CYBERSECURITY PAPER 1

Section A

1) What is the difference between data security, privacy, and integrity?
2) Explain why passwords should be frequently updated.
3) Describe how firewalls protect computer systems from unauthorized access.
4) What is a digital signature, and how is it used in data security?
5) Define malware and list two common types.
6) How do phishing and pharming pose security risks to individuals?
7) What are access rights, and why are they important in a multi-user system?
8) How does encryption protect data from hackers?
9) Differentiate between malicious hacking and ethical hacking.
10) What are session cookies, and how do they differ from permanent cookies?
11) What is the role of biometrics in securing modern devices?
12) Explain how a virus infects a computer.
13) Describe a Trojan horse and how it differs from a virus.
14) What are logic bombs and their potential impact on a system?
15) Explain the importance of anti-spyware software.
16) How does DNS cache poisoning work in a pharming attack?
17) What is the significance of HTTPS in ensuring secure communication online?
18) How do validation checks help in maintaining data accuracy?
19) What is a checksum, and how is it used to verify data integrity?
20) Define parity checking and its use in data transmission.
21) What are the main functions of antivirus software?
22) Explain how phishing emails deceive users into sharing personal information.
23) What is the difference between a worm and a virus?
24) Describe how backups can mitigate data loss due to hardware failure.
25) How does a retina scan ensure secure access to a device?
26) What is the role of user accounts in data security?
27) Explain the function of heuristic checking in antivirus software.
28) How can password strength impact data security?
29) What is automatic repeat request (ARQ) and its role in data transmission?
30) Explain the Modulo-11 check digit algorithm.
31) What is the purpose of check digits in ISBNs and barcodes?

32)Why is it important to have parity blocks when transferring data?
33)What is the role of uninterruptible power supplies (UPS) in preventing data loss?
34)How does biometric fingerprint scanning work?
35)Describe the concept of data validation in spreadsheet applications.
36)What is a visual check, and how does it help prevent data entry errors?
37)What is the difference between data verification and validation?
38)How do pop-ups on websites potentially pose security risks?
39)What is a firewall gateway, and how does it function in network security?
40)Describe how a Trojan horse can compromise system security.
41)Explain the significance of data protection laws in ensuring data privacy.
42)What is the impact of a worm attack on network security?
43)How do heuristic checks identify potential malware?
44)Describe the process of re-transmission in ARQ when data corruption is detected.
45)Explain how parity bits are used in ensuring correct data transmission.
46)How do email phishing filters work in detecting fraudulent emails?
47)What is a security breach, and how can it be mitigated?
48)Why is regular system scanning essential for maintaining data integrity?
49)How do bots contribute to cybersecurity risks?
50)What are the key features of a strong password?

Section B

1) What is the difference between plaintext and ciphertext?
2) Define symmetric encryption.
3) What is the main drawback of symmetric encryption?
4) What is the purpose of a public key in asymmetric encryption?
5) Describe block cipher and stream cipher.
6) What is a key distribution problem in symmetric encryption?
7) How does asymmetric encryption improve security compared to symmetric encryption?
8) What is block chaining in encryption?
9) What is SSL (Secure Sockets Layer) used for?
10) Explain how Transport Layer Security (TLS) works.
11) What are the main components of TLS?
12) How does public key infrastructure (PKI) work?
13) Define digital certificate.
14) What role does a certificate authority (CA) play?
15) What are digital signatures used for?
16) Explain the term digest in cryptography.
17) How does quantum cryptography differ from classical cryptography?
18) Define quantum key distribution (QKD).
19) What is the significance of public key encryption?
20) How are session keys used in secure communication?
21) What is the difference between https and http?
22) Explain eavesdropping in the context of network security.
23) What is the role of a private key in encryption?
24) Describe the concept of non-repudiation.
25) What are the four security concerns when data is transmitted over a network?
26) What is meant by data integrity?
27) What is data privacy and why is it important?
28) How does block cipher encryption improve security?
29) Explain session caching in the context of TLS.
30) What is a digital signature and how is it formed?
31) What is a self-signed digital certificate?
32) How does asymmetric encryption ensure confidentiality?
33) What is the purpose of the handshake protocol in SSL/TLS?

34)Explain hashing algorithms used in digital signatures.
35)What is the difference between symmetric and asymmetric encryption?
36)Describe how digital certificates are acquired.
37)What is the role of the public key in a digital certificate?
38)What is a cipher in cryptography?
39)How does block chaining prevent identical ciphertext from being produced?
40)What are the advantages of using TLS over SSL?
41)How does PKI (Public Key Infrastructure) authenticate users?
42)Explain how SSL ensures data integrity.
43)What is the significance of a digital certificate in secure communication?
44)How does quantum cryptography use photons for encryption?
45)Describe how a handshake initiates communication in SSL.
46)Explain record protocol in TLS.
47)What is the role of a digest in creating a digital signature?
48)What is the process of key exchange in encryption?
49)How does a photon function in quantum cryptography?
50)What is session caching, and how does it enhance performance?