BHARTIYA SKILL DEVELOPMENT UNIVERSITY

Registration No.: .....

Set – A

School of Computing Skills

Session: 2022-23 (Winter Semester)

B. Voc. Program, 3rd Semester,

End-Sem. Examination

Course Code: ITN1302 **Time: 2 Hour**

Course Name: Wireless Networks **Max. Marks: 50**

Section – A

10X01 = 10 Marks

Q1. GSM is a secure _____ system.

(a) Wired

(b) Wireless

(c) Simple

(d) Complex

Q2. SIM in the GSM network stands for _____.

(a) Subscriber Identity Module

(b) Subscriber Investigation Mobile

(c) Subscriber Identification Mobile

(d) Smart Identification Module

Q3. _____ used by the service providers of telecommunications to manage networks.

(a) Base Station Subsystem

(b) Network Switching Subsystem

(c) GPRS Core Network

(d) Operations Support System (OSS)

Q4. GSM offers services like _____.

(a) voice

(b) Data

(c) Roaming

(d) All the above

Q5 The permanent data of the subscriber is stored in _____.

(a) Home Location Register (HLR)

(b) Visitor Location Register (VLR)

(c) Authentication Center (AUC)

(d) Equipment Identity Register (EIR)

Q6. In wireless ad-hoc network _____

(a) access point is not required

(b) access point is must

(c) nodes are not required

(d) all nodes are access points

Q7. In wireless distribution system _____

(a) multiple access point are inter-connected with each other

(b) there is no access point

(c) only one access point exists

(d) access points are not required

Q8. In wireless network an extended service set is a set of _____

(a) connected basic service sets

(b) all stations

(c) all access points

(d) connected access points

Q9. The frequency band of Bluetooth radio is around _____

(a) 2.1 GHz

(b) 2.3 GHz

(c) 2.4 GHz

(d) None of the above

Q10. The single piconet formed by _____

(a) One slave and one master

(b) One slave and multiple masters

(c) Multiple slaves and one master

(d) Multiple slaves and multiple masters

Section – B

04X04 = 16 Marks

Q1. What is a wireless LAN?

Q2. What is an access point?

Q3. What are IBSS and BSS in WLAN?

Q4. Do I Need a License to Operate WLANs?

Section – C

04X06 = 24 Marks

Q1. Calculate the link margin for link with following parameters. 20 dBm(Tx Power), + 10 dBi (Tx Antenna Gain), - 2 dB (Tx Cable Losses), -114 dB (free space loss @5 km), + 14 dBi (Rx Antenna Gain), - 2 dB (Rx Cable Losses, -74 dBm (expected received signal level) , -(-82 dBm) (sensitivity of Rx).

Q2. Explain the difference between TDMA, FDMA and CDMA? Which of these are used in GSM networks?

Q3. What is the difference between WiFi and Bluetooth?

Q4. What are three different type of satellites based on their orbit? Also mention their orbit heights.

Set – A

Bhartiya Skill Development University

School of Computing Skills

Session: 2022 (Winter Semester)

B. Voc. Program, 3rd Semester,

End-Sem. Examination

Course Code: ITN1302 **Time: 2 Hour**

Course Name: Wireless Networks **Max. Marks: 50**

Section – A

Answers

Q1. B

Q2. A

Q3. D

Q4. D

Q5. A

Q6. A

Q7. A

Q8. A

Q9. C

Q10. A

Section – B

Ans1. A WLAN is a type of Local Area Network (LAN) that uses high frequency radio waves rather than wires to communicate and transmit data. It is a flexible data communication system implemented as an extension to or as an alternative for, a wired LAN.

Ans2. An access point connects wired and wireless networks together and enables the sending and receiving of data between wireless clients and the wired network. Using multiple access points increases total system capacity and range. Users can "roam" between access points without losing their connection similar to the way a cellular phone can roam between cellular phone towers.

Ans3. Independent Basic Service Set (IBSS) allows two or more devices to communicate directly with each other without a need for a central device.Basic Service Set (BSS) wireless LAN is established using a central device called an Access Point that centralizes access and control over a group of wireless devices.

Ans4. WLAN equipment operates in a 2.4 GHz and 5 GHz frequency spectrum which are license free in India. We do not need any license to operate a WLAN in these two frequency bands.

Section – C

Ans1. 8 db.

Ans2. TDMA, FDMA and CDMA are access techniques to utilize time, frequency and code respectively. TDMA means Time Division Multiple Access, FDMA means Frequency Division Multiple Access and CDMA means Code Division Multiple Access. GSM uses both TDMA and FDMA. FDMA and TDMA are used in GSM Networks.

Ans3. WiFi fall under WLAN category while Bluetooth fall under WPAN category. WLAN specifications are published under IEEE 802.11 and Bluetooth under IEEE 802.15 standards. Bluetooth is the standard for wireless personal area networks or WPAN. It allows high speed transmission of data over very short distances. WiFi covers more distance then Bluetooth.

Ans4. There are essentially three types of Earth orbits: high Earth orbit, medium Earth orbit, and low Earth orbit. Many weather and some communications satellites tend to have a high Earth orbit, farthest away from the surface. Satellites that orbit in a medium (mid) Earth orbit include navigation and specialty satellites, designed to monitor a particular region. Most scientific satellites, including NASA's Earth Observing System fleet, have a low Earth orbit.

When a satellite reaches exactly 42,164 kilometers from the center of the Earth (about 36,000 kilometers from Earth's surface), it enters a sort of "sweet spot" in which its orbit matches Earth's rotation.

Medium Earth Orbit

Closer to the Earth, satellites in a medium Earth orbit move more quickly. Two medium Earth orbits are notable: the semi-synchronous orbit and the Molniya orbit.

The semi-synchronous orbit is a near-circular orbit (low eccentricity) 26,560 kilometers from the center of the Earth (about 20,200 kilometers above the surface).

Less than 1000KM is the LEO.

BHARTIYA SKILL DEVELOPMENT UNIVERSITY

Registration No.: .....

Set – B

School of Computing Skills

Session: 2022-23 (Winter Semester)

B. Voc. Program, 3rd Semester,

End-Sem. Examination

Course Code: ITN1302 **Time: 2 Hour**

Course Name: Wireless Networks **Max. Marks: 50**

Section – A

10X01 = 10 Marks

Q1. Which of the following is the world's first cellular system to specify digital modulation and network level architecture?

a) GSM

b) AMPS

c) CDMA

d) IS-54

Q2. Which of the following memory device stores information such as subscriber's identification number in GSM?

a) HLR

b) VLR

c) SIM

d) SMS

Q3. Which of the following does not come under the subsystem of GSM architecture?

a) BSS

b) NSS

c) OSS

d) Channel

Q4. Which of the following subsystems provides radio transmission between mobile stations and MSC?

a) BSS

b) NSS

c) OSS

d) BTS

Q5. SIM in the GSM network stands for _____.

a) Subscriber Identity Module

b) Subscriber Investigation Mobile

c) Subscriber Identification Mobile

d) Smart Identification Module

Q6. The transmitter-receiver combination in the satellite is known as a _____

a) Relay

b) Repeater

c) Transponder

d) Duplexer

Q7. Which multiple access technique is used by IEEE 802.11 standard for wireless LAN?

a) CDMA

b) CSMA/CA

c) ALOHA

d) CSMA/CD

Q8. A Bluetooth network is called ----------.

a) piconet

b) scatternet

c) bluenet

d) none of the above

Q9. An interconnected collection of piconet is called _____

a) scatternet

b) micronet

c) mininet

d) multinet

Q10. Bluetooth is the wireless technology for _____

a) local area network

b) personal area network

c) metropolitan area network

d) wide area network

Section – B

04X04 = 16 Marks

Q1. How do we increase the capacity (when subscribers increase) in GSM networks?

