N.G.M COLLEGE

PG DEPARTMENT OF COMPUTER SCIENCE

SUBJECT TITLE: INFORMATION SECURITY

SUBJECT CODE: 18PCS103

K1 LEVEL QUESTIONS

1._____ at its most fundamental level is random data.

a.Salt

b.password

c.dictonary

d.algortithm

Ans:a

2._____ oftentimes giveaway what is the server is running.

a.Code message

b.Error message

c.code address

d.Error address

Ans:b

3._____ are one of the network admin’s bestfriend and worst headaches.

a.sticky ports

b.ports sticky

c.sticky admin

d.port admin

Ans:a

4.Which best describes how malicious code can get on your computer?

a. Email attachments

b. Downloaded software from non-authoritative sources and websites

c. Sharing diskettes from computers without up to date antivirus software

d. All of the above

Ans:d

5. A way of verifying a message's integrity after transport across a network is through the use of:

a. A Message Authentication Code

b. Steganography

c. An encryption key

d. A cipher

Ans:a

6.Which of the following alert codes is not supported by SSLv3?

a) record_overflow

b) no_certificate

c) internal_error

d) decode_error

Ans:b

7.In TLS padding can be upto a maximum of ____

a) 79 bytes

b) 127 bytes

c) 255 bytes

d) none of the mentioned

Ans:c

8.Which processor speed refers to billions of cycles per second?

a.megahertz

b.gigahertz

c.terahertz

d.petaflops

Ans:b

9. Confidentiality with asymmetric-key cryptosystem has its own

a.Entities

b.Data

c.Problems

d.Translator

Ans:c

10. SHA-l has a message digest of

a.160 bits

b.512 bits

c.628 bits

d.820 bits

Ans:a

11. Message authentication is a service beyond

a.Message Confidentiality

b.Message Integrity

c.Message Splashing

d.Message Sending

Ans:b

12. A hash function guarantees integrity of a message. It guarantees that message has not be

a.Replaced

b.Over view

c.Changed

d.Violated

Ans:c

13. What type of symmetric key algorithm using a streaming cipher to encrypt information?

a.RC4

b. Blowfish

c.SHA

d.MD5

Ans:a

14. What type of attack uses a fraudulent server with a relay address?

a. NTLM

b. MITM

c. NetBIOS

d.SMB

Ans:b

15. Which of the following is independent malicious program that need not any host program?

a.Trap doors

b.Trojan horse

c.Virus

d.Worm

Ans:d

16.Which computer was installed at the U.S Census Bureau in 1951?

a.MARK 1
b.ENIAC
c.UNIVAC
d.UNIVAC1

Ans: c

17. Which company technology have a developed a keyboard made only of light?

a.DELL
b.INTEL
c.CONESTA, INC
d.LOGITECH
Ans: c

18. Which of the following is not a conceptual resource?

a. Data
b. Decisions
c. Information
d. Personnel
Ans: d

19. . _____not an essential ingredient of each value activity?

a. Purchased inputes
b. Human resources
c. Technology
d. Outputs
Ans: d

20. ._____is not an information resources?

a. Information specialists
b. Materials
c. Users
d. Facilities
Ans: b

21. which of the following components does information not flow through?

a. Database
b. Information processor
c. Report writing software
d. Mathematical models
Ans: b

22. The fact that e-mail has provided an entirely new means of communication is referred to as:

a. The transformation factor

b. The invisibility factor

c. Logical malleability

d. The communication factor

Ans:a

23. . _____not an essential ingredient of each value activity?

a. Purchased inputes

b. Human resources

c. Technology

d. Outputs

Ans: d

24. ._____is not an information resources?

a. Information specialists

b. Materials

c. Users

d. Facilities

Ans: b

25. What is the maximum character Linux supports in its filenames?

a. 8

b.128

c. 256

d. Unlimited

Ans:c

26. What are the three types of IS policies?

a. Enterprise Information Security Policy (EISP), Reading Policy, Understanding policy.

b. Managerial guidance, Technical specifications, Documentation.

c. Enterprise Information Security Policy (EISP), Issue-Specific Security Policy (ISSP) and Systems-Specific Policy (SysSP).

d. The Information Security Blueprint, Baselining and Best Business Practices.

Ans: c

27. What are the three types of IS policies?

a. Enterprise Information Security Policy (EISP), Reading Policy, Understanding policy.

b. Managerial guidance, Technical specifications, Documentation.

c. Enterprise Information Security Policy (EISP), Issue-Specific Security Policy (ISSP) and Systems-Specific Policy (SysSP).

d. The Information Security Blueprint, Baselining and Best Business Practices.

