Crypto Engineering Quiz 2

1.

Only hashlib, random, and time library are used. Those are all built-in libraries.
To run the code: python problem1.py

a.

Plaintext: orange

SHA-1: ef0ebbb77298e1fbd81f756a4efc35b977c93dae

Time spent: 0.001 seconds

Tries: 124

```
Hash:  ef0ebbb77298e1fbd81f756a4efc35b977c93dae
Password: orange
time: 0.0010001659393310547
tries:124
```

b.

Plaintext: starfish

SHA-1: 0bc2f4f2e1f8944866c2e952a5b59acabd1cebf2

Time spent: 0.002 seconds

Tries: 2681

```
Hash:  0bc2f4f2e1f8944866c2e952a5b59acabd1cebf2
Password: starfish
time: 0.00299835205078125
tries:2681
```

c.

SALT: redbull

Plaintext: puppy

SHA-1: 0bc2f4f2e1f8944866c2e952a5b59acabd1cebf2

Time spent: 0.006 seconds

Total tries: 5639

```
Hash:  9d6b628c1f81b4795c0266c0f12123c1e09a7ad3
Password: redbullpuppy
time: 0.006002902984619141
tries:5639
```

d.

random sample and try

still running…

2.

Only hashlib and time library are used. Those are all built-in libraries. To run the code: python problem2.py		
The results:		
Hash type	checksum	time
MD5	cab08b36195edb1a1231d2d09fa450e0	0.242s
SHA1	b29ae9b33d33304b3b966f2921cc5bfb3cb3c3ce	0.121s
SHA 224	2dd11ca85546f0bf1029299f5d38 383ab0f0942b61ae1b92b5a384be	0.134s
SHA 256	1cadc5e09cbb81044e256f9fc67090fcf86 d7a596145eb615844fe15341451e6	0.131s
SHA 512	e6eaef73af4b739daf7e8874e1f3b87b4d320f95 4347e912c6cbb33f686c428b94832c46f7928e9c f685e14452f5a0e3209edae501ac222fa6eaae7dbbb7488a	0.224s
SHA 3-224	26c55e271dc576d3db2653dc952ab 5303cc521ff788acd63a9f16716	0.352s
SHA 3-256	02db744889e01a17accabbb69a0eca 49a39058ed560d673170c631f096bef1be	0.360s
SHA 3-512	58d0bc115ddaa7a8a03245b054be6e9b59d338508 d00313b486b81430f51514c1ca5b3d569093ea795 e0d97c2c17861925af55250fff5a4a2250b5897d381dba	0.652s
Fastest: SHA-1 for 0.12100362777709961 s		
Rank: SHA1: 0.12100362777709961 s SHA256: 0.13199853897094727s SHA224: 0.13499855995178223 s SHA512: 0.22400116920471191 s MD5: 0.24299907684326172 s SHA3-224: 0.3529987335205078 s SHA3-256: 0.36099958419799805 s SHA3-512: 0.6529996395111084 s		

```
----------res----------
type: md5
time: 0.24299907684326172
checksum:cab08b36195edb1a1231d2d09fa450e0


type: sha1
time: 0.12100362777709961
checksum:b29ae9b33d33304b3b966f2921cc5bfb3cb3c3ce


type: sha224
time: 0.13499855995178223
checksum:2dd11ca85546f0bf1029299f5d38383ab0f0942b61ae1b92b5a384be


type: sha256
time: 0.13199853897094727
checksum:1cadc5e09cbb81044e256f9fc67090fcf86d7a596145eb615844fe15341451e6


type: sha512
time: 0.22400116920471191
checksum:e6eaef73af4b739daf7e8874e1f3b87b4d320f954347e912c6cbb33f686c428b94832c46f7928e9cf685e14452f5a0e3209edae501ac222fa6eaae7dbbb7488

type: sha3_224
time: 0.3529987335205078
checksum:26c55e271dc576d3db2653dc952ab5303cc521ff788acd63a9f16716


type: sha3_256
time: 0.36099958419799805
checksum:02db744889e01a17accabbb69a0eca49a39058ed560d673170c631f096bef1be


type: sha3_512
time: 0.6529996395111084
checksum:58d0bc115ddaa7a8a03245b054be6e9b59d338508d00313b486b81430f51514c1ca5b3d569093ea795e0d97c2c17861925af55250fff5a4a2250b5897d381db
```

```
----------rank----------
type: sha1
time: 0.12100362777709961
checksum:b29ae9b33d33304b3b966f2921cc5bfb3cb3c3ce


type: sha256
time: 0.13199853897094727
checksum:1cadc5e09cbb81044e256f9fc67090fcf86d7a596145eb615844fe15341451e6


type: sha224
time: 0.13499855995178223
checksum:2dd11ca85546f0bf1029299f5d38383ab0f0942b61ae1b92b5a384be


type: sha512
time: 0.22400116920471191
checksum:e6eaef73af4b739daf7e8874e1f3b87b4d320f954347e912c6cbb33f686c428b94832c46f7928e9cf685e14452f5a0e3209edae501ac222fa6eaae7dbbb7488


type: md5
time: 0.24299907684326172
checksum:cab08b36195edb1a1231d2d09fa450e0


type: sha3_224
time: 0.3529987335205078
checksum:26c55e271dc576d3db2653dc952ab5303cc521ff788acd63a9f16716


type: sha3_256
time: 0.360999584197998O5
checksum:02db744889e01a17accabbb69a0eca49a39058ed560d673170c631f096bef1be


type: sha3_512
time: 0.6529996395111084
checksum:58d0bc115ddaa7a8a03245b054be6e9b59d338508d00313b486b81430f51514c1ca5b3d569093ea795e0d97c2c17861925af55250fff5a4a2250b5897d381db
```