Q2. What Is IMEI in GSM Technology?

Q3. What Are the Services Offered by GSM Technology?

Q4. Name few applications of Bluetooth?

Section – C

04X06 = 24 Marks

Q1. What is the difference between GEO MEO and LEO satellites?

Q2. Explain the difference between IBSS, BSS and ESS.

Q3. What is the difference between Wi-Fi and Bluetooth?

Q4. Calculate the link margin for link with following parameters.
22 dBm(Tx Power), + 11 dBi (Tx Antenna Gain), - 3 dB (Tx Cable Losses), -114 dB (free space loss @5 km), + 14 dBi (Rx Antenna Gain), - 3 dB (Rx Cable Losses, -74 dBm (expected received signal level) , -(-82 dBm) (sensitivity of Rx).

BHARTIYA SKILL DEVELOPMENT UNIVERSITY

Answer Key

Set – B

School of Computing Skills

Session: 2021-22 (Winter Semester)

B. Voc. Program, 3rd Semester,

End-Sem. Examination

Course Code: ITN1302 **Time: 2 Hour**

Course Name: Wireless Networks **Max. Marks: 50**

Section – A

Answers

Q1. A

Q2. C

Q3. D

Q4. A

Q5. A

Q6. C

Q7. B

Q8. A

Q9. A

Q10. B

Section – B

Ans1. **Cell splitting** is the process of subdividing a congested cell into smaller cells, each with its own base station and a corresponding reduction in antenna height and transmitter power. Cell splitting increases the capacity of a cellular system since it increases the number of times that channels are reused. Another way to increase the capacity is sectorisation. In this method the radius of the cell remains same bot instead of three sectors we increase the number to 6. This will double the capacity of the cell.

Ans2. International Mobile Equipment Identity is a number usually unique for identifying GSM,WCDMA and iDEN mobile phones.

•It is generally printed inside the battery compartment of the phone.

•The number can be displayed on the screen by entering *#06# into the keypad on most of the phones.

•A stolen phone can be stopped from accessing the network within the country, by using IMEI number for valid devices.

•Unlike CDMA/MEID's electronic serial number, the IMEI is only used for identifying the

device and has no permanent relation to the subscriber

•The subscriber is identified by IMSI number, stored on the SIM card, which then can be transferred to any other handset.

Ans3. The services offered by GSM are ISDN compatible

•GSM allows synchronous data and asynchronous data to be transported as bearer service, one of the telecommunication services offered by GSM, and forms ISDN terminal

•The data could be either transparent service or nontransparent service

•Telephony is one of the services offered by GSM, which an emergency and the service provider is notified by dialing 3 digits

•By using appropriate fax adapter, G3 fax service is supported

•One of the features of GSM is Short Messaging Service

•Certain services, namely supplementary services are provided on top of tele services or bearer services by GSM, such as, caller identification, call forwarding, multiparty conversations, barring outgoing calls and call waiting.

Ans4.

- Wireless control of and communication between a cell phone and a hands free headset or car kit. This is the most popular use.
- Wireless networking between PCs in a confined space and where little bandwidth is required.
- Wireless communications with PC input devices such as mouse and keyboards and output devices such as printers.
- Transfer of files between devices via OBEX.
- Transfer of contact details, calendar appointments, and reminders between devices via OBEX.
- Replacement of traditional wired serial communications in test equipment, GPS receivers and medical equipment.
- For remote controls where infrared was traditionally used.
- Sending small advertisements from Bluetooth enabled advertising hoardings to other, discoverable, Bluetooth devices.
- Wireless control of a games console, Nintendo's Wii and Sony's PlayStation 3 will both use Bluetooth technology for their wireless controllers.
- Sending commands and software to the upcoming LEGO Mindstorms NXT instead of infra-red.

BHARTIYA SKILL DEVELOPMENT UNIVERSITY

Section – C

Ans1. There are essentially three types of Earth orbits: high Earth orbit, medium Earth orbit, and low Earth orbit. LEO satellites orbit at an altitude below 2,000km/1,243 miles above mean sea level, while MEO satellites orbit in the region between LEO and GEO (geostationary) satellites – 2,000-35,800km/1,243-22,245 miles. When a satellite reaches exactly 42,164 kilometers from the center of the Earth (about 36,000 kilometers from Earth's surface), it enters a sort of "sweet spot" in which its orbit matches Earth's rotation.

Ans2. BSS stands for Basic Service Set — these are the stations that can communicate with each other at the physical layer (PHY) of the OSI model. Every BSS is identified with a BSSID, which is the MAC address of the Wi-Fi chipset that runs on a Wireless Access Point (WAP) servicing the BSS. IBSS, which stands for Independent BSS (IBSS), is a type of ad-hoc BSS that can't connect to any other basic service set since it contains no access points. This means it cannot connect to any other basic service set. ESS stands for Extended Service Set. An ESS contains several connected Basic Service Sets whose access points (APs) are connected by a distribution system.

Ans3. Wi-Fi fall under WLAN category while Bluetooth fall under WPAN category. WLAN specifications are published under IEEE 802.11 and Bluetooth under IEEE 802.15 standards. Bluetooth is the standard for wireless personal area networks or WPAN. It allows high speed transmission of data over very short distances. Wi-Fi covers more distance then Bluetooth.

Ans4. 9 db.

BHARTIYA SKILL DEVELOPMENT UNIVERSITY

Registration No.: ..... Name - .....

School of Computing Skills

SET-A

B.Voc Program, III Semester (2022)

End-Sem. Examination

Course Code : ITN1303

Course Name : Basic of Network Security **Time: 2 hour**

Instruction: Explain in detail for long answer **Max. Marks : 50**

Section-A

10X1= 10 Marks

Q.1 What is plain text in cryptography .

a) simple text
b) encrypted text
c) Cipher text
d) none of above

Q.2 What is cipher test .

a) encryption text
b) Plain Text
c) algorithm
d) None of above

Q.3 What is the software called which when get downloaded on computer scans your hard drive for personal information and your internet browsing habits.

a) Backdoors
b) Key-logger
c) Malware
d) Antiware
e) Spyware

Q.4 Full form of DOS

a) Denial of service
b) Data of service
c) Denial of system
d) None of above

Q.5 Which one is not a computer virus .....

a) Avast
b) Trojan horse
c) Logic bomb
d) Spyware

Q.6 Which is a network scanning tool .....

a) Nmap
b) Zenmap
c) Wireshark

d) All of above

Q.7 Which one is DOS attack tool .....

a) LOIC
b) Brute force
c) NmaP
d) Smap

Q.8 What is full form of CAPTCHA.

a) Completely Automated Public Turing test to tell Computers and Humans Apart
b) Company Automated Public Turing test to tell Computers and Humans Apart
c) Computer Automated Public Turing test to tell Computers and Humans Apart
d) Cryptograpghy Automated Public Turing test to tell Computers and Humans Apart

Q.9 Full form of DDOS

a) Denial of Service
b) Distributed Denial of service
c) Danger Denial of service
d) Distributed Denial of system .

Q.10 What is MITM .

a) Man in the middle attack
b) Master in the middle attack
c) More in the middle attack
d) Measure in the middle attack

Section B

04X04= 16 Marks

Q.1 Explain cryptography and steganography.

