CMR INSTITUTE OF TECHNOLOGY

USN | | | | | | | | | | |

Internal Assesment Test – III May 2019

Sub:	**Cyptography, Network Security & Cyber Law**							Code:	**15CS61**
Date:	**13 / 05 / 2019**	Duration:	90 mins	Max Marks:	50	Sem:	**VA,B & C**	Branch:	**CSE**
Note: Answer any 5 full questions choosing 3 questions from Module-4 and 2 questions from Module-5									

	Module-4	**Marks**	**OBE**	
			CO	**RBT**
1.	What are the different attacks on WEP? Explain how these attacks are mitigated in TKIP and CCMP?	[10]	CO5	L2
2.	Explain the different types of Firewalls.	[10]	CO5	L1
3.	Write short note on : SOAP, WSDL	[5+5]	CO5	L1
4.	Explain types of IDS with their tasks.	[10]	CO5	L2
5.	What is Code Red? Explain the following propagation model of Code Red. i). Simple epidemic Model ii) Kermack- McKendrick model	[10]	CO5	L2

CMR INSTITUTE OF TECHNOLOGY

USN | | | | | | | | | | |

Internal Assesment Test – III May 2019

Sub:	**Cyptography, Network Security & Cyber Law**							Code:	**15CS61**
Date:	**13/ 05 / 2019**	Duration:	90 mins	Max Marks:	50	Sem:	**VA,B & C**	Branch:	**CSE**
Note: Answer any 5 full questions choosing 3 questions from Module-4 and 2 questions from Module-5									

	Module-4	**Marks**	**OBE**	
			CO	**RBT**
1.	What are the different attacks on WEP? Explain how these attacks are mitigated in TKIP and CCMP?	[10]	CO5	L2
2.	Explain the different types of Firewalls.	[10]	CO5	L1
3.	Write short note on : SOAP, WSDL	[5+5]	CO5	L1
4.	Explain types of IDS with their tasks.	[10]	CO5	L2
5.	What is Code Red? Explain the following propagation model of Code Red. i). Simple epidemic Model ii) Kermack- McKendrick model	[10]	CO5	L2

	Module-5			
6.	Define the following terms under the Information Technology Act, 2000 i) Certifying authority ii). Cyber Appellate Tribunal iii). Digital Signature iv). Secure System v). Controller	[2*5]	CO6	L1
7.	Explain various offences and punishments of cyber crime.	[10]	CO6	L1
8.	Describe the duties of Subscribers. Discuss also the penalties and adjudication under section-43 of the IT Act, 2000 for a). damage to a computer/computer systems b). failure to furnish information, return etc…	[10]	CO6	L2

	Module-5			
6.	Define the following terms under the Information Technology Act, 2000 i) Certifying authority ii). Cyber Appellate Tribunal iii). Digital Signature iv). Secure System v). Controller	[2*5]	CO6	L1
7.	Explain various offences and punishments of cyber crime.	[10]	CO6	L1
8.	Describe the duties of Subscribers. Discuss also the penalties and adjudication under section-43 of the IT Act, 2000 for a). damage to a computer/computer systems b). failure to furnish information, return etc…	[10]	CO6	L2

1) What are the different attacks on WEP? Explain how these attacks are mitigated in TKIP and CCMP? [10]

The two attacks are Known plaintext attack (Confidentiality) and Modification (Integrity) of Message.

Data Protection in TKIP & CCMP

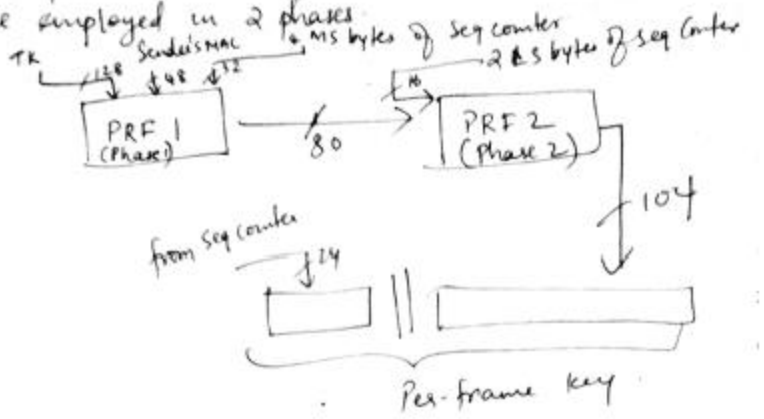
The weaknesses in WEP using stream ciphers, RC4 prompted IEEE 802.11i standards committee to seek the replacement. AES was chosen. Thus WPA (Wireless Protected Access) was born. Technical name for WPA is Temporal key Integrity Protocol (TKIP).

