CMR
INSTITUTE OF
TECHNOLOGY

USN										

Internal Assesment Test – II June 2021

Sub:	**Cyptography, Network Security & Cyber Law**							Code:	**17CS61**
Date:	**26 / 06 / 2021**	Duration:	90 mins	Max Marks:	50	Sem:	**VI**	Branch:	**CSE/ISE**
Note: Answer any 5 full questions									

		Marks	**OBE**	
			CO	**RBT**
1.	With relevant diagram, explain how SHA-1 algorithm is used to compute MAC.	[10]	CO3	L2
2. a)	Explain how Diffie-Hellman key exchange algorithm is used for exchanging a shared secret between two communicating parties.	[6]	CO3	L2
b)	Generate the public and private key pair using RSA algorithm and perform encryption and decryption. p=11, q=5, Message=1001	[4]	CO3	L3
3.	What is Digital Certificate? Explain the X.509 digital certificate format	[2+8]	CO4	L2
4.	Explain the following. i)Shared Secret based Mutual Authentication ii). Asymmetric Key Based Authentication	[5+5]	CO4	L2
5	Explain Needham-Schroeder Protocol	[10]	CO4	L2
5.	Demonstrate the working of Kerberos Protocol	[10]	CO4	L2
7.	Who is a Controller? Outline his functions and powers	[10]	CO6	L1
8.	Discuss the provisions of IT ACT	[10]	CO6	L1

1) With relevant diagram, explain how SHA-1 algorithm is used to compute MAC. [10]

SHA-1 (160 bit hash)

In SHA-1, the message is split into blocks of size 512 bits.
The length of the original message in bytes is converted to its binary format of 64 bits. Between the end of the message and the length field, a pad is inserted so that the length of the message+pad+64 is a multiple of 512. The pad has the form: 1 followed by the required no of 0's.
How SHA-1 computes hash of a message?

① Array Initializations- (80 word)
Each block is split into 16 words, each 32 bits wide. These 16 words occupy the first 16 positions of an array of 80 words. Remaining 64 ~~bits~~ words are obtained from:

$$w_i = w_{i-3} \oplus w_{i-8} \oplus w_{i-14} \oplus w_{i-16}; \; 16 < i \leq 80$$

— ①

② Hash Computations

A 160 bit ~~hash~~ shift register is used to compute the intermediate hash values. Initially, it is assigned a fixed pre-determin value. S1, S2, S3, S4 & S5 are the five 32-bi words making up the shift register. The bits of the shift register are then mangled together with each of the words of the array in turn. Mangling is achieved using Boolean operations: $\sim, +, \vee, \oplus, \wedge$, Rotate.

SHA-1 hash of the message is the content of the shift register after all the message blocks have been processed using the below procedure:-

```
initialize shift register, S1 S2 S3 S4 S5
for each block of the (message+pad+length) {
  create 80-word array using eqn ①
  for i = 1 to 80 {
    temp ← $S5 + (S1 << 5) + F_i(S_2, S_3, S_4) + k_i + w_i$
      $S_5 \leftarrow S_4$
      $S_4 \leftarrow S_3$
      $S_3 \leftarrow S_2 >> 2$
      $S_2 \leftarrow S1$
      $S_1 \leftarrow$ temp }
  }
}
```

$S1 << 5 \Rightarrow$ Rotation of S1 by 5 bitpositions to left
$S2 >> 2 \Rightarrow$ " " S2 by 2 " " right

Initial values in S_1, S_2, S_3, S_4, S_5 & K_i, $1 \le i \le 80$ are all predetermined.

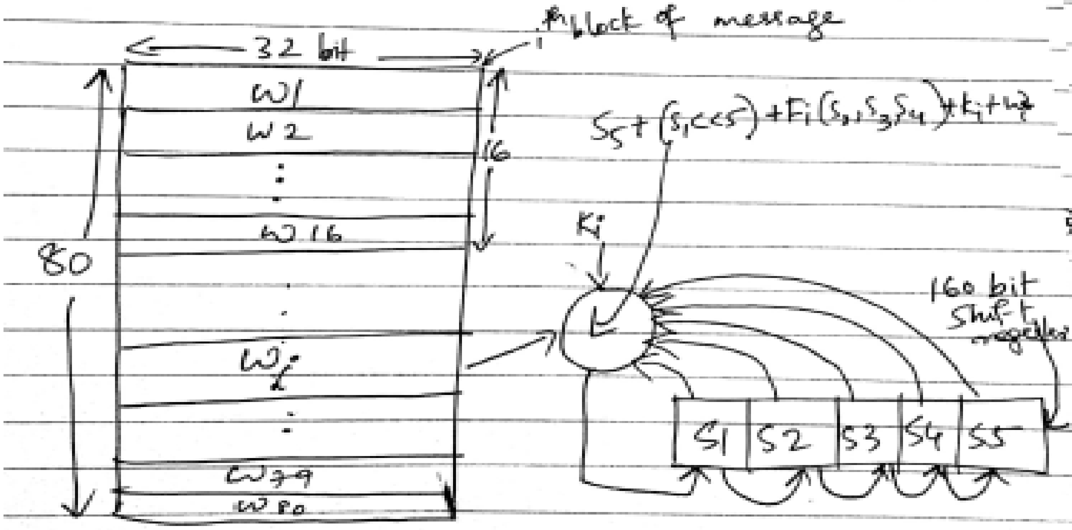
F_i is defined below: (80 processing funcs)

