CYBERSECURITY PAPER 2

Section A

1) Explain the concept of DNS cache poisoning and how it facilitates pharming.
2) How does data validation prevent incorrect entries in critical systems like healthcare?
3) What are the differences between horizontal parity and vertical parity in parity checking?
4) How does a check digit algorithm detect transposition errors in data entry?
5) Explain the process of double-entry verification and its importance in critical systems.
6) Describe how firewalls can be bypassed and how to mitigate such risks.
7) What security measures can prevent spyware from collecting sensitive data?
8) How do retina scans ensure high accuracy in user authentication?
9) What are the legal implications of malicious hacking versus ethical hacking?
10) Explain how encryption algorithms ensure secure communication across the internet.
11) How does antivirus software distinguish between legitimate software and malware?
12) Discuss how parallel systems can prevent data loss during hardware failure.
13) What is the role of checksum algorithms in preventing data corruption during transmission?
14) How does biometric voice recognition improve data security over traditional passwords?
15) Explain how pharming can redirect users to malicious websites without their knowledge.
16) What is the role of digital signatures in email authentication?
17) How does two-factor authentication (2FA) improve security in online systems?
18) Explain how strong encryption protocols like AES work to secure data.
19) How does firewall logging help in identifying security threats?
20) What are the limitations of antivirus software in detecting new, unknown malware?
21) Explain how logical access control prevents unauthorized data access.
22) What role does ARQ play in ensuring data transmission integrity?
23) How can keylogging software be used for malicious purposes, and how is it detected?

24) Describe the process of DNS spoofing and its impact on cybersecurity.

25) How does ARQ help recover lost data during transmission in mobile networks?

26) What are parallel backups, and how do they improve data recovery?

27) Explain how biometric facial recognition works in mobile devices.

28) What are the key differences between spyware and adware?

29) How does two-factor authentication reduce the risk of phishing attacks?

30) Discuss the role of firewalls in managing inbound and outbound network traffic.

31) How does checksum verification work in detecting data tampering during transmission?

32) What is the function of a network firewall in securing organizational data?

33) Explain how DNS poisoning can be prevented using modern security techniques.

34) How do botnets contribute to large-scale cyberattacks?

35) What is the importance of end-to-end encryption in messaging apps?

36) How does a Trojan horse disguise itself, and what makes it particularly dangerous?

37) What are the risks associated with using weak passwords in high-security systems?

38) Explain the importance of patch management in preventing software vulnerabilities.

39) How does HTTPS encryption protect against man-in-the-middle attacks?

40) What are the challenges of using biometrics in large-scale systems?

41) How does automatic repeat request (ARQ) handle timeouts in data transmission?

42) Explain how virus heuristics help in identifying unknown malware.

43) What is the importance of encryption keys in securing sensitive data?

44) How do hardware firewalls differ from software firewalls?

45) What is logic bomb malware, and how is it triggered?

46) How do strong passwords prevent brute-force attacks?

47) What is the role of validation and verification in preventing data entry errors?

48) How can security awareness training reduce the risk of phishing and pharming?

49) What is the Modulo-11 method, and where is it commonly applied?

50) How can DNS spoofing result in widespread data breaches?

Section B

1) Compare the pros and cons of symmetric and asymmetric encryption.
2) Explain how block cipher encryption prevents unauthorized access.
3) Describe the key distribution problem and its impact on network security.
4) How does the session key ensure secure communication in SSL?
5) How does TLS improve the security of online transactions?
6) What are the four key security concerns when transmitting data over a network?
7) Describe the role of certificate authorities in issuing digital certificates.
8) What is the importance of the handshake process in establishing SSL/TLS connections?
9) How does public key encryption solve the key distribution problem?
10) Explain how block chaining adds an additional layer of security in encryption.
11) Compare stream cipher with block cipher.
12) How does quantum cryptography leverage the properties of photons?
13) What is the significance of the Transport Layer Security (TLS) record protocol?
14) How do hashing algorithms ensure data integrity in digital signatures?
15) Explain the concept of session caching in TLS and how it improves performance.
16) What is the difference between a self-signed certificate and a certificate from a certificate authority?
17) How does public key infrastructure (PKI) enhance security in online communications?
18) Explain the role of quantum key distribution (QKD) in secure communication.
19) How does TLS separate the handshake from the record protocol?
20) What are the security advantages of using digital signatures?
21) What is the purpose of the XOR operation in block cipher encryption?
22) Describe the steps in generating a digital signature.
23) How does QKD ensure the security of encryption keys?
24) What are the limitations of SSL compared to TLS?
25) Explain the significance of session keys in TLS communication.
26) How does quantum cryptography overcome the limitations of classical encryption methods?
27) What is the role of a certificate authority (CA) in verifying digital certificates?
28) How does block cipher chaining prevent attacks on encryption systems?

29)Explain the process of asymmetric encryption using public and private keys.

30)Describe the hashing process involved in digital signatures.

31)What are the main differences between stream cipher and block cipher encryption methods?

32)How does the quantum key distribution (QKD) protocol protect against eavesdropping?

33)Explain the steps involved in acquiring a digital certificate from a certificate authority.

34)How does asymmetric encryption improve over symmetric encryption in terms of key distribution?

35)Describe how session caching works in Transport Layer Security (TLS).

36)What are the challenges of implementing quantum cryptography in modern systems?

37)How does SSL handshake establish secure communication between two devices?

38)Explain how digital certificates are verified by browsers.

39)Compare the digest produced by a hashing algorithm to the original data.

40)How does TLS ensure privacy and data integrity during transmission?

41)Describe the role of certificate authorities (CAs) in maintaining secure internet communication.

42)What are the advantages of session caching in reducing communication overhead in TLS?

43)How does the key exchange mechanism work in quantum cryptography?

44)Describe how digital signatures are used in authenticating online transactions.

45)How does SSL/TLS prevent third parties from eavesdropping on communication?

46)What is the purpose of using XOR in block cipher encryption?

47)Explain the difference between symmetric and asymmetric keys in cryptography.

48)How do hashing algorithms contribute to the creation of digital signatures?

49)What is the role of digital certificates in SSL/TLS handshakes?

50)How does quantum cryptography ensure the secure distribution of encryption keys?