1)  Client and Server communicate with each other. I would like to authenticate **Server** using **challenge response scheme**.

**Authentication Process**: Server will generate a key pair say (K1, K2). He will send key K1 to client to start the communication. Client after receiving the key from the server, sends a random number say N (nonce) encrypted with key K1 to authenticate the server. He will send the nonce to check whether the key K1 was actually sent by the server or any attacker in the middle. Server after receiving the encrypted message will decrypt it using the key K2 to provide his proof of authenticity. Server will able to decrypt the message because both, K1 and K2 are created by server. If it is not able to decrypt the encrypted message, then the recipient of the encrypted message is a malicious user not the actual server.

-------------------------------------------------------------------------------

 2) In the scenario, it is shown that User A will send Na to User B. User B after receiving Na, encrypts Na with the shared secret key K and send it back to User A along with its own random no Nb. User A will receive this and decrypts the message and encrypts this shared secret key along with the random no Nb and sends it back to User B. User B after receiving this, starts the session by sending the session key encrypted with the shared secret key.

Now, a man in the middle want to attack and decrypt their communication. So, for doing this he will do the following:

 Na will be firstly received by man in the middle and this attacker will send his own random number to User B. User B will think that the number is received by User A.

 He will encrypt the number with the key and send it to User A along with his own random number. Man in the middle will receive this and sends his own random number along with the encrypted message received from User B.

 Now, User A after receiving encrypted message along with the random number sent by User B which is actually sent by the attacker, will encrypt the random number of attacker with his key and send it to User B which is again received by the man in the middle. Man in the middle will get to know the key as the key is encrypting the random number of attacker. Now attacker will encrypt the random number of User B with that key and forward it to User B.

 User B after receiving his own number in key will be ensured that the number is resent by User A only and then he will start the session by sending the session key to User A which will again be received by the attacker.

Thus how attacker or man in the middle will try to decrypt the future communication of User A and User B.

-------------------------------------------------------------------

3) **(a)**    One time pad is a type of encryption which is unbreakable. Message encrypted by the one time pad contains no information about the plain text. It is impossible to break.

**(b)**   As One Time Pad is an unbreakable, it is not used generally, i.e. it is not the widely used encryption technique. It is required only for the tasks that require high security.

**(c)**    Plain text : SENDMOREMONEY

After shifting the alphabets of plain text by 9 0 1 7 23 15 21 14 11 11 2 8 9, we get the cipher as BEOKJDMSXZPMH

**Cipher Text: BEOKJDMSXZPMH**

**(d)**  Now, we are given

**Cipher Text: BEOKJDMSXZPMH**

**Plain Text: CASHNOTNEEDED**

So, now we have to calculate the key. To calculate the key, we will see that after how many shifts of plain text, we have received our cipher text.

For example: Plain text is ‘C’ and we want ‘B’ as our cipher text. So, we will shift the letter ‘C’ by 25 positions to get ‘B’. In this way, we can get out complete key stream.

**Key Stream: 25  4  22  3  22  15  19  5  19  21  12  8  4**

-------------------------------------------------------------------------------

4)    In Steganography, we need to be secretive about our algorithms because it is very easy to break steganography compared to cryptography. But when steganography is used with cryptography, it increases the time needed to break the steganography. This is because, when steganography is used with cryptography a lot material gets added to the texts and pitchers which makes difficult for the attacker to suspect and he won’t even attempt to decrypt as he/she doesn’t know that there is an encrypted text. This is the case of security with obscurity.

**The Cipher message is:**

Dear George,

Greetings to all at Oxford. Many thanks for your

letter and for the summer examination package.

All Entry Forms and Fees Forms should be ready

for final dispatch to the Syndicate by Friday

20th or at the very latest, I’m told by the 21st.

Admin has improved here, thought there’s room

for improvement still, just give us all two or three

more years and we’ll really show you! Please

don’t let these wretched 16+ proposals destroy

your basic O and A pattern. Certainly this

sort of change, if implemented immediately,

would bring chaos.

 Sincerely yours;

As, the cipher text is given, so to receive the embedded message from the cipher text, we will use **KNOWN CIPHERTEXT** technique.

We will analyze the given text and will try to find the subset or the patter out of the given text which makes meaningful text.

Firstly, we will take first word of each sentence. It will form “Greettings letter All for 20th Admin for more don’t your sort would”. This sentence is not meaningful.

Now, taking last word of each sentence will give “**your package ready Friday 21st room three please destroy this immediately”.**Now this sentence is meaningful. So this will be our plain text message in the above paragraph.

 ------------------------------------------------------------------------------