$$F_i(S_2, S_3, S_4) = (S_2 \wedge S_3) \vee (\sim S_2 \wedge S_4) \quad 1 \le i \le 20$$

$$F_i(S_2, S_3, S_4) = (S_2 \oplus S_3 \oplus S_4) \quad 21 \le i \le 40$$

$$F_i(S_2, S_3, S_4) = (S_2 \wedge S_3) \vee (S_2 \wedge S_4) \vee (S_3 \wedge S_4) \quad 41 \le i \le 60$$

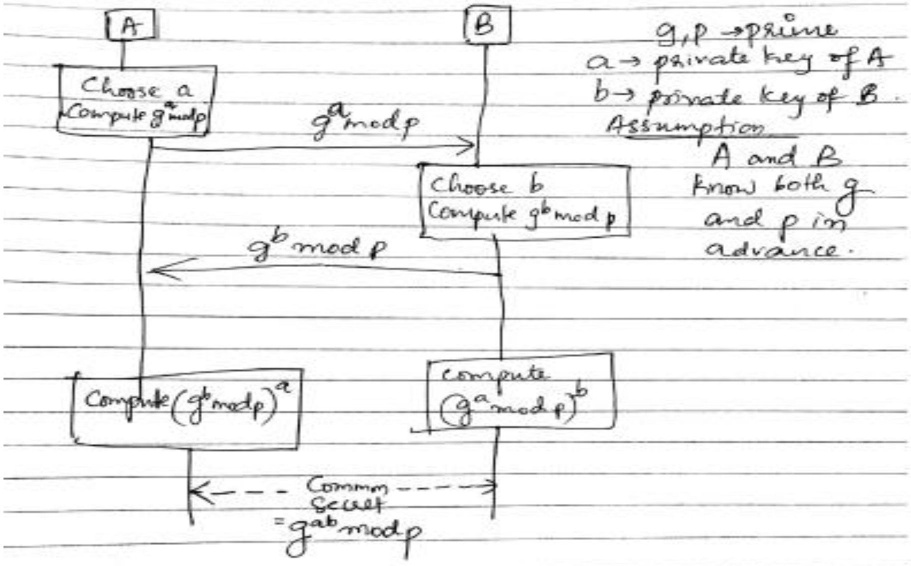
$$F_i(S_2, S_3, S_4) = S_2 \oplus S_3 \oplus S_4 \quad 61 \le i \le 80.$$



Computation of SHA-1

2) a) Explain how Diffie-Hellman key exchange algorithm is used for exchanging a shared secret between two communicating parties.
[6]

Diffie-Hellman Key Exchange



① A chooses a random integer a, $1 < a < p-1$,
Computes g^a mod p and sends to B.
② B chooses a random integer b, $1 < b < p-1$,
Computes g^b mod p and sends to A.
③ B then computes $(g^a \text{ mod } p)^b \text{ mod } p = g^{ab} \text{ mod } p$.
⑤ A then computes $(g^b \text{ mod } p)^a \text{ mod } p = g^{ab} \text{ mod } p$

A and B both share a common secret,
g^{ab} mod p.
a → A's private key, g^a mod p – A's public key.

3) What is Digital Certificate? Explain the X.509 digital certificate format [2+8]