Q.2 What is RSA algorithm.

Q.3. Difference between symmetric and asymmetric key encryption.

Q.4 Explain digital signature.

Section C

04X06=24 Marks

Q.1 Explain any 4 Software vulnerability.

Q.2 Explain any 4 Hardware vulnerability.

Q.3 Explain any 4 Firmware vulnerability.

Q.4 Explain why Network Policy is important for any of the company.

Registration No.: ..... Name - .....

School of Computing Skills

B.Voc Program, III Semester (2022)

End-Sem. Examination

Course Code : ITN1303

Course Name : Basic of Network Security **Time: 2 hour**

Instruction: Explain in detail for long answer **Max. Marks : 50**

ANSWER SHEET

Section-A

1X10 = 10 Marks

Q.1 A

Q.2 A

Q.3 E

Q.4 A

Q.5 A

Q.6 A

Q.7 A

Q.8 A

Q.9 A

Q.10 A

Section – B

Answer 1 : Cryptography is a method of protecting information and communications through the use of codes, so that only those for whom the information is intended can read and process it.

Steganography is the practice of concealing a message within another message or a physical object

Answer 2: RSA algorithm is asymmetric cryptography algorithm. Asymmetric actually means that it works on two different keys i.e. **Public Key** and **Private Key.** As the name describes that the Public Key is given to everyone and Private key is kept private.

An example of asymmetric cryptography :

1. A client (for example browser) sends its public key to the server and requests for some data.
2. The server encrypts the data using client's public key and sends the encrypted data.
3. Client receives this data and decrypts it.

Answer 3 :

Key Differences	Symmetric Encryption	Asymmetric Encryption
Size of cipher text	Smaller cipher text compares to original plain text file.	Larger cipher text compares to original plain text file.
Data size	Used to transmit big data.	Used to transmit small data.
Resource Utilization	Symmetric key encryption works on low usage of resources.	Asymmetric encryption requires high consumption of resources.
Key Lengths	128 or 256-bit key size.	RSA 2048-bit or higher key size.
Security	Less secured due to use a single key for encryption.	Much safer as two keys are involved in encryption and decryption.
Number of keys	Symmetric Encryption uses a single key for encryption and decryption.	Asymmetric Encryption uses two keys for encryption and decryption
Techniques	It is an old technique.	It is a modern encryption technique.
Confidentiality	A single key for encryption and decryption has chances of key compromised.	Two keys separately made for encryption and decryption that removes the need to share a key.
Speed	Symmetric encryption is fast technique	Asymmetric encryption is slower in terms of speed.
Algorithms	RC4, AES, DES, 3DES, and QUAD.	RSA, Diffie-Hellman, ECC algorithms.

Answer 4 : A digital signature is a mathematical scheme for verifying the authenticity of digital messages or documents. A valid digital signature, where the prerequisites are satisfied, gives a recipient very high confidence that the message was created by a known sender, and that the message was not altered in transit.

Section C

Answer 1:

1. Broken Access Control

User restrictions must be properly enforced. If they are broken, it can create a software vulnerability. Untrustworthy agents can exploit that vulnerability.

2. Cryptographic Failures

Sensitive data — such as addresses, passwords, and account numbers — must be properly protected. If it isn't, untrustworthy agents take advantage of the vulnerabilities to gain access.

3. Injection

Injection flaws occur when untrusted data is sent as part of a command or query. The attack can then trick the targeted system into executing unintended commands. An attack can also provide untrustworthy agents access to protected data.

4. Insecure Design

Insecure design refers to risks related to design flaws, which often includes the lack of at least one of the following:

- Threat modeling
- Secure design patterns
- Secure design principles
- Reference architecture

5. Security Misconfiguration

Security misconfigurations are often the result of:

- Insecure default configurations.
- Incomplete or impromptu configurations.
- Open Cloud storage.
- Misconfigured HTTP headers.
- Wordy error messages that contain sensitive information.

6. Vulnerable and Outdated Components

Components are made up of libraries, frameworks, and other software modules. Often, the components run on the same privileges as your application. If a component is vulnerable, it can be exploited by an untrustworthy agent. This causes serious data loss or server takeover.

7. Identification and Authentication Failures

Authentication and session management application functions need to be implemented correctly. If they aren't, it creates a software vulnerability that can be exploited by untrustworthy agents to gain access to personal information.

8. Software and Data Integrity Failures

Software and data integrity failures refer to assumptions made about software updates, critical data, and CI/CD pipelines without verifying integrity. In addition, deserialization flaws often result in remote code execution. This enables untrustworthy agents to perform replay, injection, and privilege escalation attacks.

9. Security Logging and Monitoring Failures

Insufficient logging and monitoring processes are dangerous. This leaves your data vulnerable to tampering, extraction, or even destruction.

10. Server-Side Request Forgery

Server-side request forgery refers to data that shows a relatively low incidence rate with above average testing coverage, and an above-average rating for Exploit and Impact potential.

Answer 2 :

Hardware vulnerabilities

1. Directory traversal

Old computer routers can have serious flaws that enable remote adversaries to take control of them. A Kyle Lovett security researcher, for instance, found that more than 700,000 ADSL routers distributed to various customers suffered from the "directory traversal" vulnerability that provides hackers with a way to extract administrative details.

2. Rowhammer

Rowhammer is classified as a vulnerability affecting some recent DDR DRAM devices where repeated access to a memory row can result in bit flips in adjustment rows. This means that, tentatively, a hacker can change any value of the memory's bit.

3. Meltdown RDCL

Meltdown RDCL (Rogue Data Cache Load) capitalizes on the non-functional execution capabilities of Intel CPUs. Hackers can use it to break through the kernel's privilege boundaries, which typically safeguard sensitive secrets.

4. Thunderclap

Thunderclap is a collection of hardware vulnerabilities that reside in the Thunderbolt hardware interface produced by Intel. It can be used by hackers with physical access to a Thunderbolt port to overtake a target system in just a few seconds, executing arbitrary code at the highest level of privilege and gaining access to encryption keys, passwords, banking logins and other data.

5. Speculative Store Bypass (SBS)

A variant of the Spectre security vulnerability, SSB or Speculative Store Bypass enables hackers to execute memory readers before memory write addresses are revealed. It can also be used to leak cross-process data. The vulnerability impacts Intel, AMD and ARM variants of processors.

6. Screwed drivers

According to researchers at Eclypsium, over 40 drivers from major BIOS vendors — including Huawei, Asus, Toshiba and NVIDIA — are susceptible to "screwed drivers" vulnerabilities. These are driver design flaws that enable hackers to escalate user privileges in order to access OS kernel models. The escalation opens and writes access to control registers (CR), model-specific registers (MSR), chipset I/O space, kernel and physical virtual memory.

Answer 3 :

Firmware vulnerabilities

1. Intel SA-00191

Specific Intel firmware is susceptible to security vulnerabilities that may allow hackers to disclose sensitive information, escalate privileges and launch DoS (Denial of Service) attacks. Products that incorporate Intel technology, such as the NetApp suite of products, are also at risk until hardware vendors move them to a patched and secure platform.

2. Thunderstrike

Thunderstrike allows hackers to exploit vulnerabilities in the firmware of Apple Macbooks in order to inject firmware rootkits when malicious systems were connected with Thunderbolt ports. Attackers primarily target Thunderbolt-linked accessories that are using Option ROMs, infecting all Macs that connected to it at boot. The infected machines can then pass the malicious code to other accessories, which could then affect other Macs.

