

VU Learning HUB

CS204 Quiz File

Chapter-wise Solved MCQs

vulearninghub.xyz

Lesson 1: Introduction to Cyber Society, Cyber Culture and Cyber Space

Q1. According to the handout, which of the following is NOT identified as a primary component of cyber society?

- A) Cyber culture
- B) Cyberspace
- C) Cyber infrastructure
- D) Physical transportation systems

Q2. Which statement best captures the relationship between cyber culture and cyber society?

- A) Cyber culture is a broader concept that encompasses cyber society
- B) Cyber culture is the set of shared behaviors, norms, and values emerging within cyberspace and forms part of cyber society
- C) Cyber culture and cyber society are unrelated
- D) Cyber society is a subset of cyber culture limited to gaming

Q3. In the handout's discussion of cyber space, which characteristic distinguishes cyberspace from physical space?

- A) It requires physical travel
- B) It is a virtual, borderless environment enabling instant global interaction
- C) It is limited to one country
- D) It cannot support communication

Q4. Which example best illustrates cyber culture?

- A) Online gaming communities developing unique slang and norms
- B) A printed newspaper
- C) A physical library
- D) A handwritten letter

Answer Key

1. D) Physical transportation systems are not listed as a component of cyber society.
2. B) Cyber culture comprises shared behaviors, norms, and values emerging in cyberspace and is part of cyber society.
3. B) Cyberspace is described as a virtual, borderless environment enabling instant global interaction.
4. A) Online gaming communities with unique slang and norms exemplify cyber culture.

Lesson 2: Fundamentals of E-Commerce

Q1. Which of the following best defines e-commerce as presented in the handout?

- A) Buying and selling of goods and services over electronic networks, primarily the internet
- B) Only online banking
- C) Physical retail stores
- D) Barter trade

Q2. Which is an example of a B2C e-commerce model?

- A) A manufacturer selling to a wholesaler
- B) An online retailer selling directly to consumers (e.g., Daraz)

- C) Government procurement
- D) Employee intranet

Q3. What is a key advantage of e-commerce highlighted in the handout?

- A) Limited market reach
- B) 24/7 availability and global customer reach
- C) Higher physical overhead
- D) Slower transactions

Q4. Which of the following is a challenge of e-commerce mentioned in the handout?

- A) Unlimited trust
- B) Security and privacy concerns in online transactions
- C) No competition
- D) Instant delivery always

Answer Key

1. A) E-commerce is defined as buying and selling goods and services over electronic networks, primarily the internet.
2. B) B2C involves businesses selling directly to consumers, e.g., an online retailer like Daraz.
3. B) E-commerce offers 24/7 availability and access to a global customer base.
4. B) Security and privacy concerns are key challenges in online transactions.

Lesson 3: Introduction to Cyber Crime

Q1. How does the handout define cyber crime?

- A) Any crime committed with a physical weapon
- B) Criminal activities carried out using computers or the internet
- C) Only hacking
- D) Traffic violations

Q2. Which of the following is an example of cyber crime?

- A) Phishing emails stealing credentials
- B) A printed book
- C) A physical theft without computers
- D) A handwritten note

Q3. What distinguishes cyber crime from traditional crime according to the handout?

- A) It always involves violence
- B) It is committed in cyberspace, often crossing jurisdictional boundaries
- C) It is never serious
- D) It requires no technology

Q4. Which is NOT a type of cyber crime discussed?

- A) Hacking
- B) Identity theft
- C) Online fraud
- D) Playing offline chess

Answer Key

1. B) Cyber crime is defined as criminal activities carried out using computers or the internet.
2. A) Phishing emails that steal user credentials are a classic example of cyber crime.
3. B) Cyber crime occurs in cyberspace and frequently crosses jurisdictional boundaries.
4. D) Playing offline chess is not a cyber crime.

Lesson 4: Cyber Security

Q1. What is the primary goal of cyber security as described in the handout?