Implementation of 802.11i that uses AES → WPA-2. Its technical name is Counter mode with CBC MAC protocol (CCMP).

TKIP

- RC4 encryption key is used to generate key stream.
- The encryption key in TKIP is 128 bits.
- It generates a random & different encryption key for each frame sent.
- It employs a process called 2-phase key mixing
- I/ps:- 128 bit temporal key TK, Sender's MAC address, 4 bytes (Most significant bytes) of 48-bit frame sequence counter.
- Randomizing capabilities of key mixing function & large key space will guarantee that key stream collisions will never occur.
- Sequence counter is incremented for each frame sent. The receiver receives a frame only if fresh frame's seq no > previous frame received from the same sender. Prevents replay attacks.

- Two pseudo random functions (PRF1 and PRF2) are employed in 2 phases



CCMP

- Uses AES for encryption & decryption, & for providing message source authentication / integrity.
- A packet number (PN) is maintained at both sender & receiver.
- PN is incremented by the sender after each frame is sent. Upon receipt of a fresh frame in that session, receiver compares the value of PN in CCM header vs the value stored by it. If former is less than stored, frame is discarded

The first task in preparing a frame for transmission is to compute MIC.

- It is computed using AES in CBC (Cipher block chaining mode with block size = 128 bits.
- The key performing encryption in each stage is TK.
- The IV for MIC computation is a nonce - which includes 48 bit PN.
- The second & third blocks used in MIC computation are fields such as MAC addresses, sequence control, frame type.
- Next, the blocks in the frame data are sequentially processed resulting in 8-byte MIC.
- Next step is encryption.
- Frame data & MIC are concatenated & then encrypted using AES in counter mode.

① $A_i = E_{TK}(PN + i * j)$, $j \rightarrow$ constant known to sender & receiver

② $C_i = A_i \oplus P_i$

- Frame now includes CCMP header & MIC.

Upon receipt of the frame, receiver reverses the operations performed by sender followed by MIC verification.

2) Explain the different types of Firewalls. [10]

21.1.3 Firewall Types

Firewalls can be classified into the categories described in rest of this section.

Packet Filters and Stateful Inspection

Processing the ruleset in Table 21.1 involves checking for matches in the IP, TCP, or UDP headers. For example, it may be necessary to check whether a packet carries a certain specific source or destination IP address or port number. The earliest firewall designed to perform this task was referred to as a *packet filtering firewall*. It is often performed by the *border router* or *access router* that connects the organization's network to the Internet. In effect, the border router becomes the first line of defence against malicious incoming packets. We next explain why the packet filtering firewall is inadequate.

Consider an external mail server (IP address = ABC) that wishes to deliver mail to an organization. For this purpose, it should first establish a TCP connection with the organization's mail server, MS. Consider the arrival of a packet with the following attributes:

Source IP address = ABC
Destination IP address = MS
TCP destination port = 25 (SMTP port)
ACK flag set

Such a packet would be part of a normal flow provided a connection between ABC to MS has been established. But suppose such a connection has not yet been established. Should the packet still be allowed in?

The simple packet filter will allow the packet to enter even if no prior connection between ABC and MS was established. It should be noted that such packets are often used to perform *port scans*. Without an existing connection, the MS would send an RST in response to receipt of such a packet. Thus, such packets provide information to the sender regarding which ports are open on various hosts within the organization.

A simple packet filter merely inspects the headers of an incoming packet in isolation. It does not view a packet as part of a connection or flow. Hence, it will not be able to filter out such packets arriving from ABC. What is needed is a *stateful packet inspection firewall*. Such a firewall uses a packet's TCP flags and sequence/acknowledgement numbers to determine whether it is part of an existing, authorized flow. If it is participating in the establishment of an authorized connection or if it is already part of an existing connection, the packet is permitted, otherwise it is dropped. In the above example of the packet from ABC, the stateful packet inspection firewall will realize that it has not encountered the first two packets in the three-way handshake and will hence drop this packet.

Application Level Firewalls

A packet-filtering firewall, even with the added functionality of stateful packet inspection, is still severely limited. It understands the network and transport layer headers but is indifferent to the application being run. What is needed is a firewall that can examine the *application payload* and scan packets for worms, viruses, spam mail, and inappropriate content. Such a device is called a *deep inspection firewall*.

