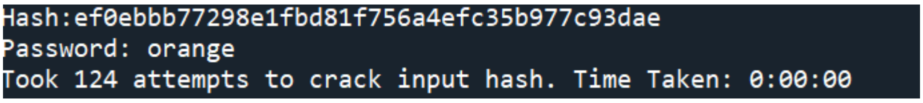
密碼工程 Quiz2

學號:112550090 姓名:曾士珍

Problem1

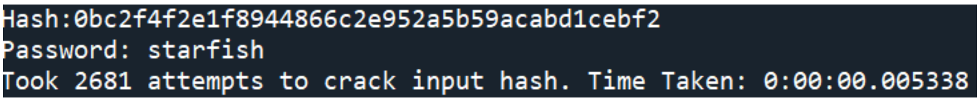
程式碼按執行即可

a) 用 python 內建的 sha1 解密函式解密



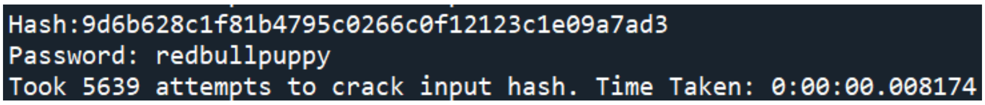
```
Hash:ef0ebbb77298e1fbd81f756a4efc35b977c93dae
Password: orange
Took 124 attempts to crack input hash. Time Taken: 0:00:00
```

b) 用 python 內建的 sha1 解密函式解密



```
Hash:0bc2f4f2e1f8944866c2e952a5b59acabd1cebf2
Password: starfish
Took 2681 attempts to crack input hash. Time Taken: 0:00:00.005338
```

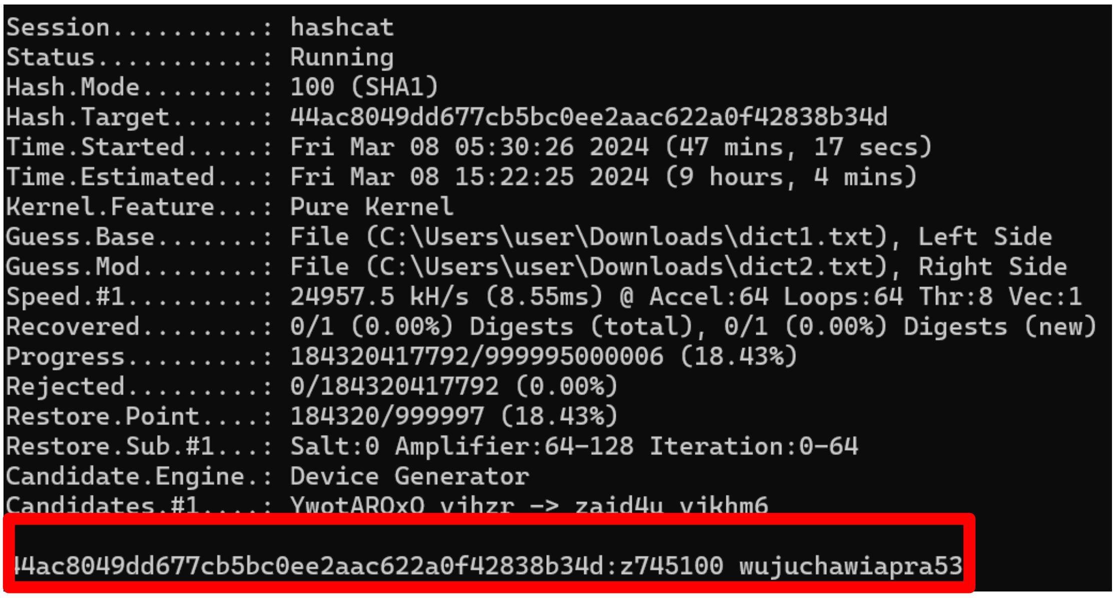
c) 用 python 內建的 sha1 解密出前半部的密碼，在枚舉後半部的密碼，合起來在用 python 內建的 sha1 解密函式解密



```
Hash:9d6b628c1f81b4795c0266c0f12123c1e09a7ad3
Password: redbullpuppy
Took 5639 attempts to crack input hash. Time Taken: 0:00:00.008174
```

d)將 password 檔案顛倒(想從文件檔最後面開始試)並複製兩份分別為 dict1 及 dict2，將 dict2 中的每個字串前都加一個空格，再利用 hashcat 跑出答案