3. MergePoint EMS command injection

Researchers at Eclypsium found a command injection vulnerability in MergePoint EMS component of BMC firmware. Hackers can use it to run malicious code with escalated privileges on a machine running the vulnerable BMC firmware. Companies like Lenovo and Gigabyte use the MergePoint EMS component as the firmware of the baseboard management controller that ships with some variants of their server-line motherboards.

4. ROCA

ROCA, or the Return of Coppersmith, allows the RSKA keys generated through Infineon's SEs (Secure Elements) and TPMs (Trusted Platform Modules) to be highly vulnerable to factorization attacks. These attacks are specifically designed to recover the RSA keys.

Successful exploitation could potentially enable a hacker to remotely reverse-calculate encryption keys by just having a single victim's public key.

5. Windows Error Reporting CVE-2019-0863

Certain versions of Microsoft Windows are prone to a privilege-hijacking vulnerability that allows hackers to gain escalated privileges. The vulnerability, referred to as CVE-2019-0863, is associated with the Windows Error Reporting feature and is being leveraged by adversaries who have gained remote access to target systems. They're able to activate arbitrary code execution at the kernel level via malware that allows them to go from user to admin-level execution in a matter of seconds.

6 Intel NUC Kit buffer overflow

Outdated firmware in Intel NUC (Next Unit of Computing), a mini-computer kit used for digital signage, gaming and more, suffers from a buffer overflow vulnerability that could enable hackers to potentially execute DoS (Denial of Service), escalation of privileges and data disclosure through local access. Typically, the root cause of such vulnerabilities is coding errors. Common development errors that can result in buffer overflows include neglecting to cross-check overflow issues and failing to assign big enough buffers.

7 Key Reinstallation Attacks (KRACK)

Key Reinstallation Attacks, or KRACK, target a weakness in the firmware of the WPA2 wireless security standard, which is used to secure most Wi-Fi networks in existence. Adversaries can use the exploit to intercept the traffic between a victim's device and their router and launch man-in-the-middle attacks, such as injecting malicious data into the wireless stream for modifying web pages or installing malware.

Answer 4 :

A network that follows well-defined policies capably fills business needs that it is designed to support. Think of network policies as objectives or goals. Without clear objectives, your network can't be set up to deliver optimally, and without goals, its performance can't be measured.

Business intent and agility

Network policies reflect business intent. Network controllers ingest business intent and create policies that help achieve the desired business outcomes. Policies are enforced and carried out by network equipment such as switches, routers, wireless access points, and wireless LAN controllers. Networks operated in an ad hoc fashion, without guiding policies, will likely fail to deliver optimally.

Consistency of experience

Well-executed policies in the network provide consistency of service throughout it, regardless of locations, means of connectivity, or devices in use. This means users and things can use the network from anywhere and still have the same access privileges and quality of network experience.

Network automation

Network devices and their operations can be better automated when guidance exists. With policies, configurations can be automated and orchestrated so that each device does what's required to achieve the larger objectives.

Performance monitoring

Once well-understood goals are defined, metrics can be established to measure how the network is delivering. Continuous analysis of performance helps ensure that policies are being followed and business objectives are being met.

Network security

With policies in place, any violations can be easier to detect. Security is more easily enforced, threats more quickly contained, and risk rapidly reduced with security-related policies.

BHARTIYA SKILL DEVELOPMENT UNIVERSITY

Registration No.: ..... Name - .....

School of Computing Skills

SET-B

B.Voc Program, III Semester (2022)

End-Sem. Examination

Course Code : ITN1303

Course Name : Basic of Network Security Time: 2 hour

Instruction: Explain in detail for long answer Max. Marks : 50

Section-A

10X1 = 10 Marks

Q.1 Viruses and Trojan Horses are often called.

a) software
b) malware

Q.2 A virus can insert itself into documents on your computer.

a) false
b) true

Q.3 100% of viruses are harmful to your computer.

a) True
b) False

Q.4 The most common examples of Identity Theft are _____.

a) Social Security Numbers
b) Bank Account numbers
c) Credit Card Numbers
d) All of the Above

Q.5 The field that covers a variety of computer networks, both public and private, that are used in everyday jobs.

a) Artificial Intelligence
b) ML
c) Network Security
d) IT

Q.6 Network Security provides authentication and access control for resources.

a) True
b) False

Q. 7 Which is not an objective of network security.

a) Identification
b) Authentication
c) Access control
d) Lock

Q.8 The process of verifying the identity of a user.

a) Authentication
b) Identification
c) Validation
d) Verification

Q.9 An algorithm in encryption is called _____.
a) Algorithm
b) Procedure
c) Cipher
d) Module

Q.10 The information that gets transformed in encryption is _____.
a) Plain text
b) Parallel text
c) Encrypted text
d) Decrypted text

Section B

04X04= 16 Marks

Q.1 Explain network policy .

Q.2 What is cipher test with example .

Q.3. Explain type of encryption .

Q.4 Explain digital signature with diagram .

Section C

04X06=24 Marks

Q.1 Explain RSA algorithm with 6 steps .

Q.2 Explain why malware , virus is dangers for any organization .

Q.3 Explain different type of network security Vulnerability.

Q.4 Explain what is need of network policy.

Registration No.: ..... Name - .....

School of Computing Skills

B.Voc Program, III Semester (2022)

End-Sem. Examination

Course Code : ITN1303

Course Name : Basic of Network Security **Time: 2 hour**

Instruction: Explain in detail for long answer **Max. Marks : 50**

Section A

Q.1 B

Q.2 A

Q.3 B

Q.4 D

Q.5 C

Q.6 A

Q.7 d

Q.8 A

Q.9 C

Q.10 C

SECTION B

Answer 1 : Network policy is a collection of rules that govern the behaviors of network devices. Just as a federal or central government may lay down policies for state or districts to follow to achieve national objectives, network administrators define policies for network devices to follow to achieve business objectives.

Answer 2: Ciphertext is **encrypted text transformed from plaintext using an encryption algorithm.** Ciphertext can't be read until it has been converted into plaintext (decrypted) with a key. The decryption cipher is an algorithm that transforms the ciphertext back into plaintext.

Answer 3 :

Symmetric Key Encryption	Asymmetric Key Encryption
It only requires a single key for both encryption and decryption.	It requires two keys, a public key and a private key, one to encrypt and the other one to decrypt.
The size of cipher text is the same or smaller than the original plain text.	The size of cipher text is the same or larger than the original plain text.
The encryption process is very fast.	The encryption process is slow.
It is used when a large amount of data is required to transfer.	It is used to transfer small amounts of data.
It only provides confidentiality.	It provides confidentiality, authenticity, and non-repudiation.
The length of key used is 128 or 256 bits	The length of key used is 2048 or higher
In symmetric key encryption, resource utilization is low as compared to asymmetric key encryption.	In asymmetric key encryption, resource utilization is high.
Examples: 3DES, AES, DES and RC4	Examples: Diffie-Hellman, ECC, El Gamal, DSA and RSA

Answer 4 A digital signature is **an electronic, encrypted, stamp of authentication on digital information such as email messages, macros, or electronic documents**. A signature confirms that the information originated from the signer and has not been altered.

Section c :

Answer 1 : RSA encryption algorithm is a type of public-key encryption algorithm. To better understand RSA, lets first understand what is public-key encryption algorithm.