Ans: c

28. . What do we call sending data electronically off-site via a remote backup service?

a. Remote journaling.

b. Electronic Vaulting.

c. Data Base Shadowing.

d. Logging.

Ans: b

29. What do we call the off-site that contains all the necessary offices, equipment and data to be used as a business continuity plan?

a. Warm site

b. Hot site

c. Cold site

d. Time share site

Ans: b

30. When do we classify an attack as an incident?

a. The attacks are directed against information assets

b. The attacks have a realistic chance of success

c. The attacks could threaten confidentiality, integrity, or availability of information resources

d. All of the above.

Ans: d

31. multiple layers of Security?

a.Hardware Security

b.Cyber Security

c.Information Security

d.Physical Security

Ans:d

32. characteristics of CIA triangle?

a.Authenticity

b.Confidentiality

c.Integrity

d.Utility

Ans:b

33. . characteristics of Information Security?

a. scability

b.portability

c..Availability

d.estability

Ans:c

34. What are the components of information system?

a.Software

b.Security

c.Scalability

d.utility

Ans:a

35.phases of SDLC Waterfall method?

a..internal Design

b.external design

c.Logical Design

d.networkdesign

Ans:c

36. What type of symmetric key algorithm using a streaming cipher to encrypt information?

a. RC4

b. Blowfish

c. SHA

d. MD5

Ans:a

.

37.Charles Babbage invented

a. ENIAC

b. Difference Engine

c. Electronic Computer

d. Punched Card

Ans:b

38.What type of attack uses a fraudulent server with a relay address?

a. NTLM

b. MITM

c. NetBIOS

d. SMB

Ans:b

39.Which is the maximum character Linux supports in its filenames?

a. 8

b. 128

c. 256

d. Unlimited

Ans:c

40.Which of the following is independent malicious program that need not any host program?

a. Trap doors

b. Trojan horse

c. Virus

d. Worm

Ans:d

41. Workers whose job focus is on the creation, distribution, and use of information are commonly called:

a. Data workers
b. Information workers
c. Knowledge workers
d. Computer workers
Ans: c

42. When businesses move data and information through a communications medium_____.

a. Inter-connectivity

b. Networking

c. Data communication

d. Communication network

Ans : c

43. Find x for the CRT when x= 2 mod 3; x= 3 mod 5; x = 2 mod 7

a) 33

b) 22

c) 23

d) 31

Ans:c

44. Consider a function: f(n) = number of elements in the set {a: 0 <= a < n and gcd(a,n) = 1}. What is this function?

a) Primitive

b) Totient

c) Primality

d) All of the mentioned

Ans:b

45. _____ has been employed as an educational enhancement in Sub-Saharan Africa since the 1960s.

a.ICT

b. OLP

c. OLPC

D. ICTM

Ans: a

Short answers:

45. ICT Development Index

The ICT Development Index ranks and compares the level of ICT use and access the various countries around the world.

46.Data transmission

Data transmission has three aspects: transmission, propagation, and reception.[

47.What's the difference between Symmetric and Asymmetric encryption?

- Symmetric encryption uses the same key to encrypt and decrypt, while Asymmetric uses different keys for encryption and decryption.

48.What is SSL ?

- SSL is identity verification, not hard data encryption.
- It is designed to be able to prove that the person you are talking to on the other end is who they say they are.

49.what is POST code means?

- ✓ POST is one of the best tools available when a system will not boot. Normally through the use of either display LEDs in more modern systems, or traditionally through audio tones, these specific codes can tell you what the system doesn't like about its current setup.

50.What is the CIA triangle?

- ➢ Confidentiality, Integrity, Availability. As close to a 'code' for Information Security as it is possible to get, it is the boiled down essence of InfoSec

N.G.M COLLEGE

PG DEPARTMENT OF COMPUTER SCIENCE

SUBJECT TITLE: INFORMATION SECURITY

SUBJECT CODE: 18PCS103

K2 LEVEL QUESTIONS

Unit-1

1. **What is the difference between encryption and hashing?**
   Point 1: Encryption is reversible whereas hashing is irreversible. Hashing can be cracked using rainbow tables and collision attacks but is not reversible.
   Point 2: Encryption ensures confidentiality whereas hashing ensures Integrity.

