Q1 -

512-bit plaintext:
C98E38D0A6584D2457D74A59D0A512CF1D5B6CA15835D3F03F16E9F749DA9A58646282F2206BEF078
5FB39FB8739E6F380E072206A6C6D9D13A09AB7825ABA24
Plaintext 1: C98E38D0A6584D2457D74A59D0A512CF
Plaintext 2: 1D5B6CA15835D3F03F16E9F749DA9A58
Plaintext 3: 646282F2206BEF0785FB39FB8739E6F3
Plaintext 4: 80E072206A6C6D9D13A09AB7825ABA24
256-bit key: C33319521704CC51EB0A67E17C8A2C2C3CC3157CB83EF1C4734020F753119E65
IV: 5EF6FF8D9C228CBDAA4F123D8B4BCBF0

Round 1:
256-bit key, IV in hex Encrypted = 75f404542ca4ac946a4a088695808592 = EncryptedText1
EncryptedText1 in hex XOR Plaintext1 in hex = bc7a3c848afce1b03d9d42df4525975d = CipherText1

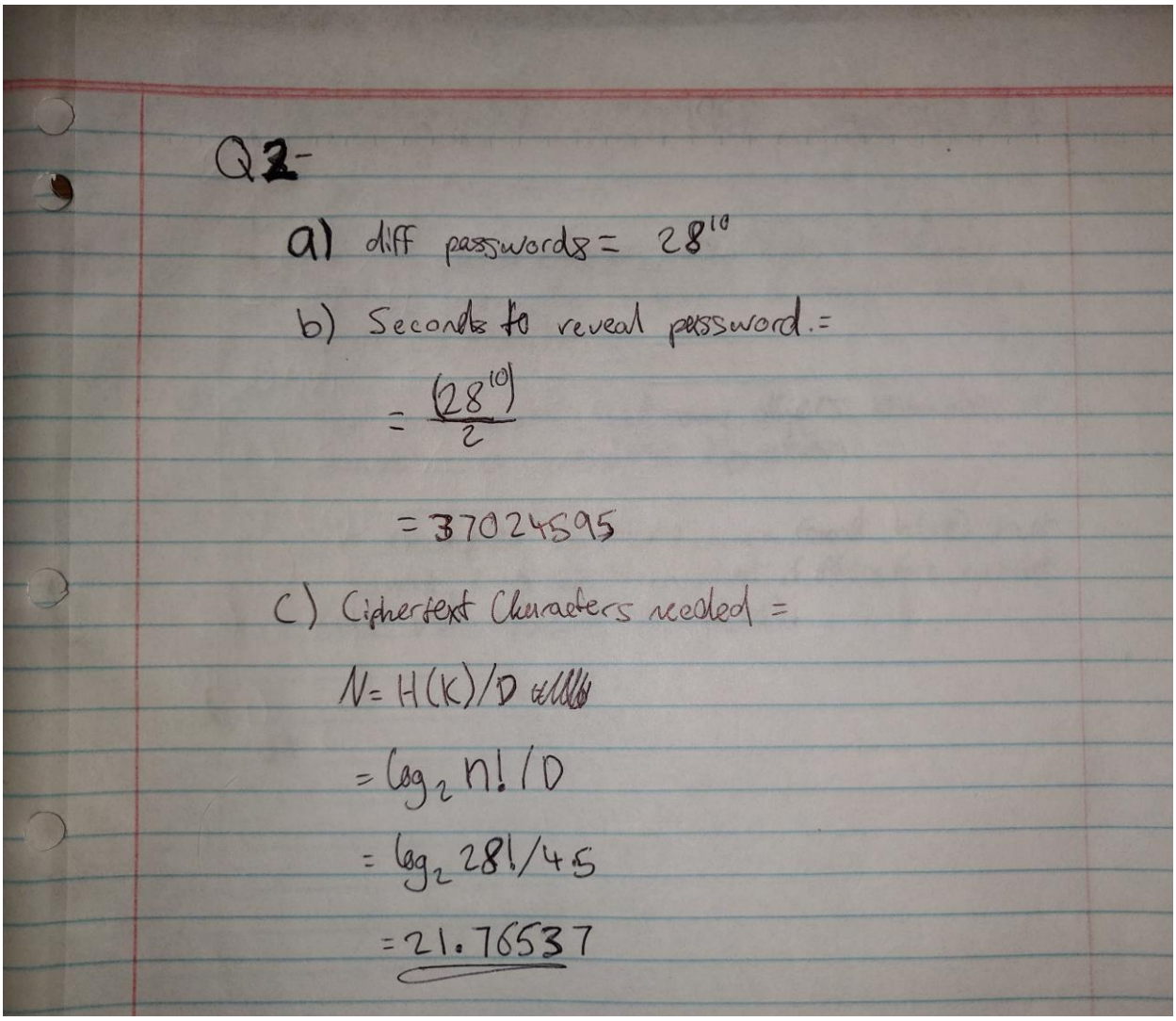
Round 2:
IV++ = 5EF6FF8D9C228CBDAA4F123D8B4BCBF1,
256-bit key, IV in hex Encrypted = 445f483a0d8b7e5f840a17d8f4d6406f = EncryptedText2
EncryptedText2 in hex XOR Plaintext2 in hex = 5904249b55beadafbb1cfe2fbd0cda370 = CipherText2