3.

Only numpy library is used, to install, run: pip install numpy To calculate the difference: python problem3.py -d To permute the words: python problem3.py -p
First, use the program to calculate the vowel difference. I guess the size is 7*14 or 14*7, which is a more reasonable shape. We can get:

```
E:\Code\CryptoEngineering\Lab2
→ python .\problem3.py -d
shape: 7x14
UIHISTEXTDENQS Vowel Count: 5 diff: 0.6000000000000005
OHIEWIFTTYOING Vowel Count: 6 diff: 0.39999999999999947
NGGCPEDRAFEOAN Vowel Count: 5 diff: 0.6000000000000005
CEISNNOSRSCDEO Vowel Count: 5 diff: 0.6000000000000005
SPRTIOWRTOOALP Vowel Count: 5 diff: 0.6000000000000005
VALETIEXLVHAAT Vowel Count: 6 diff: 0.39999999999999947
AABCEECSONERFE Vowel Count: 7 diff: 1.3999999999999995
Average of diff: 0.6571428571428573

shape: 14x7
UHSETEQ Vowel Count: 3 diff: 0.19999999999999973
OIWFTON Vowel Count: 3 diff: 0.19999999999999973
NGPDAEA Vowel Count: 3 diff: 0.19999999999999973
CINORCE Vowel Count: 3 diff: 0.19999999999999973
SRIWTOL Vowel Count: 2 diff: 0.8000000000000003
VLTELHA Vowel Count: 2 diff: 0.8000000000000003
ABECOEF Vowel Count: 4 diff: 1.1999999999999997
IITXDNS Vowel Count: 2 diff: 0.8000000000000003
HEITYIG Vowel Count: 3 diff: 0.19999999999999973
GCERFON Vowel Count: 2 diff: 0.8000000000000003
ESNSSDO Vowel Count: 2 diff: 0.8000000000000003
PTOROAP Vowel Count: 3 diff: 0.19999999999999973
AEIXVAT Vowel Count: 4 diff: 1.1999999999999997
ACESNRE Vowel Count: 3 diff: 0.19999999999999973
Average of diff: 0.557142857142857
```

7*14, Average diff: 0.65 UIHISTEXTDENQS OHIEWIFTTYOING NGGCPEDRAFEOAN CEISNNOSRSCDEO SPRTIOWRTOOALP VALETIEXLVHAAT AABCEECSONERFE	14*7, Average diff: 0.55 UHSETEQ OIWFTON NGPDAEA CINORCE SRIWTOL VLTELHA ABECOEF IITXDNS

	HEITYIG GCERFON ESNSSDO PTOROAP AEIXVAT ACESNRE
We can see that 14*7 is better, so start searching for the answer manually. Since the first two character is TH, so we can permute the first word to THSEUEQ. Then guess the first three word is THE, so permute the word to THESUEQ. Maybe the next phrase is QUESTION, so permute it to THEQUES. At this time, the permutation is [4, 1, 3, 6, 0, 5, 2], and the paragraph is THEQUES TIFNOOW AGDANEP RIOECCN TRWLSOI LLEAVHT OBCFAEE DIXSINT YETGHII FCRNGOE SSSOEDN OTRPPAO VEXTAAI NCSEARE Still quite weird, so try to switch the two Es and see.	

```
E:\Code\CryptoEngineering\Lab2
→ python .\problem3.py -p
THEQUES
TIONOFW
AGEANDP
RICECON
TROLSWI
LLHAVET
OBEFACE
DINSIXT
YEIGHTI
FCONGRE
SSDOESN
OTAPPRO
VEATAXI
NCREASE
```

THEQUES
TIONOFW
AGEANDP
RICECON
TROLSWI
LLHAVET
OBEFACE
DINSIXT
YEIGHTI
FCONGRE
SSDOESN
OTAPPRO
VEATAXI
NCREASE
This is the answer!
The original plaintext is:
THE QUESTION OF WAGE AND PRICE CONTROLS WILL HAVE TO BE FACED IN SIXTY EIGHT IF CONGRESS DOES NOT APPROVE A TAX INCREASE.
And the reverse permutation is [4, 1, 5, 6, 0, 3, 2]
So, the original encryption permutation is [4, 1, 6, 5, 0, 2, 3]