A special kind of application-level firewall is built using proxy agents. Such a "proxy firewall" acts as an intermediary between the client and server. The client establishes a TCP connection to the proxy and the proxy establishes another TCP connection with the server as shown in Fig. 21.1. To a client, the proxy appears as the server and to the server, the proxy appears as the client. Since there is no direct connection between the client and the server, worms and other malware will not be able to pass between the two, assuming that the proxy can detect and filter out the malware. Hence, the presence of the proxy enhances security.

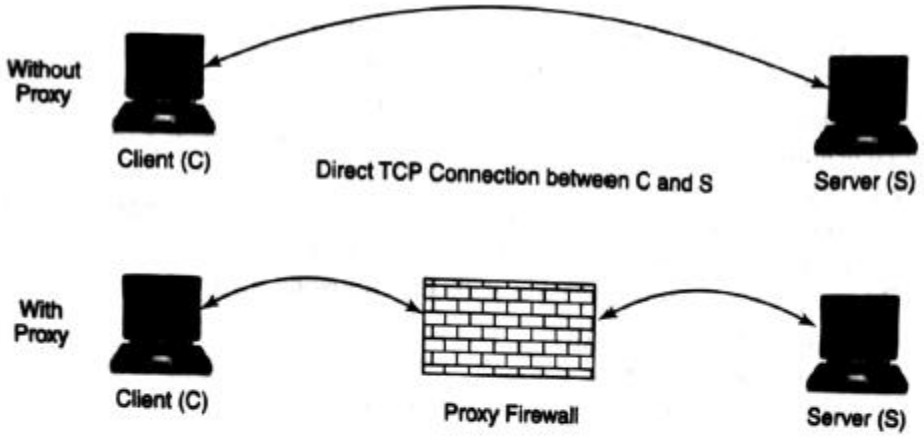


Figure 21.1 *Proxy firewall*

There are proxy agents for many application layer protocols including HTTP, SMTP, and FTP. In addition to filtering based on application layer data, proxies can perform client authentication and logging. An HTTP proxy can also cache webpages. Caching has a major impact on performance. If the webpage is cached in a web proxy server located in the client's organization, the response time could be greatly reduced compared to that where the page has to be fetched from the external web server. Also, caching reduces the demand on external communication bandwidth while easing the load on the web server.

3) Write short note on : SOAP, WSDL [5+5]

SOAP

What is SOAP?

- SIMPLE OBJECT ACCESS PROTOCOL
- For exchanging structured information over internet.
- SOAP can be used over any transport protocol such as TCP, HTTP, SMTP
- SOAP defines a model for processing individual, one-way messages
- The mapping between soap message and an underlying transport protocol is referred as SOAP binding.
- Soap may run on top of http ot SMTP.

19

SOAP Message Format

- SOAP message consists of three parts:
  - SOAP Envelope
  - SOAP Header (optional)
  - SOAP Body

SOAP Header:

- The Header element is a generic container for control information
- Header blocks should contain information that influences payload processing
- Header is optional

SOAP Body:

- The Body element represents the message payload

20

```
<?xml version="1.0"?>
<soap:Envelope
 xmlns:soap = "http://www.w3.org/2001/12/soap-envelope . . .>
  <soap:Body xmlns:X="http://www.stockQuote.com/price">
    <X:GetPrice xmlns:X = "http://www. . . " >
      <X:StockName> MyStartUp </X:StockName>
    </X:GetPrice>
  </soap:Body>
</soap:Envelope>
```

(a) SOAP message in HTTP POST request

April 29th, 2003 Organizing and Searching Information with XML 21

```
<?xml version="1.0"?>
<soap:Envelope
 xmlns:soap = "http://www.w3.org/2001/12/soap-envelope . . . >
  <soap:Body xmlns:X="http://www.stockQuote.com/price">
    <X:GetPriceResponse xmlns:X = "http://www. . . " >
      <X:Price> 3847 </X:Price>
    </X:GetPriceResponse>
  </soap:Body>
</soap:Envelope>
```

(b) SOAP message in HTTP response

22

WSDL:

WSDL

- Web services Definition langauge
- "An XML format for describing network services as a set
- Contains information where the service is located, what the service does, and how to invoke the service such as types ,messages,operation,port types,and bindings.
- Operation:abstract definition of a n action.
- Message: abstract definition of data beingexchanged as a part of operation.