2. **What is the difference between Asymmetric and Symmetric encryption and which one is better?**
   Symmetric encryption uses the same key for both encryption and decryption, while Asymmetric encryption uses different keys for encryption and decryption.
   Symmetric is usually much faster but the key needs to be transferred over an unencrypted channel. Asymmetric on the other hand is more secure but slow. Hence, a hybrid approach should be preferred. Setting up a channel using asymmetric encryption and then sending the data using symmetric process.

3. **Explain risk, vulnerability and threat?**
   Back this up with an easy to understand example.
   Vulnerability (weakness) is a gap in the protection efforts of a system, a threat is an attacker who exploits that weakness. Risk is the measure of potential loss when that the vulnerability is exploited by the threat e.g. Default username and password for a server – An attacker can easily crack into this server and compromise it.

4. **Are you a coder/developer or know any coding languages?**
   Although this is not something an information security guy is expected to know but the knowledge of HTML, JavaScript and Python can be of great advantage. HTML and JavaScript can be used in web application attacks whereas python can be used to automate tasks, exploit development etc. A little knowledge of the three can be of great advantage - both in the interview and on the floor.

5. **What is a Security Misconfiguration?**
   Security misconfiguration is a vulnerability when a device/application/network is configured in a way which can be exploited by an attacker to take advantage of it.

This can be as simple as leaving the default username/password unchanged or too simple for device accounts etc.

6. **What is a Black hat, white hat and Grey hat hacker?**
   Black hat hackers are those who hack without authority. White hat hackers are authorised to perform a hacking attempt under signed NDA. Grey hat hackers are white hat hackers which sometimes perform unauthorised activities.

7. **What is a firewall?**
   A firewall is a device that allows/blocks traffic as per defined set of rules. These are placed on the boundary of trusted and untrusted networks.

8. **What is port scanning?**
   Port scanning is process of sending messages in order to gather information about network, system etc. by analysing the response received.

9. **How do you handle AntiVirus alerts?**
   Check the policy for the AV and then the alert. If the alert is for a legitimate file then it can be whitelisted and if this is malicious file then it can be quarantined/deleted. The hash of the file can be checked for reputation on various websites like virustotal, malwares.com etc. AV needs to be fine-tuned so that the alerts can be reduced.

10. **Software testing vs. penetration testing?**
    Software testing just focuses on the functionality of the software and not the security aspect. A penetration testing will help identify and address the security vulnerabilities.

Unit-2

11. **What is data leakage? How will you detect and prevent it?**
    Data leak is when data gets out of the organisation in an unauthorised way. Data can get leaked through various ways – emails, prints, laptops getting lost, unauthorised upload of data to public portals, removable drives, photographs etc. There are various controls which can be placed to ensure that the data does not get leaked, a few controls can be restricting upload on internet websites, following an internal encryption solution, restricting the mails to internal network, restriction on printing confidential data etc.

12. **What are the different levels of data classification and why are they required?**
    Data needs to be segregated into various categories so that its severity can be defined, without this segregation a piece of information can be critical for one but not so

critical for others. There can be various levels of data classification depending on organisation to organisation, in broader terms data can be classified into:
Top secret – Its leakage can cause drastic effect to the organisation, e.g. trade secrets etc.
Confidential – Internal to the company e.g. policy and processes.
Public – Publically available, like newsletters etc.

13. **In a situation where a user needs admin rights on his system to do daily tasks, what should be done – should admin access be granted or restricted?**
    Users are usually not provided with admin access to reduce the risk, but in certain cases the users can be granted admin access. Just ensure that the users understand their responsibility. In case any incident happens, the access should be provided for only limited time post senior management approval and a valid business justification.

14. **What is the difference between data, information, and knowledge?**
    a. Data are the raw bits and pieces of facts and statistics with no context. Data can be quantitative or qualitative. Information is data that has been given context. Knowledge is information that has been aggregated and analyzed and can be used for making decisions.

15. **Explain in your own words how the data component relates to the hardware and software components of information systems.**
    a. There are numerous answers to this question, but all should be variations onthe following: Data is processed by the hardware via software. A database is software that runs on the hardware. Hardware stores the data, software processes the data.

16. **What is the difference between quantitative data and qualitative data? In what situations could the number 42 be considered qualitative data?**
    Quantitative data is numeric, the result of a measurement, count, or some other mathematical calculation. Qualitative data is descriptive. The number 42 could be qualitative if it is a designation instead of a measurement, count, or calculation. For example: that player's jersey has number 42 on it.