3.2 DIGITAL CERTIFICATES

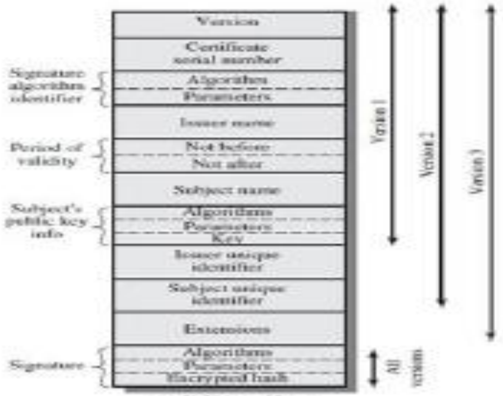
3.2.1 Certificate Types

- A digital certificate is a signed document used to ***bind a public key to the identity of a person.***
- Example such as An individual's identity could be his/her name, national identification number, e-mail .or postal address, employer, etc. or some combination of these.
- **CA:**The entity that issues certificates is a **trusted entity called a certification Authority (CA)certificate authority.**
- Certificates may be issued to individuals, to organizations, or even to servers.
- The most basic type of certificate may be applied for through regular e-mail with the applicant stating his/her public key, name, e-mail address, etc.
- In this case, the CA requires no credentials from the applicant.
- It simply assumes that the applicant is in possession of the (uncompromised) private key corresponding to the Public key contained in the application received via e-mail.
- The verifier of such a certificate should realize that the above certificates are **"Trust at your own risk certificates."**
- To carry more weight, certificate issuance would require the CA to perform identity verification of the applicant.
- The CA may have to obtain and verify several details of the applicant this task would be delegated by the *CA to the registration Authority (RA)*

3.2.2 X.509 Digital Certificate Format

- X.509 is an ITU standard specifying the format for **public key certificates.**
- The fields of an X.509 certificate together with their meaning are as follows:
  1. **Certificate Serial Number and Version** :Each certificate issued by a given CA will have a unique number.
  2. **Issuer information:** The distinguished name of an entity includes his/her/its "common name," e-mail address, organization, country, etc.
  3. **Certificate signature and associated signing algorithm information:** It is necessary to verify the authenticity of the certificate. For this purpose, it is signed by the issuer. So, the certificate should include the issuer's digital signature and also the algorithm used for signing the certificate.
  4. **Validity period:** There are two date fields that specify the ***start date and end date*** between which the certificate is valid.
  5. **Subject information** :This includes the distinguished name of the certificate's subject or owner.
     - For example, if a customer intends to communicate with an e-commerce web server at www.B-Mart.com, then the customer's browser will request B-Mart's certificate.
     - Client-side software will check whether the "Common Name" in B-Mart's certificate tallies with B-Mart's domain name.

   - Other information, such as the subject's country, state, and organization, may be included.
  6. **Subject's public key information:** The public key, the public key algorithm (e.g., RSA or DSA), and the public key parameters (modulus in the case of RSA and modulus + generator in case of Diffie-Hellman).



(a) X.509 certificate

Figure 3.1 A digital certificate

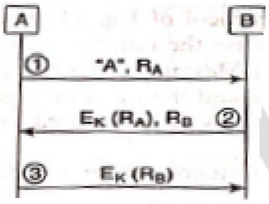
3.2.3 Digital Certificates in Action

4) Explain the following. i)Shared Secret based Mutual Authentication

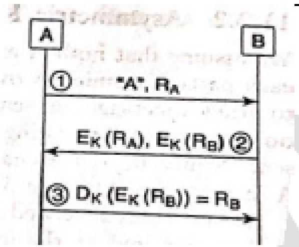
ii) Asymmetric Key Based Authentication

3.7.1 Shared Secret-based Authentication

- This is a mutual authentication using *a secret key shared by both parties.*

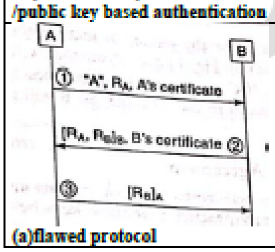
Figure : Mutual authentication using a shared secret	**Description**
 **(a) Flawed protocol**	**Message 1**: A communicates its **identity A** and its challenge in the form of a nonce **R_A**. **Message 2**: B responds to the challenge by encrypting, R_A with **common secret key , K, that A and B share.** B also sends its own challenge, R_B, to A. **Message 3**: A's response to B's challenge in the third message appears to complete the protocol for mutual authentication. , there are some serious flaws in it.

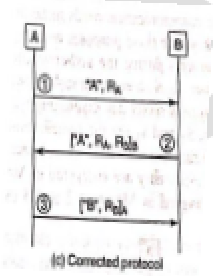
- What has the attacker C accomplished?
- C has successfully impersonated A to B.
- Message 3 was required to complete the authentication of C (posing as A) to B.
- C initiated the authentication protocol with A, presenting to A the same challenge it had received from B.
- A's response to the challenge in Message 2' was used by C to convince B that it was A that was trying to establish communication with him. This attack is termed a **Reflection Attack** since a part of the message received by an attacker is reflected back to the victim.
- In this case, the reflected message fragment is $E_K(R_B)$. This attack is also called a **Parallel Session Attack**

 A B ① "A", R_A E_K (R_A), E_K (R_B) ② ③ D_K (E_K (R_B)) = R_B **(c) Corrected protocol**	Figure c: the protocol might require the responder to encrypt his challenge, while the initiator would be required to decrypt her challenge. **Encrypting both R_A and R_B**

3.7 .2 Asymmetric Key-based Authentication

- We assume that both *A and B have public key/private key pairs.*
- The *notation $[m]_A$ means a message m, sent together with A's signature on m.*
- In the protocol of Fig. (a), each party transmits its own nonce and challenges the other to sign it.