23

WSDL

```
<message name="message1">
   <part name=" . . . " type=" . . . "/>
</message>

<message name="message2">
   <part name=" . . . " type=" . . . "/>
</message>

<portType name="portType1">
  <operation name=" . . . ">
      <input message="message1"/>
      <output message="message2"/>
  </operation>
</portType>
```

Port type that includes one operation comprising two messages

24

4) Explain types of IDS with their tasks. [10]

Types of IDS

Events of interest to an IDS

Variable Monitored	Event of interest	Possible Attack
No. of access to specific file	Tenfold increase over norm	DOS Attack
Login frequency	Unusually high	Attempted break-in
TCP header flags	Invalid combination	Port Scan
O.S. calls	Particular sequence of calls	Specific Virus Attack

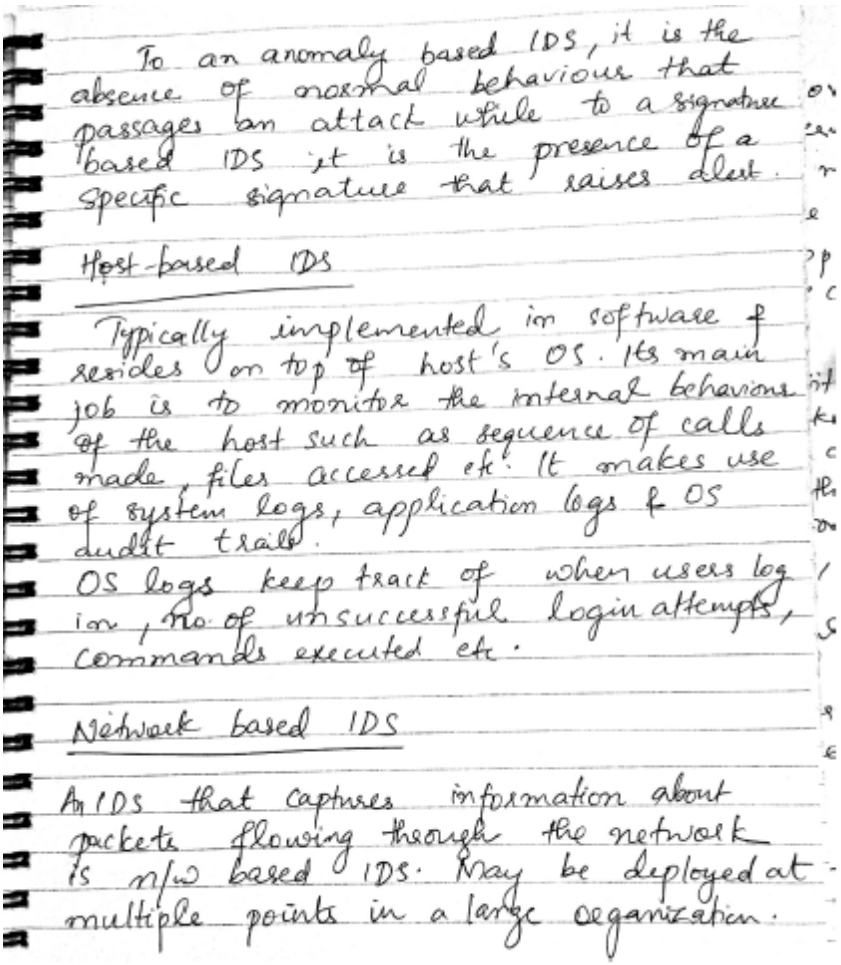
A real-world IDS monitors 100s of variables for interesting patterns.
Some of the variables are bit patterns in the packet header or payload, Some are based on the counts of certain occurrence within a time interval.

Anomaly based IDS

- Involves making a determination whether the behaviour of the system is a statistically significant departure from the normal. The IDS will have to learn, over time, what constitutes normal activity, usage and behaviour.
eg: Consider monitoring the number of TCP SYN packets and FIN packets in each successive 10-second interval. A disproportionate number of SYN packets & FIN packets indicate several half-open TCP connections — SYN flood attack.

Signature based IDS

It works by identifying specific patterns of events or behaviour that accompany an attack. It maintains a database of known signatures. It attempts to obtain a match b/w the currently observed behaviour of the system & an entry in this database.
eg: Specific byte sequence in a worm payload.



To an anomaly based IDS, it is the absence of normal behaviour that passages an attack while to a signature based IDS it is the presence of a specific signature that raises alert.

Host-based IDS

Typically implemented in software & resides on top of host's OS. Its main job is to monitor the internal behaviors of the host such as sequence of calls made, files accessed etc. It makes use of system logs, application logs & OS audit trails.
OS logs keep track of when users log in, no. of unsuccessful login attempts, commands executed etc.

