1 Problem 1

a) Output:

```
Hash: ef0ebbb77298e1fbd81f756a4efc35b977c93dae
Password: orange
Took 124 attempts to crack input hash. Time Taken: 0.0002129077911376953
```

b) Output:

```
Hash: 0bc2f4f2e1f8944866c2e952a5b59acabd1cebf2
Password: starfish
Took 2681 attempts to crack input hash. Time Taken: 0.004041910171508789
```

c) Output:

```
Hash: 9d6b628c1f81b4795c0266c0f12123c1e09a7ad3
Password: redbullpuppy
Took 2854 attempts to crack input hash. Time Taken: 0.004421234130859375
```

d) Output:

```
Hash: 44ac8049dd677cb5bc0ee2aac622a0f42838b34d
Password: z745100 wujuchawiapra53
Command: hashcat -m 100 -a 1 44ac8049dd677cb5bc0ee2aac622a0f42838b34d
                                              revdict1.txt revdict2.txt
```

```
44ac8049dd677cb5bc0ee2aac622a0f42838b34d:z745100 wujuchawiapra53

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 100 (SHA1)
Hash.Target......: 44ac8049dd677cb5bc0ee2aac622a0f42838b34d
Time.Started.....: Fri Mar  8 02:15:30 2024 (1 hour, 19 mins)
Time.Estimated...: Fri Mar  8 03:35:02 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (revdict1.txt), Left Side
Guess.Mod........: File (revdict2.txt), Right Side
Speed.#3.........: 42077.7 kH/s (12.36ms) @ Accel:256 Loops:128 Thr:1 Vec:4
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 188803596288/999996000004 (18.88%)
Rejected.........: 0/188803596288 (0.00%)
Restore.Point....: 188416/999998 (18.84%)
Restore.Sub.#3...: Salt:0 Amplifier:94592-94720 Iteration:0-128
Candidate.Engine.: Device Generator
Candidates.#3....: z19870703a wugeatyy → Z7h6H5aE wujuchawiapra53
Hardware.Mon.SMC.: Fan0: 100%, Fan1: 99%
Hardware.Mon.#3..: Temp: 93c

Started: Fri Mar  8 02:15:24 2024
Stopped: Fri Mar  8 03:35:03 2024
```

2 Problem 2

a) Write a Python 3 program to compare the speed of the hash algorithms.
Output:

```
sha1: 0.21586 seconds
md5: 0.30677 seconds
sha512: 0.31663 seconds
sha256: 0.47160 seconds
sha224: 0.47652 seconds
sha3_224: 0.54936 seconds
sha3_256: 0.57899 seconds
sha3_512: 1.06998 seconds
```

b) Which one is the fastest?
SHA-1 is the fastest.

c) Rank the speed of each hash function.
(fastest) SHA1 > MD5 > SHA2-512 > SHA2-256 > SHA2-224 > SHA3-224 > SHA3-256 > SHA3-512 (slowest)

3 Problem 3

Given the transposition cipher:
UONCS VAIHG EPAAH IGIRL BIECS TECSW PNITE TIENO IEEFD OWECX TRSRX STTAR TLODY FSOVN EOECO HENIO DAARQ NAELA FSGNO PTE
Please decrypt this ciphertext.
Step:

a) Decompose 98 into $1 \times 98,\ 2 \times 49,\ 7 \times 14,\ 14 \times 7,\ 49 \times 2,\ 98 \times 1$.

b) Calculated the rectangle be of 14×7.

```
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 0.66
For 14 x 7 rectangle, the average of the difference is 0.56
For 49 x 2 rectangle, the average of the difference is 0.55
For 98 x 1 rectangle, the average of the difference is 0.48
```

c) The best order obtained manually is [5, 2, 6, 7, 1, 4, 3].

Cypher Text						
1	2	3	4	5	6	7
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	L	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

Plain Text						
5	2	6	7	1	4	3
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

d) Obtain the plaintext: **THE QUESTION OF WAGE AND PRICE CONTROLS WILL HAVE TO BE FACED IN SIXTY EIGHT IF CONGRESS DOES NOT APPROVE A TAX INCREASE**.

4 Appendix

Package used in the program: requests

```
pip install requests
```