Asymmetric key based authentication /public key based authentication	**Description**
 A B ① "A", R_A, A's certificate [R_A, R_B]_B, B's certificate ② ③ [R_B]_A **(a)flawed protocol**	figure (a) shows Mutual authentication using public key cryptography /asymmetric based authentication **MSG1: Identity of A, challenge sent by A , which is R_A , A's certificate** **MSG2: the string obtained by concatenating R_A , R_B signed by B, B's certificate.** **MSG3: R_B is the challenge signed by A(encrypted using A's private key)**

 A B ① "A", R_A ["A", R_A, R_B]$_B$ ② ③ ["B", R_B]$_A$ (c) Corrected protocol (c) **igure (c): Corrected protocol**	➢ One solution to the above problem is for the entities to include the **identity of the recipient in all messages signed .** ➢ This is shown in Fig.(c). ➢ **MSG 2**: the string obtained by concatenating nonce **R_A** and **R_B** is **signed** by **B** is **sent** . (Means encrypted using B's private key) ➢ **MSG 3**: R_B is the challenge provided by B and signed by **A** in response .(means encrypted using A's private key)

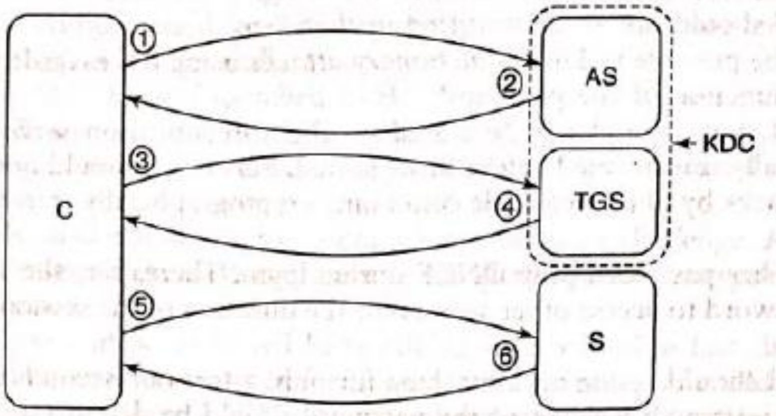
5) Demonstrate the working of Kerberos Protocol [10]

3.10 Kerberos

- A user could use the same password for all servers but distributing and maintaining a password file across multiple servers poses a securit risk.
- A password-based system should ensure the following: y
  1. The password should not be transmitted in the clear.
  2. It should not be possible to launch dictionary attacks
  3. The password itself should not be stored on the authentication server, rather it should be cryptographically transformed before being stored.
  4. It should not be possible to launch dictionary attacks by obtaining a file containing cryptographically transformed versions of the password.
  5. A user enters her password only ONCE during login. Thereafter, she should not have to re-enter her password to access other servers for the duration of the session. This feature is called **single sign-on.**
  6. The password should reside on a machine for only a few milliseconds after being entered bythe user.

The Kerberos protocol elegantly addresses many of these issues.

- Developed at MIT, Kerberos has been through many revisions.
- The latest is Kerberos Version 5.
- The KDC used in the Needham—Schroeder protocol is logically split into two entities here — the Authentication Sewer (AS) and the Ticket Granting Server (TGS).
- The sequence of messages exchanged between the client (C), the Kerberos servers (AS and TGS) and the requested server (S) is shown in Fig.3.14 .
- **There are three steps — each involving two messages**



