Problem 2:

a) C.I.A Stands for:
1. Confidentiality: - Confidentiality refers to the idea that information should only be accessible to it’s intended recipients and those authorized to receive the information.
2. Integrity: - Integrity is the idea that information should arrive at a destination as it was sent. In tehre words, the information should not be tampered with or otherwise altered.
3. Availability: - Availability refers to the idea that information should be available to those authorized to use it.

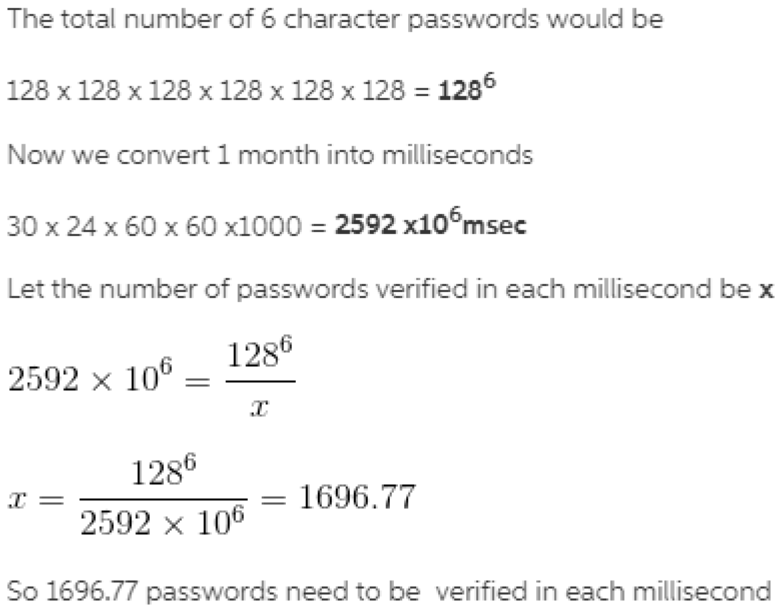
b) Private Key Cryptosystem:

When a private key cryptosystem is used, two parties who wish to communicate in secret must share a secret key. The shift cipher and affine cipher are private key cryptosystems. They are quite simple and extremely vulnerable to cryptanalysis. For extra security, a new key is used for each communication session between two parties, which require a method for generating keys and securely sharing them.

Public Key Cryptosystem:

In such a system, everyone can have a publicly known encryption key. Only the decryption keys are kept secret, and only intended recipient of a message can decrypt it. This saves the time and energy that is spent on generating new keys in case of private key cryptosystem.

c)



The total number of 6 character passwords would be

128 x 128 x 128 x 128 x 128 x 128 = **128^6**

Now we convert 1 month into milliseconds

30 x 24 x 60 x 60 x1000 = **$2592\ x10^6$msec**

Let the number of passwords verified in each millisecond be **x**

$$2592 \times 10^6 = \frac{128^6}{x}$$

$$x = \frac{128^6}{2592 \times 10^6} = 1696.77$$

So 1696.77 passwords need to be verified in each millisecond

d) MAC stands for Message Authentication Code. Its the thing that will give the sender and the receiver the assurance of untampered data. This provides the assurance that will verify both accidental and intentional modification of data received.