

Quiz 2

111550057 資工15 莊婷馨

Problem 1

How to run the code:

Run “python problem1.py” in terminal for (a)(b)(c).

Results:

```
(base) tinghsinchuang@zhuangtingxindeMacBook-Pro quiz2 % python problem1.py
(a)
Hash: ef0ebbb77298e1fbd81f756a4efc35b977c93dae
Password: orange
Took 124 attempts to crack input hash. Time Taken: 8.893013000488281e-05

(b)
Hash: 0bc2f4f2e1f8944866c2e952a5b59acabd1cebf2
Password: starfish
Took 2681 attempts to crack input hash. Time Taken: 0.0010502338409423828

(c)
Hash: 9d6b628c1f81b4795c0266c0f12123c1e09a7ad3
Password: redbullpuppy
Took 2854 attempts to crack input hash. Time Taken: 0.0011513233184814453
```

a) orange

Use “hashlib” in library to hash passwords and check by iteration.

b) starfish

c) redbullpuppy

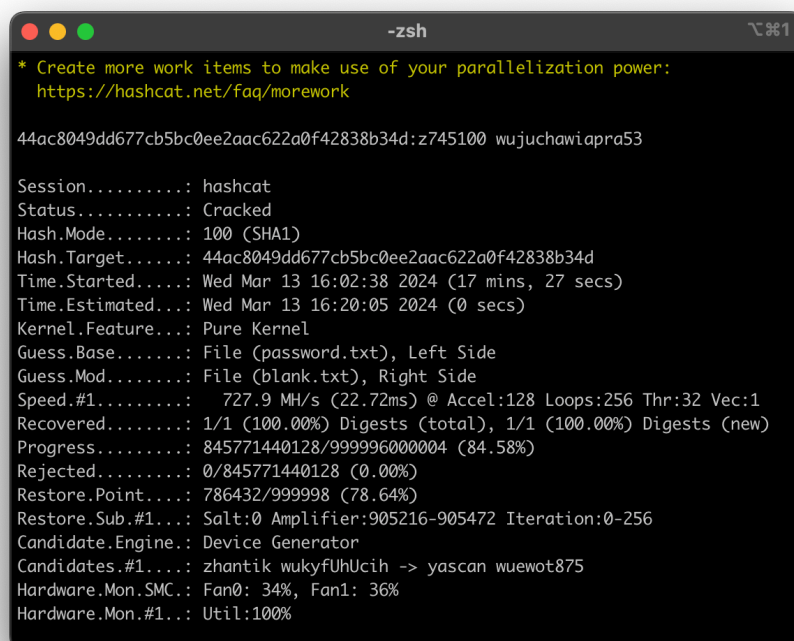
First solve the salt in the same way as (a) and (b). Add the salt (“redbull”) for every iteration.

d) z745100 wujuchawiapra53

Use hashcat with two dictionaries to get the answer. One dictionary is the original “password.txt”, the other is modified “password.txt” with a blank in the head of every line.

Attempted to solve it in problem1.py but takes too long to get a result.

command: hashcat -m 100 -a 1 h4.txt password.txt blank.txt



```
-zsh
* Create more work items to make use of your parallelization power:
  https://hashcat.net/faq/morework

44ac8049dd677cb5bc0ee2aac622a0f42838b34d:z745100 wujuchawiapra53

Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 100 (SHA1)
Hash.Target.....: 44ac8049dd677cb5bc0ee2aac622a0f42838b34d
Time.Started.....: Wed Mar 13 16:02:38 2024 (17 mins, 27 secs)
Time.Estimated...: Wed Mar 13 16:20:05 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (password.txt), Left Side
Guess.Mod.....: File (blank.txt), Right Side
Speed.#1.....: 727.9 MH/s (22.72ms) @ Accel:128 Loops:256 Thr:32 Vec:1
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 845771440128/999996000004 (84.58%)
Rejected.....: 0/845771440128 (0.00%)
Restore.Point....: 786432/999998 (78.64%)
Restore.Sub.#1...: Salt:0 Amplifier:905216-905472 Iteration:0-256
Candidate.Engine.: Device Generator
Candidates.#1...: zhantik wukyfUhUcih -> yascaan wuewot875
Hardware.Mon.SMC.: Fan0: 34%, Fan1: 36%
Hardware.Mon.#1..: Util:100%
```

Problem 2

How to run the code:

Run "python problem2.py" in terminal.