17. **What were the first four locations hooked up to the Internet (ARPANET)?**
    UCLA, Stanford, MIT, and the University of Utah

18. **What does the term packet mean?**
    The fundamental unit of data transmitted over the Internet. Each packet has the sender's address, the destination address, a sequence number, and a piece of the overall message to be sent.

19. **What was revolutionary about Web 2.0?**

Anyone could post content to the web, without the need for understanding HTML or web-server technology.

20. What makes a connection a broadband connection?

A broadband connection is defined as one that has speeds of at least 256,000 bps.

Unit-3

21. What is the difference between an intranet and an extranet?

An intranet consists of the set of web pages and resources available on a company's internal network. These items are not available to those outside of the company. An extranet is a part of the company's network that is made available securely to those outside of the company. Extranets can be used to allow customers to log in and check the status of their orders, or for suppliers to check their customers' inventory levels.

22. Briefly define each of the three members of the information security triad.

The three members are as follows:

i. Confidentiality: we want to be able to restrict access to those who are allowed to see given information.

ii. Integrity: the assurance that the information being accessed has not been altered and truly represents what is intended.

iii. Availability: information can be accessed and modified by anyone authorized to do so in an appropriate timeframe.

23. What does the term authentication mean?

The process of ensuring that a person is who he or she claims to be.

24. What is multi-factor authentication?

The use of more than one method of authentication. The methods are: something you know, something you have, and something you are.

25. What is role-based access control?

With role-based access control (RBAC), instead of giving specific users access rights to an information resource, users are assigned to roles and then those roles are assigned the access.

26. What is the purpose of encryption?

To keep transmitted data secret so that only those with the proper key can read it.

27. What are two good examples of a complex password?

There are many examples of this. Students need to provide examples of passwords that are a minimum of eight characters, with at least one upper-case letter, one special character, and one number.

28. What is pretexting?

Pretexting occurs when an attacker calls a helpdesk or security administrator and pretends to be a particular authorized user having trouble logging in. Then, by providing some personal information about the authorized user, the attackerconvinces the security person to reset the password and tell him what it is.

29. What are the components of a good backup plan?

Knowing what needs to be backed up, regular backups of all data, offsite storage of all backed-up data, and a test of the restoration process.

30. What is a firewall?

A firewall can be either a hardware firewall or a software firewall. A hardware firewall is a device that is connected to the network and filters the packets based on a set of rules. A software firewall runs on the operating system and intercepts packets as they arrive to a computer.

Unit-4

31. What does the term physical security mean?

Physical security is the protection of the actual hardware and networking components that store and transmit information resources.

32. Being a professional, what is more important Threats or Vulnerabilities?

Despite the advancements in the security systems with the years, the threats and vulnerabilities have only increased with each passing day. Assessing threats is still not under the control of any high-tech security team. Although, a threat rises from vulnerability, so if we have proper control over them, we can still try and control threats. Secondly, the type of threats remains same but the vulnerabilities are what keep on changing. Thus we need to focus on building something that has a proper defence mechanism and also can track down new vulnerabilities.

33. What is the main point of consideration when it comes to the differences between the Stored XXS and the Reflected XXS?

In case of Stored XXS, since Stored XXS is stored in a page which is static, thus, it is directly pulled out and displayed to the user directly as per needed. On the other hand, in Reflected XXS, the user has to send a request first. Now, this request will start running on the browser of the victim's computer and then will reflect the results back from the website or the browser to the user who has sent the request.

34. How does the HTTP control the State?

This is a tricky question. HTTP doesn't and will never control the state. Answers like cookies are still better. The job of the cookies is to provide a gateway to what HTTP can't do. In simpler terms, cookies serve as a hack to what HTTP fails to do.

35. Describe the 3 major first steps for securing your Linux server.

Every system has its own security software's so for securing your Linux, the first three steps are:

1. Auditing: A system scan is performed using a tool called Lynis for auditing. Every category is scanned separately and the hardening index is provided to the auditor for further steps.

2. Hardening: After the audit is complete, the system is hardened depending on the level of security it further needs. It is an important process based on the decision of auditor.

3. Compliance: The system needs to be checked almost every day for better results and also lesser threats from security point of view.

36. What are the techniques used in preventing a brute force login attack?

To avoid brute force login attacks, you generally have three kinds of techniques to go about. The first technique is to implement a policy for account lockout. In this method, an account will be locked out unless and until the administrator himself opens it. The second being progressive delays. In this method, after a few attempts of login, your account will stay locked for the next few number of days. Lastly, use a challenge-response test. This prevents any kind of automatic submissions on the login page.