Network based IDS

An IDS that captures information about packets flowing through the network is n/w based IDS. May be deployed at multiple points in a large organization.

5) What is Code Red? Explain the following propagation model of Code Red. i). Simple epidemic Model ii) Kermack- McKendrick model

Code red is an internet worm. The worm spread itself using a common type of vulnerability known as a buffer overflow. It did this by using a long string of the repeated letter 'N' to overflow a buffer, allowing the worm to execute arbitrary code and infect the machine with the worm

19.3.2 Worm Propagation Models

One of the most alarming aspects of some of the worms developed since 2001 is the speed at which they infect their victims. Modelling worm propagation is important for several reasons – it helps us obtain insights into the factors that govern its speed. It also helps in studying the efficacy of different schemes designed to retard the spread of a worm.

The Simple Epidemic Model

The Simple Epidemic Model used to study the spread of infectious diseases among humans is an appropriate starting point. The model assumes that there are only two types of entities in the population. Either an individual is *susceptible* or he is *infected*. An infected individual can infect a susceptible person. Once infected, a person remains infected and does not recover.

Let N be the size of the total population. Let $I(t)$ be the number of infected individuals at time t. The number of susceptibles at time t is then $N - I(t)$. β is the initial infection rate, i.e., each infected person attempts to pass on the infection to β susceptibles in 1 time unit. The following differential equation captures the number of infected persons at time t.

$$dI = \beta I(t)\left(1 - \frac{I(t)}{N}\right)dt \tag{19.1}$$

or

$$\beta\, dt = \left(\frac{dI(t)}{I(t)\left(1 - \frac{I(t)}{N}\right)}\right) \tag{19.2}$$

In an infinite population, each infected person infects $\beta\, dt$ susceptibles in time interval dt. However, in a finite population of size N, the probability that the target of an infective is already infected is $\frac{I(t)}{N}$. Such targets do not add to the population of newly infected. The factor $\left(1 - \frac{I(t)}{N}\right)$ in the above equations ensures that only previously uninfected entities are added to the count of the freshly infected in time interval dt.

Integrating both sides of Eq. (19.2) yields

$$I(t) = \frac{I_0 N}{I_0 + (N - I_0)e^{-\beta t}} \tag{19.3}$$

A number of organizations, research labs, etc. independently monitor incoming packets into their networks (typically Class B or Class C). They reported their observations covering the entire 24-hour period on July 19th, 2001, when Code Red-I (version 2 with the randomly seeded random number generator) was unleashed. Of interest are the *worm scan traffic* (on port 80) and also the number of unique IP addresses from where this traffic emanated.

A crucial observation is that the Simple Epidemic Model is fairly accurate in determining the number of infected machines in the first 15 hours following the outbreak of Code Red-I (Fig. 19.2). Thereafter, the observed data and the model diverge. There are several explanations for this. First, some administrators applied *patches* so that their systems, whether infected or susceptible, ceased

to be either after being patched. Also, the large amount of scan traffic caused congestion on the Internet causing a reduction in infection rate.

Kermack–McKendrick Model

The Kermack–McKendrick (K–M) model more accurately models the spread of human infectious disease by considering three (instead of two) categories of people:

- those who are susceptible (state S)
- those who are infectious (state I) and
- those who are neither, i.e. individuals who are cured or those who have succumbed to the disease (terminal state $\mathcal{T}$)

Initially, all individuals in the population are susceptible. It is possible to go from state S to I but not vice versa. An infectious person may or may not be cured. If cured, however, he is never again vulnerable to the disease (see Fig. 19.3). The transition from states I to $\mathcal{T}$ corresponds to an infected machine being patched. Such a machine is never again vulnerable to a Code Red infection.