指令：hashcat -m 100 -a 1 ${hash} dict1.txt dict2.txt

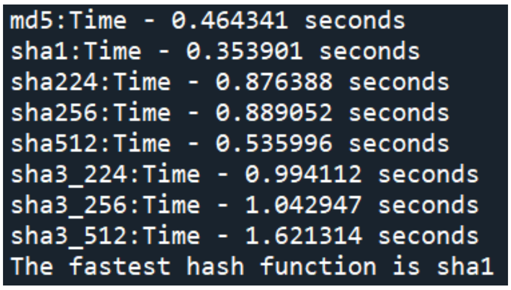


```
Session..........: hashcat
Status...........: Running
Hash.Mode........: 100 (SHA1)
Hash.Target......: 44ac8049dd677cb5bc0ee2aac622a0f42838b34d
Time.Started.....: Fri Mar 08 05:30:26 2024 (47 mins, 17 secs)
Time.Estimated...: Fri Mar 08 15:22:25 2024 (9 hours, 4 mins)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (C:\Users\user\Downloads\dict1.txt), Left Side
Guess.Mod........: File (C:\Users\user\Downloads\dict2.txt), Right Side
Speed.#1.........: 24957.5 kH/s (8.55ms) @ Accel:64 Loops:64 Thr:8 Vec:1
Recovered........: 0/1 (0.00%) Digests (total), 0/1 (0.00%) Digests (new)
Progress.........: 184320417792/999995000006 (18.43%)
Rejected.........: 0/184320417792 (0.00%)
Restore.Point....: 184320/999997 (18.43%)
Restore.Sub.#1...: Salt:0 Amplifier:64-128 Iteration:0-64
Candidate.Engine.: Device Generator
Candidates.#1....: YwotAROxO vihzr -> zaid4u vikhm6

44ac8049dd677cb5bc0ee2aac622a0f42838b34d:z745100 wujuchawiapra53
```

Problem2

a)程式碼按執行即可，以下為 output



```
md5:Time - 0.464341 seconds
sha1:Time - 0.353901 seconds
sha224:Time - 0.876388 seconds
sha256:Time - 0.889052 seconds
sha512:Time - 0.535996 seconds
sha3_224:Time - 0.994112 seconds
sha3_256:Time - 1.042947 seconds
sha3_512:Time - 1.621314 seconds
The fastest hash function is sha1
```

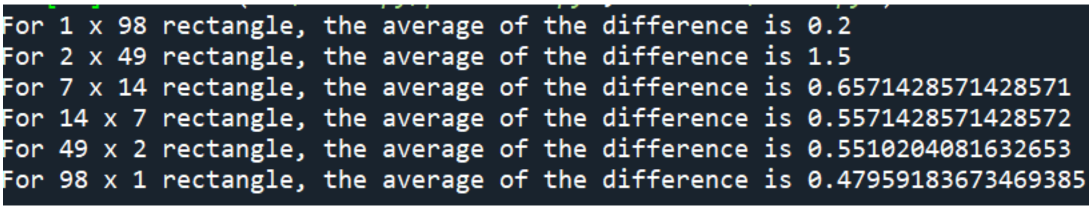
b)由上圖可以看出最快的是 sha1

c)由快到慢排序依序是：

sha1 md5 sha512 sha224 sha256 sha3_224 sha3_256 sha3_512

Problem3

有 98 個字母，先用程式過不同組合的 difference，由拆的行數跟列數來看，最有可能的拆法是 14*7 跟 7*14，由下圖 difference 的平均可以看出 14*7 比 7*14 好



```
For 1 x 98 rectangle, the average of the difference is 0.2
For 2 x 49 rectangle, the average of the difference is 1.5
For 7 x 14 rectangle, the average of the difference is 0.6571428571428571
For 14 x 7 rectangle, the average of the difference is 0.5571428571428572
For 49 x 2 rectangle, the average of the difference is 0.5510204081632653
For 98 x 1 rectangle, the average of the difference is 0.47959183673469385
```

嘗試拆成 14*7 依照英文字母的拼法觀察每行的排序順序

U	H	S	E	T	E	Q
O	I	W	F	T	O	N
N	G	P	D	A	E	A
C	I	N	O	R	C	E
S	R	I	W	T	O	L
V	I	T	E	L	H	A
A	B	E	C	O	E	F
I	I	T	X	D	N	S
H	E	I	T	Y	I	G
G	C	E	R	F	O	N
E	S	N	S	S	D	O
P	T	O	R	O	A	P

A	E	I	X	V	A	T
A	C	E	S	N	R	E
1	2	3	4	5	6	7

重排後如下：

T	H	E	Q	U	E	S
T	I	O	N	O	F	W
A	G	E	A	N	D	P
R	I	C	E	C	O	N
T	R	O	L	S	W	I
L	L	H	A	V	E	T
O	B	E	F	A	C	E
D	I	N	S	I	X	T
Y	E	I	G	H	T	I
F	C	O	N	G	R	E
S	S	D	O	E	S	N
O	T	A	P	P	R	O
V	E	A	T	A	X	I
N	C	R	E	A	S	E
5	2	6	7	1	4	3

解得 Key 為：5267143

明文如下：

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