① C request Ticket-Granting Ticket

② C receives Ticket-Granting Ticket

③ C request Service-Granting Ticket

④ C receives Service-Granting Ticket and session key

⑤ C authenticates itself to S

⑥ S authenticates itself to C

Kerberos message sequence

Step 1: Receipt of Ticket-Granting Ticket

Message 1 C → AS: "C", "TGS", Times, R_1

Message 2 AS → C: "C", Ticket_{TGS}, E_C {"TGS", $K_{C,TGS}$, *Times*, R_1}

where

$\text{Ticket}_{TGS} = E_{TGS}$ {"C", "TGS", $K_{C,TGS}$, *Times*}

Step 2: Receipt of Service-Granting Ticket

Message 3 C → TGS: "S," *Times*, Authenticator_C, Ticket_{TGS}, R_2

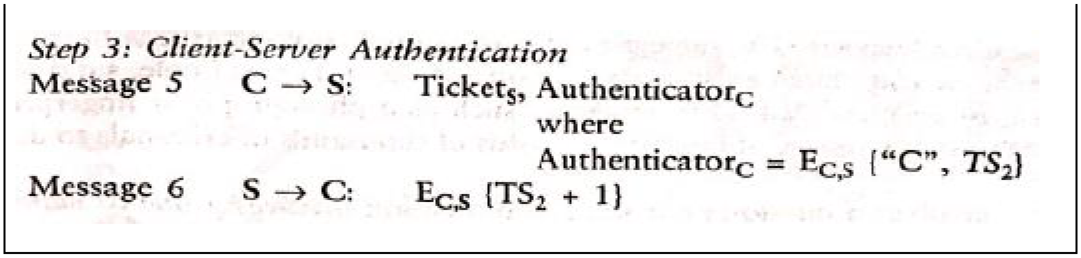
where

$\text{Authenticator}_C = E_{C,TGS}$ {"C", TS_1}

Message 4 TGS → C: "C", Ticket_S, $E_{C,TGS}$ {"S", $K_{C,S}$, *Times*, R_2}

where

$\text{Ticket}_S = E_S$ {"C", $K_{C,S}$, *Times*}



Step 3: Client-Server Authentication

Message 5 C → S: Ticket$_S$, Authenticator$_C$

where

Authenticator$_C$ = $E_{C,S}$ {"C", TS_2}

Message 6 S → C: $E_{C,S}$ {TS_2 + 1}

Step 1: Receipt of Ticket-Granting Ticket

Message 1

C → AS

- In Message 1, the client informs the AS that it wishes to communicate with the TGS.
- *"Times"* field specifies the start time and expected duration of the login session.
- "C," is the ID of the user/client who has logged in.
- R1 is a nonce generated by C

Message 2

AS → C

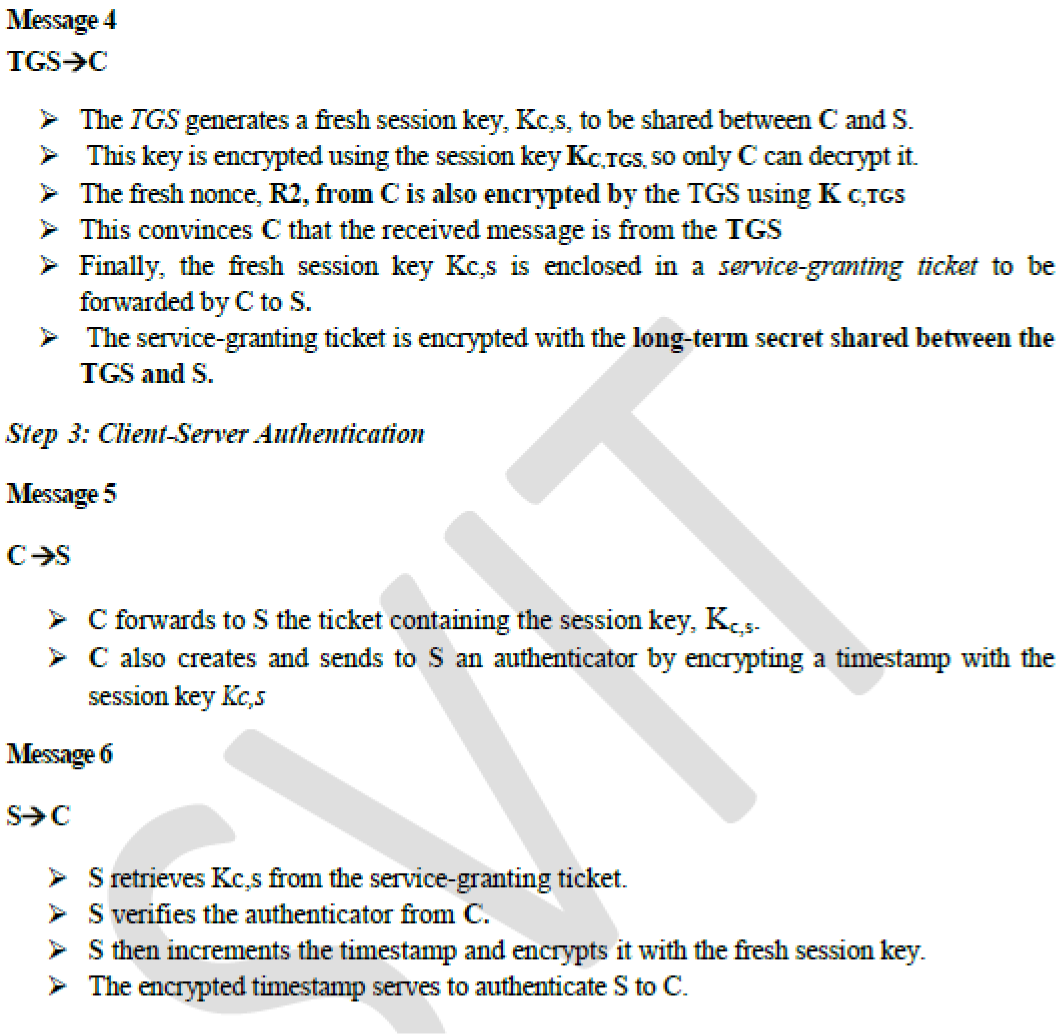
- The response from the AS (Message 2) contains a session key, **$K_{c,TGS}$**, to be used for communication between C and the TGS.
- This key is encrypted with the long-term key, KC known to C and the AS.
- This key is a function of the user's password.
- AS encrypts the nonce, that it received in Message 1.
- The nonce is used to prevent replay attacks.
- The AS also includes a TGT **(Ticket $_{TGS}$)** in connection with C's request.