Round 3:
IV++ = 5EF6FF8D9C228CBDAA4F123D8B4BCBF2,
256-bit key, IV in hex Encrypted = 26b4c3f994e1f0474020ce609ee7a2ab = EncryptedText3
EncryptedText3 in hex XOR Plaintext3 in hex = 42d6410bb48a1f40c5dbf79b19de4458 = CipherText3

Round 4:
IV++ = 5EF6FF8D9C228CBDAA4F123D8B4BCBF3,
256-bit key, IV in hex Encrypted = c7a5730e4f8531749428dcb1ad6ec67f = EncryptedText4
EncryptedText4 in hex XOR Plaintext4 in hex = 4745012e25e95ce9878846062f347c5b = CipherText4

Cipher text:
bc7a3c848afce1b03d9d42df4525975d + 5904249b55beadafbb1cfe2fbd0cda370 +
42d6410bb48a1f40c5dbf79b19de4458 + 4745012e25e95ce9878846062f347c5b =
bc7a3c848afce1b03d9d42df4525975d5904249b55beadafbb1cfe2fbd0cda37042d6410bb48a1f40c5dbf7
9b19de44584745012e25e95ce9878846062f347c5b

Q2 -


Q2-
a) diff passwords = 28^{10}
b) Seconds to reveal password.=
$= \frac{(28^{10})}{2}$
$= 37024595$
c) Ciphertext Characters needed =
$N = H(K)/D$
$= \log_2 n!/D$
$= \log_2 28!/45$
$= 21.76537$

Q3 -

Ciphertext
wep umpp rgmusfp br znj rwmpwfepk ngw wn s qsmyp powpzw agw sffnmkbzy wn ngm srrgvcwbnz wep vswpmbsqr grpk smp cpmupfwqt rwmpwfesaqp

Using the English letter frequency distribution graph and comparing the graph shown for this ciphertext, we can see that P in the ciphertext should be E.

Using the same logic that the height of the frequency of the letter shows which letter it is in the English graph, we can easily find a few more letters.

W was set to T, M was set to R, S was set to A as those were easy because they matched up with higher letter frequency on the distribution graphs.

R was not as easy and I had to go through multiple letters to find a match that made the most sense because after adding all of those other letters into the cipher text.

This was the text after adding those letters:

tee uree rgruafe br znj rtretfeek ngt tn a qarye eotezt agt affnrkbzy tn ngr arrgvctbnz tee vaterbaqr grek are cerueftqt rtretfeaaqe

After adding S as R, there was just a lot more of the same brute forcing the correct letters. Words became pretty obvious and I changed specific letters to the correct ones and finally changed all of them.