- A) To increase internet speed
- B) To protect systems, networks, and data from digital attacks
- C) To design websites
- D) To manufacture hardware

Q2. Which of the following is a common cyber security threat?

- A) Malware
- B) A printed manual
- C) A desk
- D) A chair

Q3. What does the "CIA triad" in cyber security stand for?

- A) Confidentiality, Integrity, Availability
- B) Central Intelligence Agency
- C) Computer Internet Access
- D) Crime Investigation Authority

Q4. Which practice strengthens cyber security?

- A) Using strong, unique passwords and enabling multi-factor authentication
- B) Sharing passwords publicly
- C) Disabling firewalls
- D) Clicking unknown links

Answer Key

1. B) Cyber security aims to protect systems, networks, and data from digital attacks.
2. A) Malware is a common cyber security threat.
3. A) The CIA triad stands for Confidentiality, Integrity, and Availability.
4. A) Strong unique passwords plus multi-factor authentication strengthen security.

Lesson 5: Cryptography

Q1. What is cryptography?

- A) The practice of secure communication by transforming information
- B) A type of computer virus
- C) A social media platform
- D) A hardware component

Q2. Which of the following is a symmetric encryption algorithm?

- A) AES
- B) RSA

- C) A hashtag
- D) A firewall

Q3. What is the main difference between symmetric and asymmetric encryption?

- A) Symmetric uses one shared key; asymmetric uses a public/private key pair
- B) There is no difference
- C) Symmetric is only for images
- D) Asymmetric is obsolete

Q4. What is a digital signature used for?

- A) Verifying authenticity and integrity of a message
- B) Signing printed papers
- C) Increasing font size
- D) Deleting files

Answer Key

1. A) Cryptography is the practice of secure communication through transforming information.
2. A) AES is a widely used symmetric encryption algorithm.
3. A) Symmetric encryption uses a single shared key, while asymmetric uses a public/private key pair.
4. A) Digital signatures verify the authenticity and integrity of messages.

Lesson 6: Introduction to Cyber Law

Q1. What is cyber law?

- A) The legal framework governing conduct in cyberspace
- B) Traffic rules
- C) Property tax law
- D) Maritime law

Q2. Why is cyber law important according to the handout?

- A) It provides legal recourse against cyber crimes and regulates online conduct
- B) It increases internet speed
- C) It designs hardware
- D) It is not important

Q3. Which of the following falls under cyber law?

- A) Data protection and privacy regulations
- B) Cooking recipes
- C) Sports rules
- D) Gardening tips

Q4. What is a challenge in enforcing cyber law?

- A) Jurisdictional issues since cyber crimes cross borders
- B) Too few laws
- C) No internet
- D) Lack of computers

Answer Key

1. A) Cyber law is the legal framework governing conduct and transactions in cyberspace.

2. A) Cyber law provides legal recourse against cyber crimes and regulates online behavior.
3. A) Data protection and privacy regulations fall under cyber law.
4. A) Cross-border jurisdictional issues make cyber law enforcement challenging.

Lesson 7: Cyber Law in Pakistan

Q1. Which law specifically addresses cyber crime in Pakistan?

- A) PECA 2016 (Prevention of Electronic Crimes Act)
- B) Traffic Act
- C) Property Act
- D) Labor Act

Q2. Under PECA 2016, unauthorized access to an information system is:

- A) A punishable offence
- B) Legal
- C) Encouraged
- D) Irrelevant

Q3. Which agency is primarily responsible for investigating cyber crimes in Pakistan?

- A) FIA (Federal Investigation Agency) Cybercrime Wing
- B) Traffic police
- C) Postal service
- D) Food authority

Q4. What is a penalty under PECA for cyber terrorism?

- A) Severe punishment including long imprisonment
- B) A small fine only
- C) No penalty
- D) A warning letter

Answer Key

1. A) PECA 2016 is Pakistan's dedicated cyber crime legislation.
2. A) Unauthorized access to information systems is a punishable offence under PECA.
3. A) The FIA Cybercrime Wing investigates cyber crimes in Pakistan.
4. A) Cyber terrorism attracts severe penalties including long imprisonment under PECA.