RSA algorithm uses the following procedure to generate public and private keys:

- Select two large prime numbers, p and **q**.
- Multiply these numbers to find **n = p x q,** where **n** is called the modulus for encryption and decryption.
- Choose a number **e** less than **n**, such that n is relatively prime to **(p - 1) x (q -1).** It means that **e** and **(p - 1) x (q - 1)** have no common factor except 1. Choose "e" such that $1<e<\varphi(n)$, e is prime to $\varphi(n)$,
  gcd (e,d(n)) =1
- If **n = p x q,** then the public key is <e, n>. A plaintext message **m** is encrypted using public key <e, n>. To find ciphertext from the plain text following formula is used to get ciphertext C.
  $\mathbf{C = m^e \bmod n}$
  Here, **m** must be less than **n**. A larger message (>n) is treated as a concatenation of messages, each of which is encrypted separately.
- To determine the private key, we use the following formula to calculate the d such that:
  $\mathbf{D_e \bmod \{(p - 1) x (q - 1)\} = 1}$

4. Spread Throughout Your Network

Worms are an especially disruptive type of malware for businesses. Once this malware infects a computer, it replicates itself and spreads throughout the entire network. Most companies operate all their devices on a single network — which means that a worm could damage not just one employee's computer, but the entire organization.

5. Disrupt Daily Operations

Nearly every type of malware will affect normal business operations in some form or another. Adware is specifically a nuisance for business productivity. When installed onto a computer, it enables constant popups and can even redirect your search results to advertisers' sites — making it hard for anyone to enjoy the functionality of their device.

Answer 3 : Hardware vulnerabilities

1. Directory traversal

Old computer routers can have serious flaws that enable remote adversaries to take control of them. A Kyle Lovett security researcher, for instance, found that more than 700,000 ADSL routers distributed to various customers suffered from the "directory traversal" vulnerability that provides hackers with a way to extract administrative details.

2. Rowhammer

Rowhammer is classified as a vulnerability affecting some recent DDR DRAM devices where repeated access to a memory row can result in bit flips in adjustment rows. This means that, tentatively, a hacker can change any value of the memory's bit.

3. Meltdown RDCL

Meltdown RDCL (Rogue Data Cache Load) capitalizes on the non-functional execution capabilities of Intel CPUs. Hackers can use it to break through the kernel's privilege boundaries, which typically safeguard sensitive secrets.

4. Thunderclap

Thunderclap is a collection of hardware vulnerabilities that reside in the Thunderbolt hardware interface produced by Intel. It can be used by hackers with physical access to a Thunderbolt port to overtake a target system in just a few seconds, executing arbitrary code at the highest level of privilege and gaining access to encryption keys, passwords, banking logins and other data.

5. Speculative Store Bypass (SBS)

A variant of the Spectre security vulnerability, SSB or Speculative Store Bypass enables hackers to execute memory readers before memory write addresses are revealed. It can also

Or

$D_e \bmod \varphi(n) = 1$

- The private key is <d, n>. A ciphertext message **c** is decrypted using private key <d, n>. To calculate plain text **m** from the ciphertext c following formula is used to get plain text m.

  $m = c^d \bmod n$

Let's take some example of RSA encryption algorithm:

Answer 2 :

What Can Malware Do?

In short, malware can wreak havoc on a computer and its network. Hackers use it to steal passwords, delete files and render computers inoperable. A malware infection can cause many problems that affect daily operation and the long-term security of your company. Here are some of the many things malware can do.

1. Steal Your Sensitive Information

More than 1,000 data breaches occurred in the past year alone. These breaches affected a range of diverse industries, from government operations to small and large businesses, and many got their start with malware.

Information theft is one of the most serious and costly results of malware. Once pieces of malware such as spyware and trojans are installed on your device, hackers can gather your personal and company information to sell to third-party sources. This information can include browsing history, passwords, client profiles and other sensitive data.

2. Slow Your Computer

Once a piece of malware is in action, it begins to consume a large chunk of your computer's memory. Many types of malware also replicate themselves and fill your hard drive, so there's little room left for legitimate programs. This loss of space can lead to a sluggish computer, which makes it difficult to carry on with business as usual.

3. Restrict Access to Your Files

Certain types of malware can damage or delete files and programs on your computer. Unless your data is backed up on another hard drive or cloud server, you won't be able to regain access to many of these files after a cyber attack.

One type of malware known as ransomware holds the files on your computer hostage. Ransomware hackers threaten to delete all of your data unless you give them money.

be used to leak cross-process data. The vulnerability impacts Intel, AMD and ARM variants of processors.

Answer 4 :

Benefits of network policy

A network that runs on policies can be automated more easily and therefore respond more quickly to changing needs. Many common tasks, such as adding devices and users and inserting new applications and services, can now be easily accomplished. Well-defined policies can benefit a network in the following ways:

- Align the network with business needs
- Provide consistent services across the entire infrastructure
- Bring agility through greater automation
- Make performance dependable and verifiable

An even bigger advantage to enterprises is the security gains from policy. By granularly defining policies that give users and devices the least amount of access to resources that they need to do their jobs, you can better protect sensitive data. Violations can be caught and mitigated quickly. Such zero-trust security measures reduce risk, contain threats, stop lateral movement of malware, and help verify regulatory compliance.

1.

Set - B

BHARTIYA SKILL DEVELOPMENT UNIVERSITY

Registration No.: .....

School of Computing Skills
Session: 2021-2022 (Winter Semester)
B. Voc. Program, III Semester
END Sem. Examination

SET-B

Course Code: ITN1305 **Time: 2 Hour**
Course Name: Optical fiber communication **Max. Marks: 50**
Instruction: Answer All Questions

Section – A 10X01 = 10 Marks

Q.1 OTDR stands for _____.

A Optical time domain reflectometer

B Optical transfer data rate

C Optical time data registers

D None of the mentioned

Q.2. Which one of the following is NOT a connector termination tool?

A. Shear

B. Cleaver

C. SC

D. Stripper

Q. 3. **Plastics optical cables can be used for _____.**

A. Short Range

B. Medium range of distance

C. Long range of distance

D) Very high range of distance

Q.4. A single mode optical fiber has a core diameter of _____ nm.

A. 0.1

B. 0.01

C. 0.2

D. 0.05

Q.5. Cladding in glass fiber have high refractive index than the core.

A. True

B. False

Q.6. Plastic fibers are less widely used than glass fibers

A .True
B. False

Q.7. Which among the following stages is/are adopted in Splice Loss Experiment?

A. Translational
B. Rotational
C. Both A and B
D. None of the above

Q.8. Which component of fiber-optic connector has a provision of entry for the fiber along with the fixation to connector housing?

(A) Ferrule
(B) Cable
(C) Connector Housing
(D) Coupling Device

Q.9. Which one of the following is not a guided medium of transmission?

A. Fiber–Optic cable

B. Coaxial cable

C. Twisted-pair cable

D. The atmosphere

Q.10. Multimode graded index fibres use incoherent source only.

A. True
B .False

BHARTIYA SKILL DEVELOPMENT UNIVERSITY

Section –B **04X04 = 16 Marks**

Q. 1. What is the basic construction of a fiber optic cable?

Q.2. What are the Advantages of Single Mode Fiber?

Q.3. Which device we can use to cleave the fiber?

Q.4. What Is Optical Fiber?

Section-c

04*6=24 Marks

Q1. Describe the following – I.P.A. & Sleeves.

Q.2. What Are the Advantages and Disadvantages of Optical Fiber?

Q.3. What Are the Advantages of LC Fiber Connector?