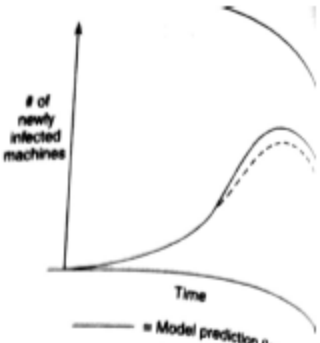


Figure 19.2 *Number of machines infected by Code Red versus time*

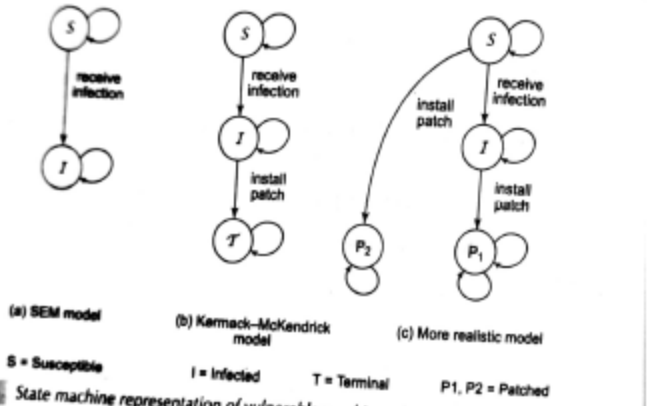


Figure 19.3 *State machine representation of vulnerable machines during a worm epidemic*

As before, let $I(t)$ be the number of infectious machines at time t, let N be the total number of machines, and let β be the infection rate. Let $S(t)$ be the number of susceptibles. So, the number of machines in the terminal state is $N - S(t) - I(t)$. The K–M set of equations is

$$\frac{dS}{dt} = -\beta I(t)\left(\frac{S(t)}{N}\right) \tag{19.4}$$

and

$$\frac{d(N - S(t) - I(t))}{dt} = \gamma I(t) \tag{19.5}$$

Equation 19.4 describes the rate at which the susceptibles decrease (due to the transition to the infectious state). Equation (19.5) captures the rate at which machines in the terminal state increase. Note that the machines in the terminal state are all those that are neither susceptible nor infectious. Analogous to β, γ is the rate at which the infectious machines transit to the terminal state.

While the K–M model better explains the spread of Code Red compared to the Simple Epidemic Model, it still falls short. Its implicit assumptions are at variance with the spread of Internet scanning worms. In particular:

- Machines that are *susceptible but not infectious may also be patched*. Thus, there ought to be a transition from state S to state $\mathcal{T}$. This is not factored into the model.
- The *infection rate*, β, *is network-dependent*. As the worm continues to spread, it will consume network resources such as bandwidth leading to traffic congestion. This in turn will slow down the infection rate. However, both the models considered here assume β to be constant.
- The K–M model assumes that the rate of transitioning from the infectious to the terminal state is a constant, γ. During the early stages of the worm epidemic, not much is known about it. So few machines will be patched. However, once the epidemic sets in and there is more public awareness, more administrators will apply patches. This rate will decrease after most worm-aware administrators have applied their patches. Thus, the rate at which machines are patched, and hence γ, *is far from constant*.

A state diagram of a model that factors the patching of susceptible machines is shown in Fig. 19.3(c).

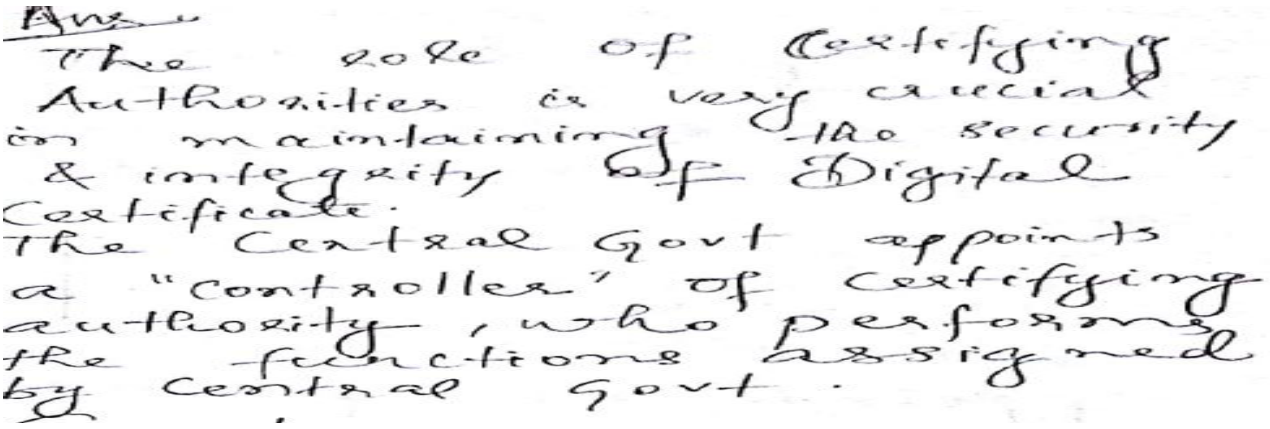
6) Define the following terms under the Information Technology Act, 2000
i) Certifying authority ii). Cyber Appellate Tribunal
iii). Digital Signature iv). Secure System v). Controller

"Certifying Authority" means a person who has been ***granted a license to issue a Digital Signature Certificate*** under section 24;

..'***digital signature"*** means ***authentication of any electronic record*** by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3;

- **Secure System:**
  - ➔Refers to computer hardware, software, and procedure that is reasonably secure from unauthorised access and misuse.
  - ➔Provides a reasonable level of liability and correct operation,
  - ➔Is reasonably suited to performing the intended functions.
  - ➔Adheres to generally accepted security procedure.