37. How can you defend yourself against CSRF attacks?

To defend yourself against CSRF attacks, you can opt for two available methods. Firstly, with every request try to include a random token. In this way a unique string of tokens will be generated which is a good safeguard. Secondly, for each field of form, try using different names. This will somewhat help you in becoming anonymous due to the entry of so many different names and thus will behave as a safeguard from CSRF attacks.

38. What is the need for DNS monitoring?

The Domain Name System allots your website under a certain domain that is easily recognizable and also keeps the information about other domain names. It works like a directory for everything on the internet. Thus, DNS monitoring is very important since you can easily visit a website without actually having to memorise their IP address.

39. Define the process of Salting and state the use of Salting.

Salting is that process where you extend the length of your passwords by using some special characters. In order to use salting, you must know the entire mechanism of

salting and also, it is not that very difficult to be cracked by a person who already knows the concept of salting.

The use of salting is to make your passwords stronger and not easy to be cracked if you are someone who is prone to use of simple or ordinary words as passwords.

40. State the difference between Symmetric Key Cryptography and Public Key Cryptography.

Both of these cryptography, that is, the Symmetric Key Cryptography and the Public Key Cryptography, does the same job of encrypting and decrypting, thereby, here lies the main difference between them. Thus, the main difference between them is that in Symmetric Key Cryptography, only one key is put into use for encryption and decryption. On the other hand, in the case of Public Key Cryptography, they make use of two different keys. The public key for encryption and the private key for decryption. Generally, the Symmetric Key Cryptography is known to be faster and simpler.

Unit-5

41. How will you prevent the "Man-in-the-Middle" attack?

Commonly known as the "Bucket Brigade Attack", this attack happens through a man who is in between two different parties and controls the complete conversation without the two ends even realising that. The first method to prevent this attack would be to have an end to end encryption between both the parties. This way, they both will have an idea with whom they are talking because of the digital verification. Secondly, to prevent this, it is best to avoid open Wi-Fi networks and if it is necessary then use plugins like HTTPS, Forced TLS etc.

42. How encoding, hashing and encryption differs from one another.

1. Encoding: Encoding converts the data in a desired format required for exchange between different systems. This doesn't convert it into a secret data, but usable data. It can be further decoded through the same tools when necessary.

2. Hashing: This serves for maintaining the integrity of a message or data. This way if any day it is hampered or changed, you will get to know.

3. Encryption: Encryption ensures that the data is secure and one needs a digital verification code or image in order to open or access it.

43. SSL and HTTPS: Which is more secure?

SSL (Secure Sockets Layer) is a protocol which enables safe conversations between two or more parties over the internet. HTTPS (Hypertext Transfer Protocol Secure) is HTTP combined with SSL which provides you with a safer browsing experience with encryption. So, this is a very tricky question but SSL wins in terms of security.

44. In encryption and compression of data during transmission, which of them would you do first? Justify with proper reasons.

If I had the option to encrypt and compress data, I would first compress the data. This is because of encrypting a data we obtain a stream of bits which are random. Now, these random bits become impossible to be compressed, in other words, they are incompressible. The reason to why these random bits become incompressible is because of the lack of any patterned structure. Compressing data always requires any specific pattern to be compressed which is lacked in random bits.

45. Which is more secure? An open source project or a proprietary project?

The securities of these projects depends mainly on the size of the project, the total number of the developers who are working under this project and the one factor, which is most essential as well as important, is the control of the quality. Just the type of project won't determine its quality, the inside matter of the corresponding projects will matter.

46. How do you acquire the Cyber security related news?

There are several places from where one might get the best cybersecurity news from but it is important to remember not all of it is correct and precise. So, for the best news related to cyber security you can go for Reddit, Team Cymru, Twitter etc. You have to be on top of the news count so that you don't wait for one to inform you about the recent changes.

47. State the difference between Diffie-Hellman and RSA.

The basic difference which lies in both of these is the type of protocol they are. RSA is a protocol which is used for signing or encryption. On the other hand, Diffie-Hellman is a protocol which is used for exchange of key. Also, the RSA will expect that you have all the key materials with you beforehand, which is not the case with Diffie-Hellman.

48. How to access Active directory from Linux?

It is quite surprising but you can use Active directory from Linux or iOS system or any other system apart from windows. The directory makes use of the SMB protocol which further can be accessed from a non-windows platform with the help of the Samba program.

49. Why is using SSH from Windows better?

SSH is a connection used on different platforms on appliances for the best security. This hardens your security system against any threat and works well with Routers, SFTP and switches. It works the best with Windows although is compatible with other platforms too.