Q.4. What is SC Fiber Connector?

BHARTIYA SKILL DEVELOPMENT UNIVERSITY

Registration No.: .....

sec B

School of Computing Skills

Session: 2021-22 (Winter Semester)

B. Voc. Program, 3rd Semester,

END Sem. Examination

Course Code: ITN1305 **Time: 2 Hour Course**

Name: Optical Fiber Communication **Max. Marks: 50**

Section – A

010X01 = 10 Marks

Q.1 OTDR stands for _____.

A. Optical time domain reflectometer

B. Optical transfer data rate

C. Optical time data registers

D. None of the mentioned

Answer: A) Optical time domain reflectometer

Q.2. Which one of the following is NOT a connector termination tool?

A. Shear

B. Cleaver

C. SC

D. Stripper

Answer: C) SC

Q. 3. Plastics optical cables can be used for _____.

A. Short Range

B. Medium range of distance

C. Long range of distance

D) Very high range of distance

Answer: A) Short Range

Q.4. A single mode optical fiber has a core diameter of _____ nm.

A. 0.1

B. 0.01

C. 0.2

D. 0.05

Answer: B) 0.01

5. Cladding in glass fibre have high refractive index than the core.

A. True

B. False

Answer: B) False

Q. 6. Plastic fibers are less widely used than glass fibers .

A .True
B. False

Answer: A

Q.7. Which among the following stages is/are adopted in Splice Loss Experiment?

A. Translational
B. Rotational
C. Both A and B
D. None of the above

ANSWER: Both A and B

Q.8. Which component of fiber-optic connector has a provision of entry for the fiber along with the fixation to connector housing?

A. Ferrule
B. Cable
C. Connector Housing
D. Coupling Device

ANSWER: - Ferrule

Q.9. Which one of the following is not a guided medium of transmission?

A. Fiber–Optic cable
B. Coaxial cable
C. Twisted-pair cable
D. The atmosphere

ANSWER: A

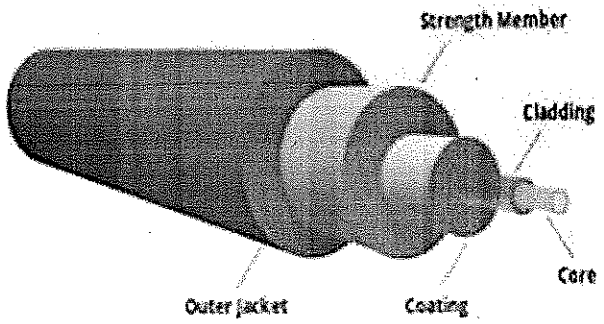
Q.10. Multimode graded index fibres use incoherent source only.

A. True
B .False

Answer: B

Section –B **04X04 = 16 Marks**

Q1. What is the basic construction of a fiber optic cable?



Q.2. What are the Advantages of Single Mode Fiber?

Ans.

Single mode fiber distance: single mode fiber supports a greater distance than multimode fiber because of its lower attenuation. For example, multimode fiber generally has a reach of several hundred meters, whereas SM fiber has the potential to reach 200 km.

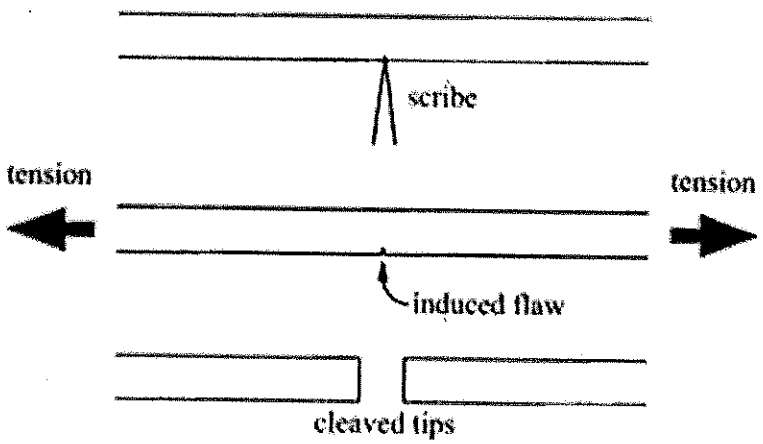
Bandwidth capacity: A single mode optical fiber cable offers a higher bandwidth than a multimode fiber optic cable.

Data dispersion: single mode fiber only transmits light of one mode, causing no modal dispersion. Single mode fiber speed: Single mode fiber doesn't have modal dispersion, modal noise, and other effects that come with multimode transmission. So it can carry signals at much higher speeds and up to 50 times more distance than multimode fiber.

Q.3. Which device we can use to cleave the fiber?

In simple terms, a cleaver is used to cut your fiber so you have two ends that will line up and can be welded together using a fusion splicer or they can be brought together in a mechanical splice. Fiber optic cleavers are essential tools when splicing and putting connectors on in the field

In the cleaving process, the brittle glass fiber is fractured in a controlled manner as shown below.



Q.4. What Is Optical Fiber?

Ans. **Optical fiber** uses light pulses instead of electrical pulses to transmit information, thus delivers hundreds of times higher bandwidth than traditional electrical systems. Fiber optic cable can be protected by sheathing and armor to make it resistant to harsh environmental conditions. Hence it is widely adopted in commercial business, governments, military and

many other industries for voice, video and data transmission. Optical fibers is used as a medium for telecommunication and networking. Light in a fiber optic cable travels through a core by constantly bouncing from the cladding, a principle termed total internal reflection. As the cladding does not absorb any light from the core, light waves travel longer distances. Fibers with a sizable core diameter may be analysed by geometrical optics. These fibers are called multi-mode fiber.

Section-c

04*6=24 Marks

Q.1. Describe the following – I.P.A. & Sleeves.

I.P.A: -

Isopropyl Alcohol is extremely effective for communication fiber optic cleaning. It easily removes offending dirt and can resolve many issues with your fiber optic installation. It can be used for any style connector, fiber optic patch cables or OTDR ports. Besides its effectiveness as a disinfectant which is one of the key benefits for many, 99% IPA evaporates quickly and cleanly, leaving behind **no significant or notable residues**

Sleeves.

Fiber splice sleeve is **composed of a steel strength member, inner fiber tube and outer shrink tube, two clear outer tubes for viewing the color of the optical fiber itself**. These sleeves are designed to fit smaller width splice trays while still accommodating both 250_m and 900_m fibers advantage of using splice sleeves is offering **lower insertion loss and provides better performance**, typical insertion loss is < 0.1 dB, therefore, it has a very low impact on overall link performance.

Q2. What Are the Advantages and Disadvantages of Optical Fiber?

Greater bandwidth & faster speed—Optical fiber cable supports extremely high bandwidth and speed. The large amount of information that can be transmitted per unit of optical fiber cable is its most significant advantage.

Cheap—Long, continuous miles of optical fiber cable can be made cheaper than equivalent lengths of copper wire. With numerous vendor's swarm to compete for the market share, optical cable price would sure to drop.

Thinner and light-weighted—Optical fiber is thinner, and can be drawn to smaller diameters than copper wire. They are of smaller size and light weight than a comparable copper wire cable, offering a better fit for places where space is a concern.

Higher carrying capacity—Because optical fibers are much thinner than copper wires, more fibers can be bundled into a given-diameter cable. This allows more phone lines to go over the same cable or more channels to come through the cable into your cable TV box. Less signal degradation—The loss of signal in optical fiber is less than that in copper wire. Light signals—Unlike electrical signals transmitted in copper wires, light signals from one fiber do not

interfere with those of other fibers in the same fiber cable. This means clearer phone conversations or TV reception.
Long lifespan—Optical fibers usually have a longer life cycle for over 100 years.

