Ans to the question no 01 (a):

Cipher text:

wep umpp rgmusfp br znj rwmpwfepk ngw wn s qsmyp powpzw agw sffnmkbzy wn

ngm srrgvcwbnz wep vswpmbsqr grpk smp cpmupfwqt rwmpwfesaqp

Plain text:

THE FREE SURFACE IS NOV STRETCHED OUT TO A LARGE EXTENT BUT ACCORDING TO OUR ASSUMPTION THE MATERIALS USED ARE PERFECTLY STRETCHABLE

Ans to the question no 01 (b):

Taking first 5 Alphabet from the cipher text:

Wep umpp

By seeing this word “wep”, I can see that P ->E as P has the highest frequency in cypher text and if I look at the common English letter frequency, I can see that E have the highest percentage. That’s why I choose that,

p->E.

After that for the cipher text E, I can apply the same formula as it is the second highest, also doing some educated guess I can determine that,

e->H

And for cipher text W I can see that I already got plaintext E and H. So, in this stage if I need to do some educated guess then I will be understood that in English “THE” is very common 3 letter word and sometimes it also starts a sentence, so by considering that I can assume that,

W->T

So I got the Plain Text “THE”

NOW, for the cipher “umpp”

We need to use the same Process:

It’s a 4-letter word where the last two letters are the same. So, I believe it could be “sees”,” Tree”,” Free” and many more. Also, if I use the word frequency system then I can get that,

For cipher text" umpp" it could be-

u->F,

m->R,

p->E,

As on the question it is mentioned that the plain text should be meaningful sentence that's why I have choose this as a most appropriate result.

Ans to the question for 02 (a)

My Student Id is -c341618.

For the Hexa-decimal, each character represent 4 bites (0-9) and (A-F)

So now the 256-bit key will be-

C3412618A9BACDEF0123456789ABCDEFC3412618A9BACDEF0123456789ABCDEF

Here, first 8 bit is my Student ID, and here I have repeated my ID for increasing the Hexa-decimal character.

Now,

Total cheracters-64.

Each character contain 4 bit-

So, (64*4)=256 bit.

For the 512 bit hexa-decimal plain text-

00112233445566778899AABBCCDDEEFF01020304050607080 90ABBCCDDEE00112233445566778899AABBCCDDEE00112233445566778899002030405060708 00

B) The Specified IV is-5F2D7CA7B3288A7F69D4E0137A8B9C00

c)

Entire plain text:
00112233445566778899AABBCCDDEEFF01020304050607080 90ABBCCDDEE00112233445566778899AA
BBCCDDEE00112233445566778899002030405060708 00

Key: C3412618A9BACDEF0123456789ABCDEFC3412618A9BACDEF0123456789ABCDEF

IV: 5F2D7CA7B3288A7F69D4E0137A8B9C00

<u>Dividing the plain text in 4 part 32 bit each:</u>

Block 1: 00112233445566778899AABBCCDDEEFF0

Block 2: 102030405060708090ABBCCDDEEF00112

Block 3: 233445566778899AABBCCDDEEFF00112

Block 4: 233445566778899A0203040506070800

Procedure:

So, here first we put our IV on the AES and then I have used the key that was generated with my student ID , after that as long as I got the encrypted text from the cipher text ,then I just XOR the first block of the plain text with the Output of AES. This procedure is similar for all the 04 blocks of my plain text. Just when I have moved from 1 block of my plain text then I need to increment my IV by 1.

Block 1:

Input of AES: 5F2D7CA7B3288A7F69D4E0137A8B9C00

Output of AES: 04f3ed8266e0984123ab2c1559cb5ac2

Result of XOR: 5e1ceb623b6ff39aa3187a99415b532

Block 2:

Input of AES: 5F2D7CA7B3288A7F69D4E0137A8B9C01

Output of AES: 4a62702cb02d94dafc822e3a1f1e6f48

Result of XOR: 148617429b62a9cd3f639e2e7f1ee6e5a

Block 3:

Input of AES: 5F2D7CA7B3288A7F69D4E0137A8B9C02

Output of AES: f3dc646766d1d8f6d6b7593e7eb94c88

Result of XOR: d0e8213101a9516c7d0b94e091494d9a

Block 4:

Input of AES: 5F2D7CA7B3288A7F69D4E0137A8B9C03

Output of AES: 2e0c6d5dcead19c29f02ab05090facbd

Result of XOR: d38280ba9d590589d01af000f08a4bd

So the whole cipher text: 5e1ceb623b6ff39aa3187a99415b532148617429b62a9cd3f639e2e7f1ee6e5a
d0e8213101a9516c7d0b94e091494d9ad38280ba9d590589d01af000f08a4bd

F)

Previous key- C3412618A9BACDEF0123456789ABCDEFC3412618A9BACDEF0123456789ABCDEF

Plain text 1:

4A3FBC92E10D7E81F20A3B4C5D6E7F90

Ciphertext: db160a342b8fa86bd58aac6bc8b44d28

Plain text 2:

4A3F**C**C92E10D7E81F20A3B4C5D6E7F90

Ciphertext: 3affd388eddcc33f469e8c2ef8a01446

Plain text 3:

4A3FCC92E10D7E81F20A3B4C5D6E7F9**1**

Ciphertext: 9d939212781ecc7dd98051a0ea0f0ebe

Plain text 4:

4**B**3FCC92E10D7E81F20A3B4C5D6E7F91

Ciphertext: 0821411a74dc0d9ba5d97bfe0aee3a11

Plain text 5:

4B3FCC9**1**E10D7E81F20A3B4C5D6E7F91

Ciphertext: 156eeb8b555608ebdf7a28bae778166a

From the above generated ciphertext it is clear that, AES exhibits the avalanche effect. This is evident because even a minor alteration of just 1 bit in the plaintext results in substantial changes to the resulting ciphertext.