50. How can you make the user authentication process more secure?

User authentication may sound very secure but it is not so secure. You need just the username and password to break into or hack into the authentication of that person. The main way of hardening is by choosing the password accordingly. You can either generate memorable passwords which are secure, passwords based on algorithm, making the use of password vaults, using authentications which are multifactor and highly secure and alternate embedding of the alphabets of a specific memorable word, are the best ways of hardening user authentication.

Department of Computer Science(S.F)
I-M.Sc.Computer Science – Question Bank – K3 level
18PCS103 – INFORMATION SECURITY

Unit- I

1.Examine the concept of E-Commerce.

2.Categorize the models of E-commerce.

3.List out the features of Business models.

4.Elucidate the key concept of revenue models.

5.List out the key notes of Business processed.

6.Examine the salient features of Economic forces and

Ecommerce.

7.List out the differences between Internet and world wide

web.

8. Discuss about Packet-Switched Networks.

9.Describe about Markup languages and the web.

10.Analyse about Internet connection options.

11.Elucidate the basic concepts of Internet2.

Unit-II

1.List out the features of E-marketing.

2.Mention the concepts of online marketing.

3.Examine the features of E-Advertising.

4.Elucidate the key concepts of E-branding.

5.List out the major issues on E-security.

6.Analyseabout information system security.

7.Concludeabout security on the internet.

8.DiscoverE-payment systems and its featuress.

9.Simplifythe classification of new E-payment systems.

10.Examine the concept of cheque payment systems on the internet.

Unit-III

1.Examine the elementsfor changing the technology.

2.Concludethe importance of knowledge management.

3.Analyse the various stages of Knowledge management.

4.Describe the seven dimensions of E-strategy .

5.Examine the concept of value chain and E-strategy.

6.Concludesecurity issues pertaining to cellular technology.

7.Examine the features of M-commerce.

8.Inspect the impact of M-commerce in India.

9.Compare and contrast E-Commerce and M-commerce.

10.Elucidate the impact of E-strategy over E-commerce.

Unit-IV

1.Examine the features of Kerberos.

2.Examine the features of X-509 authentication services.

3.ConcludeAuthentication applications.

4.Concludeabout Pretty Good Privacy.

5.Distinguish between Kerberos and X.509 certificates.

6.Analysethe key features ofS/MIME.

7.Compare and contrast Kerberos and S/MIME.

8.Inspect the role of IP security and E-Commerce.

9. Elucidate about IP security.

10.Discuss about authentication services.

Unit-V

1.Analyse the key features of Malicious software.

2.List out the major issues on Viruses and related threats.

3.Discuss about Virus counter measures.

4.Conclude about Distributed denial of service attacks .

5.Discuss about firewalls.

6.Conclude about firewall design principles.

7.Describe about trusted systems.

8.Explain about web security considerations.

9.Examine the features of secure socket layer.

10.Elucidate about transport layer security .

11.Analyse about Secure electronic transaction.

****

Department of Computer Science(S.F)
I-M.Sc.Computer Science – Question Bank – K4 & K5 level
18PCS103 – INFORMATION SECURITY

Unit- I

1.Discuss about identifying E-commerce opportunities.

2.List out the models of E-commerce.

3.Explain the international nature of E-commerces.

4.Explain the features of Internet protocols.

5.List out the salient features of Intranets and Extranets.

6.Explain about Internet2 and the Semantic web.

Unit-II

1.Explain about Digital tokens based on E-payment systems.

2.Mention the features of Customer relationship management.

3.Explainabout typical business touch points.

4.Explain about smart chains and smarter gains.

5.Explain in brief about E-supply chain components.

6.Elaborate about E-supply chain architecture.

Unit-III

1.Examine the technologies of E-commerce.

2.Explain the concept of WAP programming model.

3.Explainabout wireless technologies.

4.Discuss about the different generations in wireless communications.

5.Discuss about M-Commerce in India.

Unit-IV

1.Examine the features of Kerberos with neat sketch.

2.Distinguish between Kerberos and X.509 certificates.

3.Explain about X.509 certificates.

4.Discuss about Pretty Good Privacy.

5.Explain aboutS/MIME.

6.List out the key notes of IP Securtiy.

Unit-V

1.Explain the concept of malicious software.

2.List out the various viruses and its related threats.

3.Explain about distributed denial of service attacks .

4.Discuss about firewalls and its design principles.

5.Explain about secure electronic transaction.

****