

Probelm 1

- (a) Password: orange
- (b) Password: starfish
- (c) Password: puppy (salt term的password是redbullpuppy)

```
Hash: ef0ebbb77298e1fbd81f756a4efc35b977c93dae
Password: orange
Took 124 attempts to crack input hash. Time Taken: 0.0003370000000000396... and so on
-----
Hash: 0bc2f4f2e1f8944866c2e952a5b59acabd1cebf2
Password: starfish
Took 2681 attempts to crack input hash. Time Taken: 0.002479000000000009... and so on
-----
Hash: dfc3e4f0b9b5fb047e9be9fb89016f290d2abb06
Password: redbull
Took 2785 attempts to crack input hash. Time Taken: 0.0025409999999999877... and so on
-----
Hash: 9d6b628c1f81b4795c0266c0f12123c1e09a7ad3
Password: redbullpuppy
Took 2854 attempts to crack input hash. Time Taken: 0.003023999999999999... and so on
```

Problem 2

(a)

```
MD5: cab08b36195edb1a1231d2d09fa450e0
time: 0.557622
-----
SHA1: da39a3ee5e6b4b0d325bfe95601890afd80709
time: 8.99999999925734e-06
-----
SHA-2(224): d14a028c2a3a2bc9476102bb288234c415a2b01f828ea62ac5b3e42f
time: 4.000000000004e-06
-----
SHA-2(256): e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
time: 2.999999999752447e-06
-----
SHA-2(512): cf83e1357eefb8bdf1542850d66d8007d620e4050b5715dc83f4a921d36ce9ce47d0d13c5d85f2b0ff8318d2877eec2f63b931bd47417a81a538327af
927da3e
time: 2.999999999752447e-06
-----
SHA-3(224): 6b4e03423667dbb73b6e15454f0eb1abd4597f9a1b078e3f5b5a6bc7
time: 4.000000000004e-06
-----
SHA-3(256): a7ffc6f8bf1ed76651c14756a061d662f580ff4de43b49fa82d80a4b80f8434a
time: 2.999999999752447e-06
-----
SHA-3(512): a69f73cca23a9ac5c8b567dc185a756e97c982164fe25859e0d1dcc1475c80a615b2123af1f5f94c11e3e9402c3ac558f500199d95b6d3e3017585862
81dcd26
time: 1.99999999946489e-06
-----
SHA-3(512) > SHA-2(256) > SHA-2(512) > SHA-3(256) > SHA-2(224) > SHA-3(224) > SHA1 > MD5
```

(b)

SHA3(512)

(c)

SHA-3(512) > SHA-2(256) > SHA-2(512) > SHA-3(256) > SHA-2(224) > SHA-3(224) > SHA1 > MD5

Problem 3

98可因式分解為 7×14 與 14×7

直接進行分析

7 * 14:

UHSETEQ	3	0.2
OIWFTON	3	0.2
NGPDAEA	3	0.2
CINORCE	3	0.2
SRIWTOL	2	0.8
VLTELHA	2	0.8
ABECOEF	4	1.2
IITXDNS	2	0.8
HEITYIG	3	0.2
GCERFON	2	0.8
ESNSSDO	2	0.8
PTOROAP	3	0.2
AEIXVAT	4	1.2
ACESNRE	3	0.2
average :		0.5571428571428572

14 * 7:

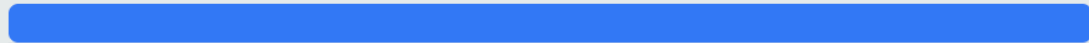
UIHISTEXTDENQS	5	0.6
OHIEWIFTTYOING	6	0.4
NGGCPEDRAFE0AN	5	0.6
CEISNNOSRSCDE0	5	0.6
SPRTIOWRT00ALP	5	0.6
VALETIEXLVHAAT	6	0.4
AABCEECS0NERFE	7	1.4
average :		0.6571428571428571

平均差異來看 14×7 較有可能

透過網頁工具

<https://www.boxentriq.com/code-breaking/columnar-transposition-cipher>

Auto Solve results



Score	Key	Text
-------	-----	------

41016	ebfgadc	the question of wage and price controls will have to be faced in sixty eight if congress does not approve a tax increase
-------	---------	--

得知plain text為 the question of wage and price controls will have to be faced in sixty eight if
congress does not approve a tax increase