Disadvantages of Optical Fiber:- Low power—Light emitting sources are limited to low power. Although high power emitters are available to improve power supply, it would add extra cost.

Fragility—Optical fiber is rather fragile and more vulnerable to damage compared to copper wires. You'd better not to twist or bend fiber optic cables too tightly.
Distance—The distance between the transmitter and receiver should keep short or repeaters are needed to boost the signal.

Q.3. What Are the Advantages of LC Fiber Connector?

The LC connector is a small form factor (SFF) connector, which is designed to join LC fiber where a connection or disconnection is required. The LC connector was first developed by Lucent Technology for Telco environment uses. Hence, LC stands for Lucent Connector mostly. In addition, LC can also stand for Little Connector and Local Connector. These LC connectors utilize traditional components of the standard connector but with a 1.25mm ceramic ferrule. Nowadays, LC fiber optic connectors are very popular in the market. The following are

- With LC connector, the cost of the system can be reduced. LC connector is half the size of the traditional SC connector. Therefore, it can double fiber density in shelves and outlets. • The polarized feature of LC connector helps maintain the transmitting or receiving direction and assures high repeatability.
- LC connector has an anti-snag latch, which can improve durability and reduce the rearrangement work caused by the cross connection.
- It is time-saving for installation, because there is no need to install the field mountable connectors.

Q.4. What is SC Fiber Connector?

A straight tip connector (ST connector) is a connector used in fiber-optic cables that utilizes a bayonet-style plug and socket. It has become the de facto standard for commercial wirings. The ST connector setup allows for unidirectional communication, so two ST connectors and two fiber cables are used for bidirectional communication. The straight tip connector features a quick-release bayonet-style connector that is cylindrical with a twist-lock coupling, 2.5-mm keyed ferrule. It was developed by AT&T and became dominant during the 1980s and 1990s for long-line systems and short-distance applications. The most prominent feature of the ST connector is the straight ferrule, a rigid plastic tube, used to hold the fiber for proper alignment for interconnection or termination.

ST connectors are spring loaded, which means they are easily inserted and removed, but one also has to make sure that they are seated properly to ensure that there is no light loss. The typical insertion loss is 0.25 db. The connector is rated for 500 mating cycles and is usable for both single- and multi-mode fiber.

his is an older style connector but is still commonly used in multimode applications. The ST connector, while older, is still commonly in use in today's fiber installations due to it being extremely easy to install and its relatively low cost compared to some other connectors.

Set - A

BHARTIYA SKILL DEVELOPMENT UNIVERSITY

Registration No.: .....

SET-A

School of Computing Skills

Session: 2021-22 (Winter Semester)

B. Voc. Program, 3rd Semester,

END Sem. Examination

Course Code: ITN1305 **Time: 2 Hour**

Course Name: Optical Fiber Communication **Max. Marks: 50**

Section – A

10X01 = 10 Marks

Q.1. In optical fiber communications, the signal source is _____ waves.

A. Light
B. Infrared
C. Radio
D. Very low-frequency

Q.2. Which of these converts the electrical signal to optical signals?

A. Optical photo detectors
B. Demultiplexers
C. Multiplexers
D. Optical modulators

Q.3. In optical fiber, the outer layer is _____ and inner layer is _____

A. core, cladding
B. cladding, core
C. transmit, reflect
D. reflect, transmit

Q.4. _____ is a guided medium.

A. Microwave
B. Radio
C. Fiber-optic cable
D. Atmosphere

Q.5. Optical splice provides a connection between

A. Transmitter to fiber
B. Receiver to fiber
C. Fiber to fiber
D. Fiber to repeater

Q.6. The material used for fabrication of inner core of an optical fiber is

A. glass or plastic
B. bimetallic
C. copper
D. liquid

Q.7. Which fiber is used for long-distance transmission?

A. multimode
B. single-mode fiber
C. dual-mode fiber
D. None of the above

Q.8. Which of the following is an Advantages of Optical Fibre Communication?

A. Economical and cost-effective
B. Thin and non-flammable
C. Less power consumption
D. All of the above

Q.9. Silica or multi-component glass are used for the fabrication of optical fibers.

A.TRUE
B. FALSE
C. Can be true or false
D. Cannot say

Q.10. The micro-bending losses are depending on

A. Diameter
B. Core material
C. Refractive index
D. Mode and wavelength

BHARTIYA SKILL DEVELOPMENT UNIVERSITY

Section-B

04*04=16 Marks

Q.1. What do you think about the safety of fiber optic cables?

Q.2. What is the purpose of an OTDR?

Q.3. What is the difference between single mode and multimode fiber?

Q.4. What do you mean by SFP module?

Section-c

06*04=24 Marks

Q .1. What is the difference between single fiber connector and multiple fiber connector?

Q.2.What is media converter explain?

Q.3. What is difference between SC and LC. Explain.

Q.4. Describe the following.

I. LIU
II. Pigtail
III. Cleaver
IV. Stripper

Set - A

BHARTIYA SKILL DEVELOPMENT UNIVERSITY

Registration No.: .....

School of Computing Skills

Session: 2021-22 (Winter Semester)

B. Voc. Program, 3rd Semester,

END Sem. Examination

Course Code: ITN1305 **Time: 2 Hour**

Course Name: Optical Fiber Communication **Max. Marks: 50**

Section – A

10X01 = 10 Marks

Q.1. In optical fiber communications, the signal source is _____ waves.

A. Light
B. Infrared
C. Radio
D. Very low-frequency

Answer: Light

Q.2. Which of these converts the electrical signal to optical signals?

A. Optical photo detectors
B. Demultiplexers
C. Multiplexers
D. Optical modulators

Answer: D

Q.3. In optical fiber, the outer layer is _____ and inner layer is _____

A. core, cladding
B. cladding, core
C. transmit, reflect
D. reflect, transmit

Answer: cladding, core

Q.4. _____ is a guided medium.

A. Microwave

B. Radio
C. Fiber-optic cable
D. Atmosphere

Answer: Fiber-optic cable

Q.5. Optical splice provides a connection between

A. Transmitter to fiber
B. Receiver to fiber
C. Fiber to fiber
D. Fiber to repeater

Answer: fiber to fiber

Q.6. The material used for fabrication of inner core of an optical fiber is

A. glass or plastic
B. bimetallic
C. copper
D. liquid

Answer: glass or plastic

Q.7. Which fiber is used for long-distance transmission?

A. multimode
B. single-mode fiber
C. dual-mode fiber
D. None of the above

Answer: B (single-mode fiber)

Q.8. Which of the following is an Advantages of Optical Fibre Communication?

A. Economical and cost-effective
B. Thin and non-flammable
C. Less power consumption
D. All of the above

Answer: D (All of the above)

Q.9. Silica or multi-component glass are used for the fabrication of optical fibers.

A.TRUE
B. FALSE

C. Can be true or false
D. Cannot say

Answer: A (TRUE)

Q.10. The micro-bending losses are depending on

A. Diameter
B. Core material
C. Refractive index
D. Mode and wavelength

Answer: Mode and wavelength

Section-B

04*04=16 Marks

Q.1. What do you think about the safety of fiber optic cables?

Wear safety glasses or googles

Fiber optic shards and splinters can be dangerous if they get into your eyes. Treat fiber optic splinters the same as glass splinters. Always wear safety glasses when working with fiber optics and use side shields for full protection.

