CYBERSECURITY PAPER 3

Section A

1) How can biometric data be compromised, and what are the risks associated with its theft?
2) Describe the intricacies of end-to-end encryption and its applications in secure messaging.
3) How does man-in-the-middle attack work, and how can it be mitigated?
4) Explain how heavily encrypted files are decrypted during cybersecurity investigations.
5) How do botnets facilitate large-scale DDoS attacks, and what are the defensive measures?
6) How can hardware-based firewalls be combined with software firewalls for enhanced protection?
7) What are the ethical concerns surrounding ethical hacking and its potential misuse?
8) Explain the technical process of DNS cache poisoning and its implications for internet users.
9) How does data integrity checking in RAID systems prevent data loss?
10) What are the computational challenges in cracking modern encryption algorithms?
11) Discuss how pharming attacks bypass traditional security measures.
12) How does quantum computing threaten the future of encryption protocols?
13) Explain how deep packet inspection works in modern firewalls and its implications for privacy.
14) How can AI-based malware adapt to bypass traditional antivirus solutions?
15) What are the implications of keylogging software on financial institutions' security?
16) Describe the computational overhead in maintaining large-scale end-to-end encrypted systems.
17) What are the limitations of checksum algorithms in detecting multiple errors in data transmission?
18) How can advanced persistent threats (APTs) evade detection by firewalls and antivirus systems?
19) Discuss the implications of deepfake technology for biometric-based authentication.
20) How can logic bombs embedded in industrial control systems compromise national security?
21) What are the mathematical foundations of Modulo-11 check digit algorithms?
22) How can steganography be used to hide malicious code within images and audio files?
23) What are the challenges in detecting rootkits in an infected operating system?
24) Explain how blockchain technology ensures the integrity and security of data.
25) How do homomorphic encryption techniques allow computations on encrypted data?
26) What are the risks associated with phishing-as-a-service on the dark web?
27) How can quantum key distribution revolutionize secure communications?
28) What are the weaknesses of hashing algorithms in ensuring data integrity?

29) How do zero-day exploits affect the security of cloud systems?
30) Explain how AI-driven phishing attacks improve upon traditional phishing methods.
31) What are the technical challenges in implementing post-quantum cryptography?
32) How can machine learning algorithms detect DNS spoofing in real-time?
33) Discuss the role of entropy in generating secure cryptographic keys.
34) What are the security concerns surrounding the use of IoT devices in critical infrastructures?
35) How does biometric spoofing work, and what countermeasures exist?
36) Explain how quantum entanglement can be used to secure data transmission.
37) How does deep learning improve intrusion detection in network security?
38) What are the challenges in securing autonomous vehicles from cyber threats?
39) How can neural networks be used in cracking complex encryption algorithms?
40) What are the potential applications of quantum cryptography in modern cybersecurity?
41) Discuss how malicious AI can be used to generate sophisticated social engineering attacks.
42) How do hardware trojans compromise system security at a fundamental level?
43) What are the side-channel attacks in cryptographic systems, and how can they be mitigated?
44) How can digital forensics be applied to recover data from encrypted hard drives?
45) What are the risks of supply chain attacks in modern technology ecosystems?
46) How does quantum key distribution (QKD) prevent eavesdropping on secure channels?
47) Discuss the security challenges in implementing nationwide biometric identification systems.
48) How can multi-factor authentication prevent man-in-the-middle attacks in online banking?
49) What are the potential weaknesses of distributed denial of service (DDoS) protection measures?
50) How can homomorphic encryption balance between computational efficiency and data security?

Section B

1) Design an encryption system using both symmetric and asymmetric encryption.
2) Explain the impact of session caching on the performance of TLS protocols.
3) How can block chaining be used to enhance the security of large data files?
4) Analyze the key distribution problem and propose solutions for overcoming it.
5) Explain how quantum cryptography can be applied to prevent eavesdropping on sensitive data.
6) Compare the security of RSA encryption with quantum encryption.
7) What challenges arise when using TLS in a multi-user system, and how can they be addressed?
8) Design a public key infrastructure (PKI) for a large organization that handles financial transactions.
9) How does quantum key distribution (QKD) change the future of encryption?
10) What are the security vulnerabilities of using self-signed certificates instead of certificates from CAs?
11) Propose an algorithm that can optimize block cipher chaining in modern encryption systems.
12) How does the handshake process ensure that both client and server are authenticated in SSL/TLS?
13) Compare the efficiency of block cipher vs stream cipher encryption techniques for large-scale applications.
14) How does quantum cryptography deal with the issue of photon tampering during transmission?
15) What role does the certificate authority (CA) play in establishing a secure communication channel in TLS?
16) How do digital certificates protect against man-in-the-middle attacks?
17) Explain how session caching improves performance during repeated secure connections in TLS.
18) What is the future of encryption with the development of quantum computing?
19) How do public key infrastructures (PKIs) ensure trust in large distributed networks?
20) Explain how hashing algorithms prevent tampering in digital signatures.
21) How does quantum key distribution (QKD) prevent man-in-the-middle attacks?
22) Design a secure communication system using block cipher encryption and digital signatures.
23) How does the XOR operation contribute to security in block cipher encryption?
24) Analyze the vulnerabilities of SSL compared to TLS.
25) Propose improvements to the digital certificate validation process to reduce fraud.
26) How does quantum cryptography ensure the security of data transmitted over long distances?
27) Explain the role of session keys in enhancing the security of Transport Layer Security (TLS).
28) Compare the performance of quantum cryptography with traditional encryption methods.
29) What are the security implications of using self-signed digital certificates in a public network?
30) Design a quantum key distribution system that can handle the security needs of a government agency.
31) What are the challenges in implementing quantum cryptography for mobile devices?

32) Explain the use of hashing algorithms in creating non-repudiation in digital signatures.
33) How does session caching improve the efficiency of the TLS handshake in secure communications?
34) Compare the effectiveness of TLS and SSL in protecting against modern cyber threats.
35) How does quantum key distribution (QKD) ensure that encryption keys are tamper-proof?
36) Analyze the weaknesses of symmetric encryption in large-scale cloud systems.
37) Explain how digital signatures verify the authenticity of online documents.
38) What are the challenges of quantum encryption in secure email communication?
39) How can digital certificates be misused by attackers to perform phishing attacks?
40) Design a certificate authority infrastructure that can prevent the misuse of digital certificates.
41) How does the TLS handshake protocol ensure the authenticity of encrypted messages?
42) What are the advantages of using quantum key distribution in financial institutions?
43) Propose a solution to improve the efficiency of block chaining in cloud-based encryption systems.
44) What are the key components of a public key infrastructure (PKI) for an e-commerce company?
45) How do digital certificates contribute to the establishment of secure sessions in SSL/TLS?
46) Analyze how quantum key distribution (QKD) handles the security challenges of fiber optic networks.
47) Explain how digital certificates prevent man-in-the-middle attacks in secure communication.
48) Propose an improvement to the digital certificate issuance process to enhance trust.
49) What are the security implications of quantum cryptography in a global network?
50) How does TLS ensure the integrity and confidentiality of video conferencing sessions?