Step 2: Receipt of Service-Granting Ticket

Message 3

C→TGS

- In Message 3, C forwards the TGT (Ticket $_{TGS}$), Authenticator $_C$ to the **TGS**
- Using this Ticket $_{TGS}$, **TGS server** extracts the session key, **$K_{C,TGS}$**, known only to C and the TGS.
- As shown above, the **Authenticator $_C$** encrypts the current time (timestamp) and ID using $K_{C,TGS}$



Message 4

TGS→C

- The *TGS* generates a fresh session key, Kc,s, to be shared between **C** and S.
- This key is encrypted using the session key **K**$_{C,TGS}$, so only **C** can decrypt it.
- The fresh nonce, **R2, from C is also encrypted by** the TGS using **K** $_{c,TGS}$
- This convinces **C** that the received message is from the **TGS**
- Finally, the fresh session key Kc,s is enclosed in a *service-granting ticket* to be forwarded by C to S.
- The service-granting ticket is encrypted with the **long-term secret shared between the TGS and S.**

Step 3: Client-Server Authentication

Message 5

C→S

- C forwards to S the ticket containing the session key, K$_{c,s}$.
- **C** also creates and sends to S an authenticator by encrypting a timestamp with the session key *Kc,s*

Message 6

S→C

- S retrieves Kc,s from the service-granting ticket.
- S verifies the authenticator from **C.**
- S then increments the timestamp and encrypts it with the fresh session key.
- The encrypted timestamp serves to authenticate S to C.

Who is a Controller? Outline his functions and powers [10]

Ans:

The role of Certifying Authorities is very crucial in maintaining the security & integrity of Digital Certificate.

The Central Govt appoints a "controller" of certifying authority, who performs the functions assigned by Central Govt.

Functions:

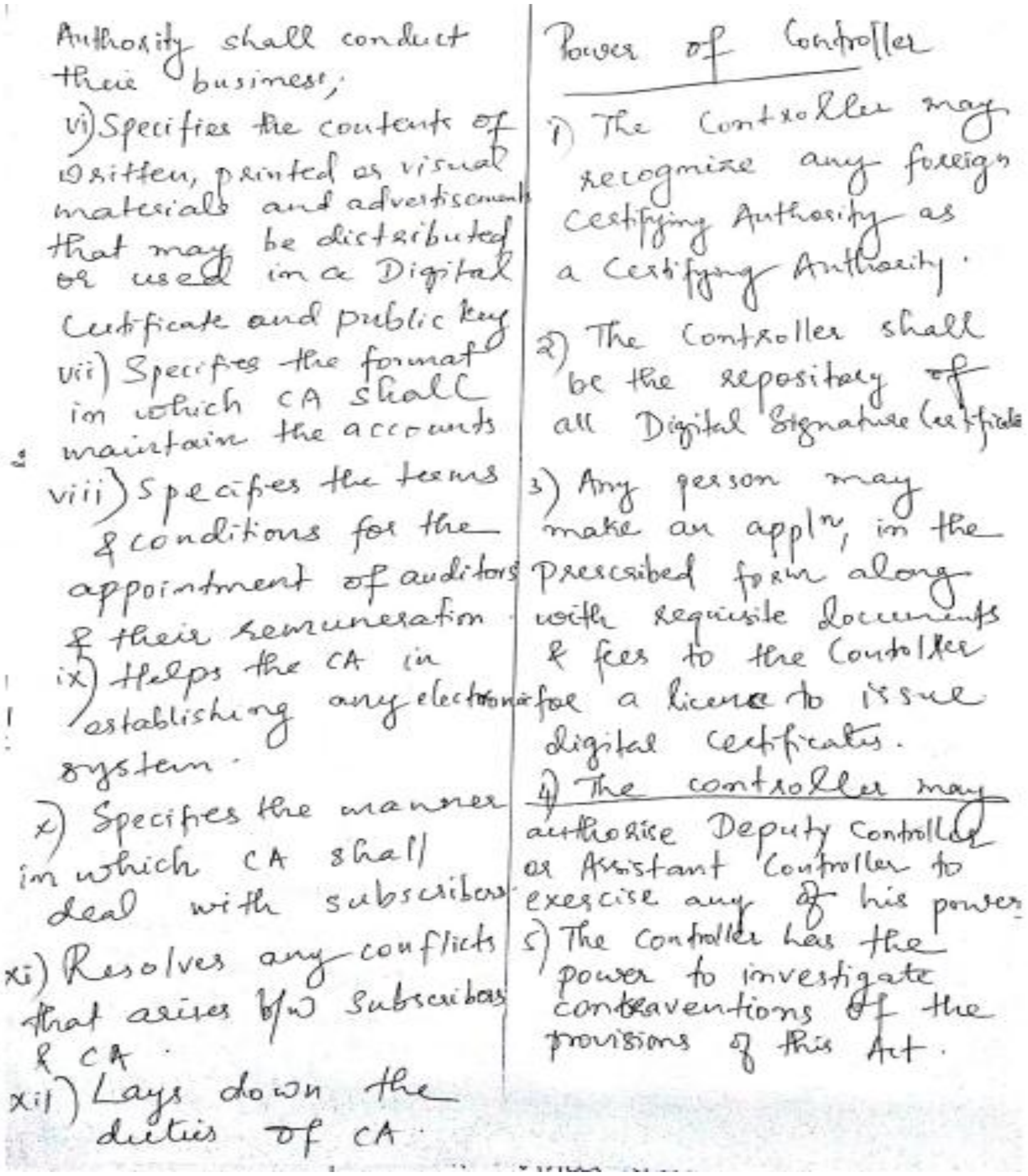
i) Supervises the activities of Certifying Authorities.

ii) Certifies public keys of Certifying authorities.

iii) Drafts the standards to be maintained by Certifying Authorities.

iv) Specifies the qualifications and experience of employees of Certifying Authorities.

v) Specify the conditions under which certifying



Authority shall conduct their business;

vi) Specifies the contents of written, printed or visual materials and advertisements that may be distributed or used in a Digital Certificate and public key

vii) Specifies the format in which CA shall maintain the accounts

viii) Specifies the terms & conditions for the appointment of auditors & their remuneration.

ix) Helps the CA in establishing any electronic system.

x) Specifies the manner in which CA shall deal with subscribers.

xi) Resolves any conflicts that arises b/w Subscribers & CA.

xii) Lays down the duties of CA.

Power of Controller

1) The Controller may recognize any foreign Certifying Authority as a Certifying Authority.

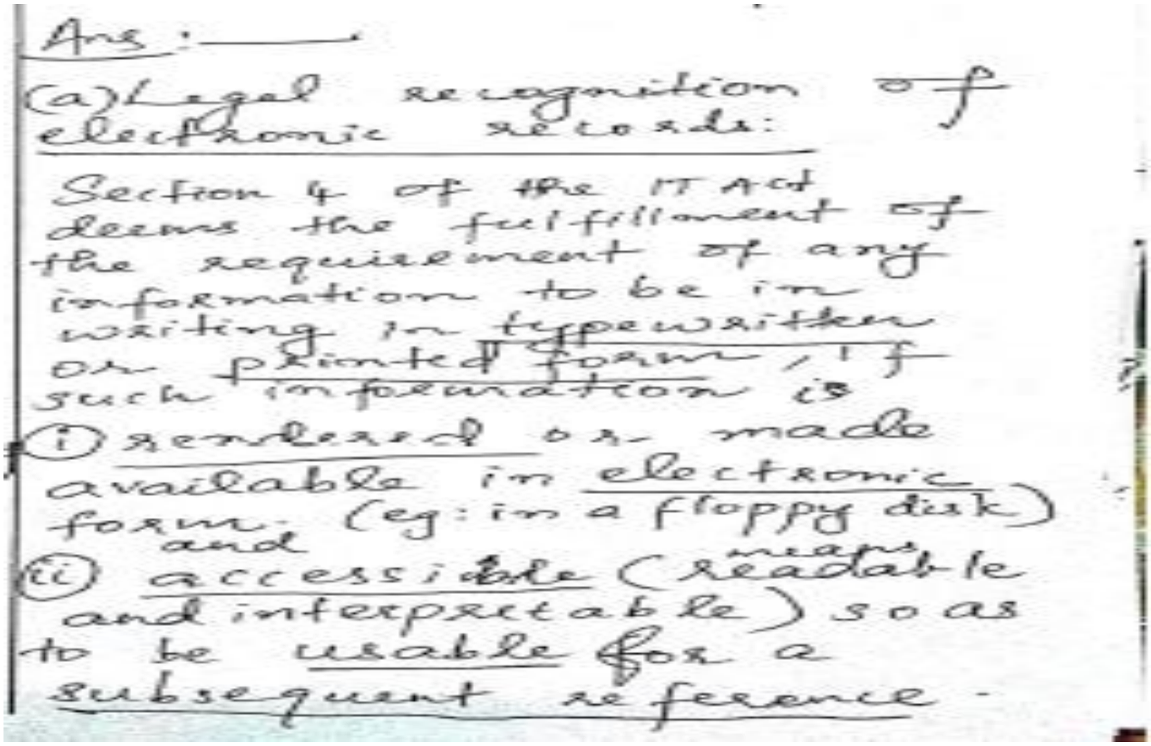
2) The Controller shall be the repository of all Digital Signature Certificate