Controller:


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.

Cyber Appellate Tribunal (Section 48):

- Establishment of cyber appellate tribunal.
- Composition of cyber appellate tribunal.
- Qualification for appointment as presiding officer of cyber appellate tribunal.
- Term of office.
- Salary, allowances, and other terms and conditions of service of presiding officer.
- Filling up of vacancies.
- Resignation and removal.
- Orders constituting appellate tribunal to be final.
- Staff of the cyber appellate tribunal.
- Appeal to cyber appellate tribunal.
- Procedure and powers of the cyber appellate tribunal.
- Right to legal representation.
- Limitation.
- Civil court not to have jurisdiction.
- Appeal to high court.
- Compounding of contraventions.
- Recovery of penalty.

7) Explain various offences and punishments of cyber crime.

Offences

1. Tampering with computer source documents

- Whoever knowingly or intentionally conceals, destroy or alters or intentionally or knowingly causes another to conceal, destroy any computer source code used for a computer or computer network, shall be punishable with imprisonment up to three years or with a fine up to 2 lakh or with both.

2. **Hacking with computer system**

- if any person dishonestly or fraudulently does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine up to 5 lakh or both.

3. Punishment for receiving stolen computer resources or communication device

- Whoever dishonestly received or retains any stolen computer resource of communication device knowing or having reason to believe the same to be stolen computer resource or communication device, shall be punished with imprisonment for a term which may extend up to 3 years or with fine up to 1 lakh or both.

4. Punishment for identity theft

- Whoever fraudulently or dishonestly make use of electronic signature ,password or unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.

5. Punishment for cheating by personation by using computer resource

- Whoever, by means for any communication device or computer resource cheats by personating, shall be punished with imprisonment of either description for a term which may extend to 3 years and shall also be liable to fine which may extend to 1 lakh rupees.

6. Punishment for violation of privacy

- Whoever, intentionally publishes or transmits the image of a private area of any person without his or her consent, shall be punished with imprisonment which may extend to 3 years or fine not exceeding 2 lakh rupees or both.

7. Punishment for cyber terrorism

- Whoever with intent to threaten the unity, integrity, security of sovereignty of India or any section of the people by- denying or cause the denial of access to any person authorized to access computer resource or attempting to penetrate or access a computer resource without authorization or exceeding authorized access.
- Whoever knowingly or intentionally penetrates or accesses a computer resource without authorization or exceeding authorized access, and by means of such conduct obtains access to information, data or computer database that is restricted.
- Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life.

8. Publishing of information which is obscene in electronic form

- Whoever publishes or transmits or causes to be published in the electronic form any material which is lascivious or appeals to the prurient interest, shall be punished with imprisonment of either description for a term which may extend to five years and with fine which may extend to 1 lakh.

9. Punishment for publishing or transmitting of material containing sexually explicit act in electronic form

- Whoever publishes or transmits or causes to be published in the electronic form any material which contains sexually explicit act or conduct shall be punished with imprisonment of either description for a term which may extend to five years and with fine which may extend to 10 lakh rupees.

10. Power of controller to give directions

- The controller may, by order, direct a CA or any employee of such authority to take such measures or cease carrying on such activities as specified in the order, if those are necessary to ensure compliance with the provisions of this act, rules made thereunder.
- Any person who fails to comply with any order under sub-section 1 shall be guilty of an offence and shall be liable on conviction to imprisonment for a term not exceeding 3 years or to a fine not exceeding 2 lakh or to both.

11. Government agency power to intercept information

- The act empowers the central/ state government authorised agency to intercept, monitor or decrypt any information generated, transmitted or stored in any computer resource if it is deemed fit in the interest of the sovereignty .
- The agency can also secure all the facilities and technical assistance from the subscriber or computer personnel to decrypt the information.
- The subscriber or any person who fails to assist the agency shall be punishable with an imprisonment for a term to 7 years.