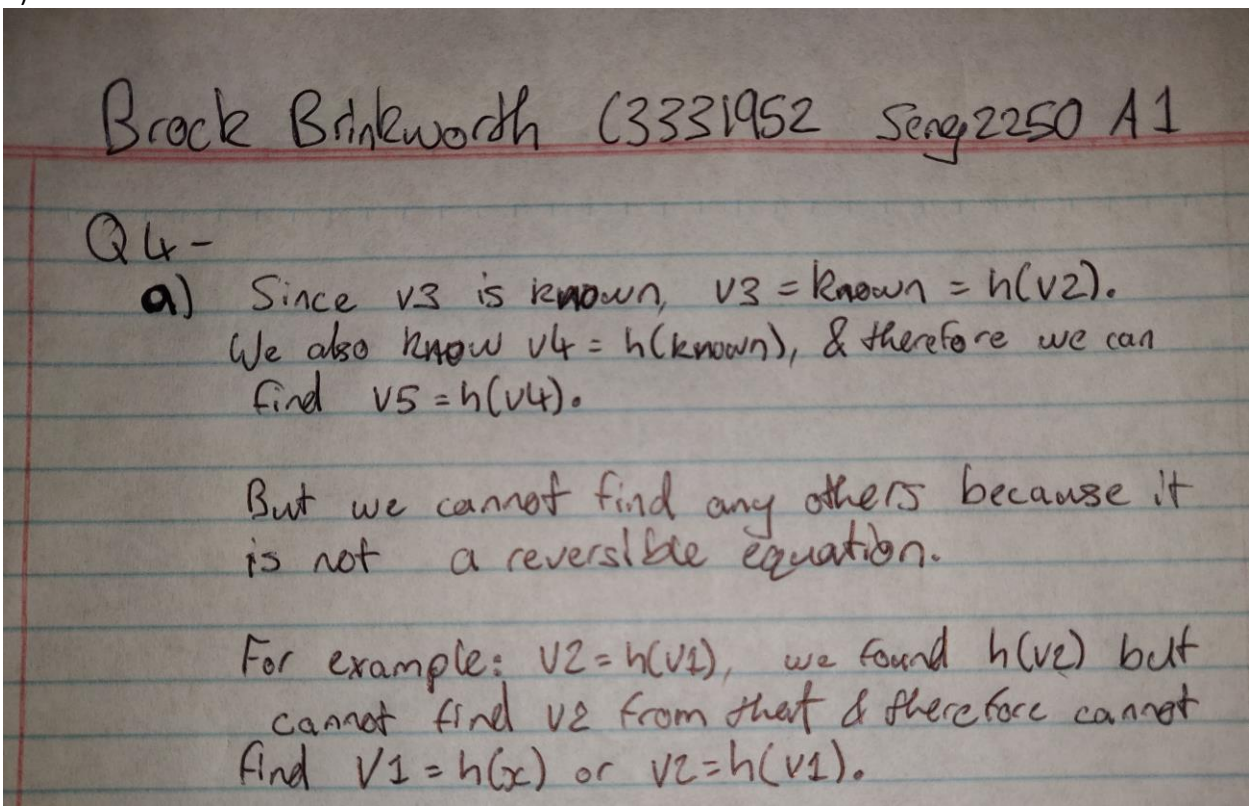
The final English text from the cipher text I found was:

The free surface is now stretched out to a large extent but according to our assumption the materials used are perfectly stretchable

CipherText	P	W	M	S	R	E	N	G	S	M	B	K	F	Z	Y	V	C
Alphabet	E	T	R	A	S	H	O	U	A	R	I	D	C	N	G	M	P

Q4 -

A)



Brock Brinkworth C3331952 Seng2250 A1

Q4 -

a) Since v3 is known, v3 = known = h(v2).
We also know v4 = h(known), & therefore we can find v5 = h(v4).

But we cannot find any others because it is not a reversible equation.

For example: v2 = h(v1), we found h(v2) but cannot find v2 from that & therefore cannot find v1 = h(x) or v2 = h(v1).

B)

1)

2)