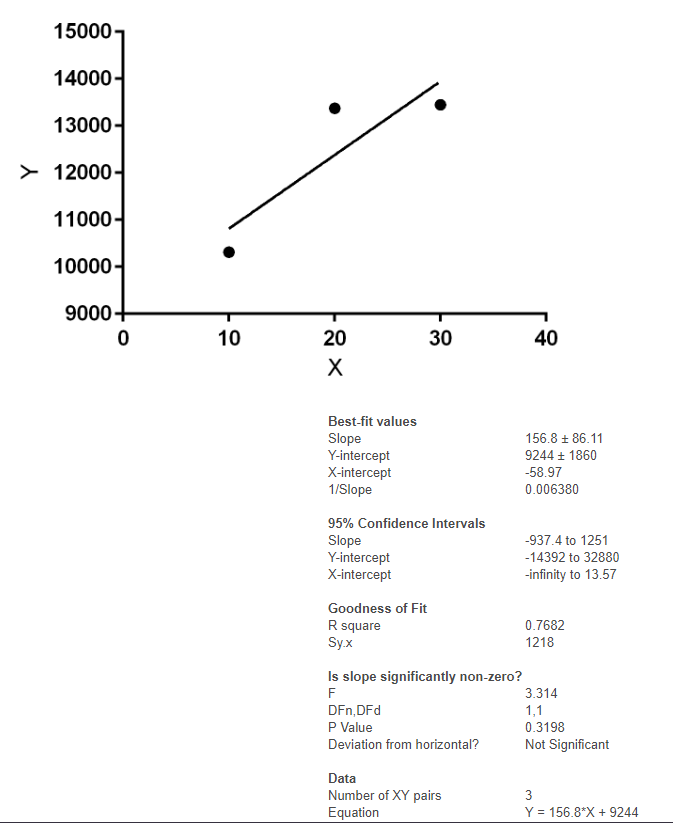
This part operates in the following manner:

Have big integer, and a function to increment the big integer. Increment big integer then output big integer in binary format. Then pass the binary big integer string into the hashing algorithm (SHa256) checker. The checker searches for up to numMatches long string in the beginning of the outgoing hash. If there is a match, document the input, the hash, and how long it took to achieve, then look for a hash starting with a string of k+1, where k is < n and n is the number of characters in the full target string, IE the birthday. Then return a result set of all matches up to the max and print out the values.

Part 3:

It seems like for my results, I got results that were very similar in their scope. All of the results were of weight 10,000 – 14,000.

So I guess that my data set can be regressed into a single linear equation:



The equation of the data would be 156.8x + 9244 according to the line of best fit.

I find it strange that I can’t find smaller values, but I think this may have to do with the way that I am calculating the weights of the output strings. I am calculating them based off their character position values. Since the hash seems to output not only UTF8 but also Unicode, the values might be a lot larger in scope. So I think the min would be a large number. Probably right around 6-7 thousand if my calculations are correct. (calculated by averaging the Unicode value set and averaging the size \* 256).