Keep food and beverages away from work areas

Fiber particles can easily get into food or drink and be swallowed. If ingested, they could become embedded in your digestive system and cause internal haemorrhaging.

Even if you keep your work area clean, the particles can easily be transferred from clothes to food and drinks. Never look directly into the end of fiber cablesProperly dispose of fiber and cable scraps

A big part of disposing of fiber and cable scraps involves keeping track of these materials. When you cleave fiber (generally in the fusion or termination process), small scraps of glass are produced. These scraps are very dangerous and can easily penetrate your skin.

Q.2. What is the purpose of an OTDR?

The process of running these tests requires the OTDR tool to input a light pulse into one end of a fiber cable. The results are based on the reflected signal that returns to the same OTDR port. Some of the light transmitted through the cable will scatter and some will be reflected and returned to the OTDR. This returned scatter and reflections are measured to gather useful information about the cable, such as loss and distances to connectors or faults. This is measured by recording the time it takes for signals to return to the OTDR.

With so many different uses for OTDR testing, setting the correct OTDR parameters can ensure the tests you run and measurements you get are accurate. For some tests, using the auto-test function may be enough to get you accurate results, but other may require you to manually set the OTDR testing parameters based on fiber cable length, type of cable, and complexity of your system. These OTDR parameters will adjust the pulse width, averaging time, dead zones, and the distance range for your given fiber run to offer the most accurate results.

Q.3. What is the difference between single mode and multimode fiber?

The major difference single-mode and multimode optical fiber is that in single-mode optical fiber light ray propagates only through a single path. On the contrary, in multimode optical fiber several light rays propagate through the waveguide at the same time. Another crucial difference between single-mode and multimode optical fiber is that **single-mode fiber has a smaller core diameter** as compared to multimode fiber. A single-mode optical fiber is a type of optical fiber that allows the propagation of only a single ray of light along the fiber. Here, the core to cladding diameter is 9 to 125 micrometres. It is also known as **uni-mode optical fiber or mono-mode optical fiber**. The diameter of the core is very small due to which only a single light ray gets transmitted through it's we are already known to the fact that an optical fiber has three basic parts namely- core, cladding and coating(buffer).

Q.4. What do you mean by SFP module?

SFP stands for small form-factor pluggable. It is a compact, hot-swappable optical transceiver module that used in telecommunications and data communications networks. Instead of being standardized by official standards, SFP is specified by the multi-source agreement (MSA). MSA is an agreement between many different transceiver manufactures to make standardized products. So the SFP is compatible across a range of telecoms vendors' hardware. And SFP module is designed to support synchronous optical networking (SONET), Gigabit Ethernet,

fiber channel and other communication standards. In addition, SFP module can be categorized into various types under Gigabit Ethernet standards and industry-accepted standards, including 1000BASE-EX, 1000BASE-ZX, 1000BASE-SR and so on.

Section-c

06*04=24 Marks

Q .1. What is the difference between single fiber connector and multiple fiber connector?

Single Mode cable is a single stand of glass fiber with a diameter of 8.3 to 10 microns that has one mode of transmission. Single Mode Fiber with a relatively narrow diameter, through which only one mode will propagate typically 1310nm or 1550nm. Carries higher bandwidth than multimode fiber, but requires a light source with a narrow spectral width. Synonyms mono-mode optical fiber, single-mode fiber, single-mode optical waveguide, uni-mode fiber.

Single-mode fiber gives you a higher transmission rate and up to 50 times more distance than multimode, but it also costs more. Single-mode fiber has a much smaller core than multimode. The small core and single light-wave virtually eliminate any distortion that could result from overlapping light pulses, providing the least signal attenuation and the highest transmission speeds of any fiber cable type.

Multimode cable is made of glass fibres, with a common diameter in the 50-to-100 micron range for the light carry component (the most common size is 62.5). POF is a newer plastic-based cable which promises performance similar to glass cable on very short runs, but at a lower cost.

Multimode fiber gives you high bandwidth at high speeds over medium distances. Light waves are dispersed into numerous paths, or modes, as they travel through the cable's core typically 850 or 1300nm. Typical multimode fiber core diameters are 50, 62.5, and 100 micrometres. However, in long cable runs (greater than 3000 feet [914.4 ml), multiple paths of light can cause signal distortion at the receiving end, resulting in an unclear and incomplete data transmission.

Q.2.What is media converter explain?

Fiber to Ethernet Converters use a opera transceiver to transform the signal from a UTP / RJ45 Ethernet link to one that can be used by a fiber optic transceiver. These Media Converters are used to enable connections of UTP **copper-based Ethernet equipment to** various optical fiber cable such as **multimode, single mode, or single strand** fiber. The benefits include,

extending Ethernet links over greater distances, protecting data from noise and interference, and **future proofing a network with additional bandwidth** capacity.

Copper-based Ethernet connections are limited to a data transmission distance of only 100 meters [328 feet] when using unshielded twisted pair (UTP) cable. By using an Ethernet to fiber conversion solution, fiber optic cabling can be used to **extend this link over a greater distance.** An Ethernet to Fiber Media Converter can also be used where there is high level of electromagnetic interference (EMI) which is a common phenomenon found in industrial plants. This interference can cause corruption of data over copper-based Ethernet links. Data transmitted over **fiber optic cable is immune to EMI noise**, ensuring optimal data transmission across the plant floor.

Q.3. What is difference between SC and LC. Explain.

Lucent Technologies, now part of Nokia, developed LC connectors in the early 2000s amid complaints that ST and SC connectors were too bulky and easy to dislodge from fiber connections. However, the initial market response to LC connectors was lacklustre due to a high license fee.

Eventually, with the availability of LC-compatible transceivers and other active networking components, this smaller version of SC connectors began taking off in new fiber applications such as fiber to the home (FTTH). The smaller form factor, with a 1.25-mm ferrule, was also a huge benefit in high-connection-density environments like data centres and telecom switching centres.

LC is also a push-pull connector, but unlike SC's locking tab, it employs a latch with a smaller ferrule, and that makes it hugely popular in data communications and other high-density patch applications

SC, abbreviated for Subscriber Connector, has also been referred to as Square Connector or Standard Connector. It's a popular fiber-optic connector due to its low-cost, durability and simple installation for both point-to-point and passive optical networking.

SC is a push-pull device that uses a ceramic ferrule to deliver highly accurate alignment in a fiber-optic link. It's a square-shaped connector—also known as "stick and click" for its SC acronym—that comes with a locking tab that enables the push-on and pull-off operation.

Q.4. Describe the following.

I. **LIU**
II. **Pigtail**
III. **Cleaver**
IV. **Stripper**

I. The LIU (optical fiber interconnecting unit) is modular and suitable for optical cable installation, bare fibers splicing & protection, pigtails storage & management. The number of fibers determines which LIU is appropriate for the application.

II. Fiber optic pigtail is a fiber optic cable terminated with a factory-installed connector on one end, leaving the other end terminated. Hence the connector side can be linked to equipment and the other side melted with optical fiber cables

III. A cleaver is a mechanical precision device whose task is to cleave the end of an optical fiber so that the cleavage surface was as flat as possible and if possible at 90° angle to the fiber itself.

IV. Stripping is the act of removing the protective polymer coating around optical fiber in
preparation for fusion splicing. The splicing process begins by preparing both fiber ends
for fusion, which requires that all protective coating is removed or stripped from the ends of
each fiber.