12. Protected system

- The appropriate government may, by notification in the official gazette, declare any computer, computer system or computer network to be a protected system.
- The appropriate government may, by order in writing, authorise the persons who are authorised to access protected systems notified under sub-section 1.
- Any person who secures access or attempts to secure access to a protected system in contravention of the provisions of this section shall be punished up to 10 years and shall be liable to fine.

13. Penalty for misrepresentation.

- Whoever makes any misrepresentation to, or suppresses any material fact from, the controller or the CA for obtaining any licence or digital signature certificate, as the case may be, shall be punished up to 2 years or with fine which may extend to 1 lakh or both.

14. Penalty for breach of confidentiality and privacy

- Any person who, in pursuance of any of the powers conferred under this act, rules or regulation made thereunder, has secured access to any electronic record, book, register or other material without the consent of the person concerned, discloses such electronic record or other material to any other person shall be punished up to 2 years of imprisonment or fine with 1 lakh or both.

15. Penalty for publishing digital signature certificate false in certain particulars

- No person shall publish a DSC with the knowledge that the CA listed in the certificate has not issued it or the subscriber listed in the certificate has not accepted it.
- Any person who contravenes the provisions of sub section 1 shall be punished up to 2 years imprisonment or fine with 1 lakh or both.

16. Publication for fraudulent purpose

- Whoever knowingly creates, publishes or otherwise makes available a DSC for any fraudulent shall be punished up to 2 years of imprisonment or fine with 1 lakh or both.

17. Act to apply for offence or contravention committed outside India

- Subject to the provisions of subsection 2, the provisions of this act shall apply also to any offence or contravention committed outside India by any person, irrespective of his nationality.
- Subject to the provisions of subsection 2, the provisions of this act shall apply also to any offence or contravention committed outside India by any person if the act or conduct constituting the offence or contravention involves a computer located in india.

18. Confiscation

- Any computer, computer system, floppies, CD, tape drives or any other accessories related thereto, in respect of which any provision of this act or rules, orders or regulations made thereunder has been or is being contravened shall be liable to confiscation.

19. Penalties or confiscation not to interfere with other punishments

- No penalty imposed or confiscation made under this act shall prevent the imposition of any other punishment to which the person affected thereby is liable under any other law for the time being in force.

20. Power to investigate offences

- Notwithstanding anything contained in the code of criminal procedure 1973, a police officer not below the rank of deputy superintendent of police shall investigate any offence under this act.

8) Describe the duties of Subscribers. Discuss also the penalties and adjudication under section-43 of the IT Act, 2000 for a). damage to a computer/computer systems
b). failure to furnish information, return etc…

Duties of subscribers

1. Generating key pair.

2. Acceptance of digital signature certificate:

- A subscriber shall be deemed to have accepted a DSC if he publishes the publication of a DSC to one or more persons, in a repository.
- By accepting a DSC, the subscriber certifies to all who reasonably rely on the information contained in the DSC that the subscriber holds the pair or all representations made by the subscriber to the CA.

3. Control of private key

- Every subscriber shall exercise reasonable care to retain control of the private key corresponding to the public key listed in his DSC and take all steps to prevent its disclosure to a person not authorised to affix the DS of the subscriber.
- If the private key corresponding to the public key listed in the DSC has been compromised, the subscriber shall communicate this without any delay to the CA in such manner as may be specified by the regulations.

Penalties and adjudication

1. Penalty for damage to computer, computer system.

- If any person without the permission of the owner accesses or secures access to such computer, downloads any data, introduces any computer contaminant or computer virus into any computer, damages any computer, disrupts any computer network, denies access or causes the denial of access to any person authorised to access any computer, provides any assistance to any person to facilitate access to a computer charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, he shall be liable to pay damages by way of compensation not exceeding 1 crore to the person.

2. Compensation for failure to protect data

- If a body corporate handling any sensitive personal data or information in a computer resource which owns is negligent in implementing and maintaining reasonable security practices such body shall be liable to pay damages to the aggrieved party.

3. Penalty for failure to furnish information return

- If any person who is required under this act should furnish any document , return to the controller or the CA fails to furnish the same , he shall be liable to a penalty not exceeding 150000 for each such failure.

4. Residuary penalty

- Whoever contravenes any rules or regulations made under this act, shall be liable to pay a compensation not exceeding 25000 to the person affected by such contravention.

5. Power to adjudicate

6. Factors to be taken into account by the adjudicating officer

- The amount of gain of unfair advantage, wherever quantifiable made as a result of the default.
- The amount of loss caused to any person as a result of the default.
- The repetitive nature of the default.