3) Any person may make an applⁿ, in the prescribed form along with requisite documents & fees to the Controller for a licence to issue digital certificates.

4) The controller may authorise Deputy Controller or Assistant Controller to exercise any of his power.

5) The Controller has the power to investigate contraventions of the provisions of this Act.

8) Discuss the provisions of IT ACT [10]



Ans :—

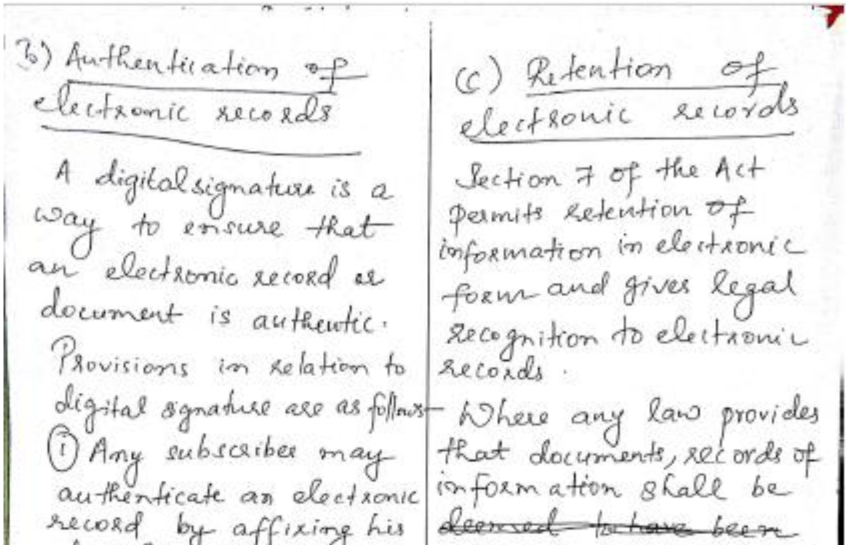
(a) Legal recognition of electronic records:

Section 4 of the IT Act deems the fulfillment of the requirement of any information to be in writing in typewritten or printed form, if such information is

(i) rendered or made available in electronic form. (eg: in a floppy disk)

and

(ii) accessible (means readable and interpretable) so as to be usable for a subsequent reference.



b) Authentication of electronic records

A digital signature is a way to ensure that an electronic record or document is authentic.

Provisions in relation to digital signature are as follows-

(i) Any subscriber may authenticate an electronic record by affixing his digital signature.

(ii) Authentication of electronic record shall be effected by the use of assymetric cryptosystem and hash function.

(iii) Any person by the use of public key of the subscriber can verify the electronic record

(iv) The private key & public key are unique to the subscriber & constitute a functioning key pair.

(c) Retention of electronic records

Section 7 of the Act permits retention of information in electronic form and gives legal recognition to electronic records.

Where any law provides that documents, records of information shall be ~~deemed to have been~~ retained for any specific period, then, that requirement shall be deemed to have been satisfied if such documents are retained in electronic form, if

(i) the information contained therein remains accessible so as to be usable for a subsequent reference;

(ii) the electronic record is retained in the original format in which it was generated, sent or received

(iii) the details of origin, destination, date & time of dispatch or receipt are available in the electronic record.