Lesson 8: E-Commerce Business Models

Q1. In a B2B e-commerce model:

- A) Businesses transact with other businesses
- B) Businesses sell to consumers
- C) Consumers sell to consumers
- D) Government sells to businesses

Q2. Which is an example of C2C e-commerce?

- A) OLX users selling to each other
- B) A factory selling to a retailer
- C) Government e-procurement

D) Intranet portal

Q3. What does B2G stand for in e-commerce?

- A) Business to Government
- B) Buyer to Group
- C) Bank to Gateway
- D) Blog to Guest

Q4. Which model involves consumers offering services to businesses?

- A) C2B
- B) B2C
- C) B2B
- D) G2C

Answer Key

1. A) B2B involves transactions between businesses.
2. A) C2C platforms like OLX enable consumers to sell to each other.
3. A) B2G means Business to Government.
4. A) C2B involves consumers providing products/services to businesses.

Lesson 9: E-Payment Systems

Q1. Which of the following is an e-payment method?

- A) Credit/debit cards, mobile wallets, and bank transfers
- B) Cash only
- C) Barter
- D) Cheques only

Q2. What is a key security feature of e-payment systems?

- A) Encryption of transaction data
- B) Public display of PINs
- C) No authentication
- D) Plain-text passwords

Q3. Which is a popular mobile wallet in Pakistan?

- A) JazzCash/Easypaisa
- B) A paper wallet
- C) A leather wallet
- D) A piggy bank

Q4. What is a risk of e-payment systems?

- A) Phishing and transaction fraud
- B) No risks
- C) Too much cash
- D) Slow typing

Answer Key

1. A) E-payment methods include cards, mobile wallets, and electronic bank transfers.
2. A) Encryption protects e-payment transaction data.

3. A) JazzCash and Easypaisa are popular mobile wallets in Pakistan.
4. A) Phishing and transaction fraud are risks of e-payment systems.

Lesson 10: Cyber Crime Types (Advanced)

Q1. What is phishing?

- A) Fraudulent attempts to obtain sensitive information by impersonating trustworthy entities
- B) A fishing sport
- C) A music genre
- D) A cooking method

Q2. What is ransomware?

- A) Malware that encrypts data and demands payment for decryption
- B) A type of firewall
- C) An antivirus
- D) A backup tool

Q3. What is identity theft?

- A) Stealing someone's personal information to commit fraud
- B) Losing an ID card
- C) Changing one's name legally
- D) Forgetting a password

Q4. What is a DDoS attack?

- A) Overwhelming a system with traffic from multiple sources to disrupt service
- B) A software update
- C) A backup process
- D) A password reset

Answer Key

1. A) Phishing impersonates trustworthy entities to steal sensitive information.
2. A) Ransomware encrypts victim data and demands payment for the decryption key.
3. A) Identity theft involves stealing personal information to commit fraud.
4. A) DDoS attacks flood systems with traffic from multiple sources to disrupt services.

Lesson 11: Social Engineering

Q1. What is social engineering in cyber security?

- A) Manipulating people to divulge confidential information
- B) Building bridges
- C) Software engineering
- D) Civil engineering

Q2. Which is a social engineering technique?

- A) Pretexting (inventing a scenario to obtain information)
- B) Compiling code
- C) Defragmenting disks
- D) Installing RAM

Q3. How can social engineering be prevented?

- A) Security awareness training and verifying identities
- B) Sharing passwords
- C) Trusting all callers
- D) Disabling antivirus

Q4. What is baiting?

- A) Offering something enticing (e.g., free downloads) to deliver malware
- B) Fishing
- C) Cooking
- D) Gardening

Answer Key

1. A) Social engineering manipulates people into divulging confidential information.
2. A) Pretexting invents a scenario to trick victims into sharing information.
3. A) Awareness training and identity verification help prevent social engineering.
4. A) Baiting lures victims with enticing offers to deliver malware.

