密碼工程 quiz2
111550035 蔡昀錚

Problem 1

(a) orange
Took 124 attempts to crack input hash. Time Taken: 0.00040078163146972656

(b) starfish
Took 2681 attempts to crack input hash. Time Taken: 0.002605915069580078

(c) redbullpuppy
Took 2854 attempts to crack input hash. Time Taken: 0.0025339126586914062

Problem 2

(a)
Use hashlib to generate the hash result and use time to record the time-used.

md5 hash: cab08b36195edb1a1231d2d09fa450e0

sha1 hash: b29ae9b33d33304b3b966f2921cc5bfb3cb3c3ce

sha224 hash: 2dd11ca85546f0bf1029299f5d38383ab0f0942b61ae1b92b5a384be

sha256 hash: 1cadc5e09cbb81044e256f9fc67090fcf86d7a596145eb615844fe15341451e6

sha512 hash:
e6eaef73af4b739daf7e8874e1f3b87b4d320f954347e912c6cbb33f686c428b94832c46f7928e9cf685
e14452f5a0e3209edae501ac222fa6eaae7dbbb7488a

sha3_224 hash: 26c55e271dc576d3db2653dc952ab5303cc521ff788acd63a9f16716

sha3_256 hash: 02db744889e01a17accabbb69a0eca49a39058ed560d673170c631f096bef1be

sha3_512 hash:
58d0bc115ddaa7a8a03245b054be6e9b59d338508d00313b486b81430f51514c1ca5b3d569093ea795
e0d97c2c17861925af55250fff5a4a2250b5897d381dba

(b) sha224 is the fastest

(c)
Ranking of hash functions by speed:
1. sha224: 0.10942697525024414 seconds
2. sha256: 0.11172986030578613 seconds
3. sha3_224: 0.27178335189819336 seconds

4. sha1: 0.28548121452331543 seconds
5. sha3_256: 0.29292893409729004 seconds
6. sha512: 0.33185887336730957 seconds
7. md5: 0.39484119415283203 seconds
8. sha3_512: 0.5022060871124268 seconds

Problem 3

(1, 98) average difference: 0.20000000000000284
(2, 49) average difference: 1.5
(7, 14) average difference: 0.6571428571428573
(14, 7) average difference: 0.557142857142857
(49, 2) average difference: 0.5510204081632651
(98, 1) average difference: 0.47959183673469374

Since we aim to find reasonable paragraph, we can ignore (1, 98), (98, 1), (2, 49), (49, 2), compare the difference between (7, 14) and (14, 7): 0.56 < 0.66, we choose (14, 7) to be the dimension.

We can get text like this:

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

After several iterations or use Markov chain model, we have the decrypted text as following:

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

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

How to run my code: put 10-million-password-list-top-1000000.txt and BigBuckBunny.mp4 Into the same file of the code file (running with Pycharm)