Results:

```
(base) tinghsinchuang@zhuangtingxindeMacBook-Pro quiz2 % python problem2.py
The fastest hash algorithm is SHA256
Rank of speed:
Rank 1 SHA256
Rank 2 SHA224
Rank 3 SHA1
Rank 4 SHA512
Rank 5 SHA3-224
Rank 6 SHA3-256
Rank 7 MD5
Rank 8 SHA3-512
```

The duration of execution is calculated by subtracting start time and end time. Then compare the duration of each hash function. Some slight difference happen between different executions.

Problem 3

Answer:

THE QUESTION OF WAGE AND PRICE CONTROLS WILL HAVE TO BE FACED IN SIXTY EIGHT IF CONGRESS DOES NOT APPROVE A TAX INCREASE

Code explanation:

Since there are 98 words in the ciphered text, the possible rectangles are $2*49$, $7*14$, $14*7$, and $49*2$. Calculate the average difference of vowels of each rectangle.

```
(base) tinghsinchuang@zhuangtingxindeMacBook-Pro quiz2 % python problem3.py
UNSAHEAHGRBESESPIEINIEDWCTSXTATOYSVEEOEIDAQALFGOT 1.399999999999986
OCVIGPAIILICTCWNTTEOEFOEXRRSTRLDFFONOCHNOARNEASNPE 1.600000000000014
average difference: 1.5

UIHISTEXTDENQS 0.6000000000000005
OHIEWIFTTYOING 0.3999999999999947
NGGCPEDRAFE0AN 0.6000000000000005
CEISNNOSRSCDE0 0.6000000000000005
SPRTIOWRTO0ALP 0.6000000000000005
VALETIEXLVHAAT 0.3999999999999947
AABCEECSONERFE 1.399999999999995
average difference: 0.6571428571428573

UHSETEQ 0.1999999999999973
OIWFTON 0.1999999999999973
NGPDAEA 0.1999999999999973
CINORCE 0.1999999999999973
SRIWTOL 0.8000000000000003
VLTELHA 0.8000000000000003
ABEC0EF 1.199999999999997
IITXDNS 0.8000000000000003
HEITYIG 0.1999999999999973
GCERFON 0.8000000000000003
ESNSSDO 0.8000000000000003
PTOR0AP 0.1999999999999973
AEIXVAT 1.199999999999997
ACESNRE 0.1999999999999973
average difference: 0.557142857142857
```

average differences of $2*49$, $7*14$, $14*7$ rectangles

```

TA 0.19999999999999996
ER 0.19999999999999996
TQ 0.8
IN 0.19999999999999996
EA 1.2
NE 0.19999999999999996
OL 0.19999999999999996
IA 1.2
EF 0.19999999999999996
ES 0.19999999999999996
FG 0.8
DN 0.8
OO 1.2
WP 0.8
ET 0.19999999999999996
CE 0.19999999999999996
average difference: 0.5510204081632651

```

average difference of 49*2 rectangle

```

THEQUES
TIONOFW
AGEANDP
RICECON
TROLSWI
LLHAVET
OBEFACE
DINSIXT
YEIGHTI
FCONGRE
SSDOESN
OTAPPRO
VEATAXI
NCREASE

```

Answer

The 49*2 rectangle has the lowest average difference. However, according to the hint, the text starts with “TH”, which is impossible in this rectangle. Therefore, the 14*7 rectangle is the most likely form. Then decrypt manually.