Lesson 12: Cyber Security Tools

Q1. What is a firewall?

- A) A network security device that monitors and filters traffic
- B) A physical wall
- C) A type of malware
- D) A printer

Q2. What does antivirus software do?

- A) Detects and removes malicious software
- B) Increases screen brightness
- C) Speeds up typing
- D) Cools the CPU

Q3. What is an IDS?

- A) Intrusion Detection System that monitors for malicious activity
- B) Internet Download Speed
- C) Internal Data Storage
- D) Image Display Software

Q4. Why are software updates important for security?

- A) They patch vulnerabilities exploited by attackers
- B) They change wallpaper
- C) They delete files
- D) They slow the system

Answer Key

1. A) A firewall monitors and filters network traffic based on security rules.
2. A) Antivirus software detects and removes malicious software.
3. A) An IDS monitors networks/systems for malicious activity or policy violations.

4. A) Updates patch security vulnerabilities that attackers exploit.

Lesson 13: Digital Forensics

Q1. What is digital forensics?

- A) Investigating cyber crimes by collecting and analyzing digital evidence
- B) A medical field
- C) Fingerprint analysis only
- D) Building computers

Q2. Which is a step in digital forensics?

- A) Preserving evidence with write-blockers to prevent alteration
- B) Deleting logs
- C) Formatting drives
- D) Ignoring chain of custody

Q3. What is chain of custody?

- A) Documented handling of evidence to maintain its integrity
- B) A jewelry chain
- C) A supply chain
- D) A password chain

Q4. Which tool is used in digital forensics?

- A) EnCase/FTK for disk imaging and analysis
- B) A hammer
- C) Paint
- D) A calculator

Answer Key

- 1. A) Digital forensics investigates cyber crimes through digital evidence collection and analysis.
- 2. A) Evidence preservation using write-blockers prevents alteration of original data.
- 3. A) Chain of custody documents evidence handling to preserve integrity for legal proceedings.
- 4. A) Tools like EnCase and FTK are used for disk imaging and forensic analysis.

Lesson 14: Cyber Ethics

Q1. What is cyber ethics?

- A) Moral principles governing behavior in cyberspace
- B) A programming language
- C) A hardware standard
- D) A network protocol

Q2. Which is an ethical issue in cyberspace?

- A) Plagiarism and intellectual property violations
- B) Eating food
- C) Driving cars
- D) Sleeping

Q3. Why is respecting intellectual property important?

- A) It protects creators' rights and encourages innovation
- B) It slows the internet
- C) It is not important
- D) It increases piracy

Q4. What is netiquette?

- A) Etiquette rules for online communication
- B) A fishing net
- C) A network cable
- D) A software license

Answer Key

1. A) Cyber ethics comprises moral principles governing conduct in cyberspace.
2. A) Plagiarism and IP violations are key ethical issues online.
3. A) Respecting IP protects creators' rights and encourages innovation.
4. A) Netiquette refers to etiquette rules for polite online communication.

Lesson 15: Emerging Trends

Q1. Which is an emerging cyber security trend?

- A) AI-driven threat detection
- B) Typewriters
- C) Paper files
- D) Abacus

Q2. What is IoT security concerned with?

- A) Securing internet-connected devices
- B) Securing doors
- C) Fishing
- D) Cooking

Q3. What is a zero-trust security model?

- A) "Never trust, always verify" — strict verification for every access request
- B) Trust everyone
- C) No passwords
- D) Open networks

Q4. Why is cyber security awareness important for society?

- A) It reduces successful attacks by making users the first line of defense
- B) It is not important
- C) It slows work
- D) It costs too much

Answer Key

1. A) AI-driven threat detection is an emerging cyber security trend.
2. A) IoT security focuses on securing internet-connected smart devices.
3. A) Zero-trust follows "never trust, always verify" with strict per-request verification.
4. A) Awareness makes users the first line of defense, reducing successful attacks.

End of Quiz

CS204 — 60 solved MCQs
Prepared by VU Learning HUB
vulearninghub.xyz