Full master list of all questions completely unified, cleaned, tagged with **appearance years** and **importance ratings (⭐)** for your **This years preparation**.

A. Cryptography & Encryption Fundamentals

1. Define cryptography. Write down the importance of cryptography. [2020, 2022] ⭐⭐⭐⭐
2. Differentiate between conventional encryption and public key encryption. [2020, 2022] ⭐⭐⭐⭐
3. What key elements must be present to build a public key cryptosystem? [2020, 2021] ⭐⭐⭐
4. State and explain the principles of public key cryptography. [2019, 2021, 2022] ⭐⭐⭐⭐⭐
5. Define encryption. Describe public key cryptographic algorithm in brief. [2018, 2020, 2021, 2022] ⭐⭐⭐⭐⭐
6. Describe public key cryptographic algorithm in brief. [2018, 2021, 2022] ⭐⭐⭐⭐
7. Differentiate between symmetric key and asymmetric key. [2018, 2020, 2021] ⭐⭐⭐
8. What is block cipher? How does Feistel cipher work in DES algorithm? [2018, 2020, 2021, 2022] ⭐⭐⭐⭐⭐
9. Draw and explain Feistel's structure for encryption and decryption. [2021, 2022] ⭐⭐⭐⭐
10. What is Feistel cipher? [2018, 2020, 2022] ⭐⭐⭐⭐
11. Describe a single round DES architecture with its operational procedure. [2018, 2020, 2021, 2022] ⭐⭐⭐⭐⭐
12. Describe general DES encryption process with diagram. Also mention some of its merits and demerits. [2019, 2020, 2021] ⭐⭐⭐⭐
13. Differentiate between AES and DES. [2020, 2022] ⭐⭐⭐⭐
14. Describe the detailed structure of AES encryption and decryption. [2020, 2022] ⭐⭐⭐⭐
15. Perform encryption and decryption using RSA algorithm for given values. [2018, 2020, 2022] ⭐⭐⭐⭐
16. Describe RSA algorithm. Which cryptosystem is related to this algorithm? [2019, 2021, 2022] ⭐⭐⭐⭐⭐
17. Describe RSA digital signature scheme with necessary diagram. [2021, 2022] ⭐⭐⭐⭐
18. Explain Diffie-Hellman key exchange algorithm. [2018, 2019, 2021, 2022] ⭐⭐⭐⭐⭐
19. State and explain middle-man attack. [2020, 2021, 2022] ⭐⭐⭐⭐⭐
20. Explain various types of cryptanalysis attack with necessary diagram. [2020, 2022] ⭐⭐⭐⭐
21. Explain cipher feedback model of operation. [2021, 2022] ⭐⭐⭐⭐
22. Describe the general structure of secure hash functions. [2021, 2022] ⭐⭐⭐⭐
23. What is hash function? Mention the requirements for hash function. [2018–2022] ⭐⭐⭐⭐⭐
24. Perform encryption and decryption using RSA algorithm (p=7, q=11, N=77, e=7, M=3). [2020, 2022] ⭐⭐⭐⭐
25. What is PKI? Is it possible to operate encryption technique without PKI? [2020, 2022] ⭐⭐⭐⭐
26. What is digital signature process for message authentication? [2021, 2022] ⭐⭐⭐⭐
27. Write down DSA algorithm. [2018–2022] ⭐⭐⭐⭐⭐
28. Describe digital signature procedure with necessary diagram. [2018, 2020, 2021, 2022] ⭐⭐⭐⭐⭐
29. Describe digital signature algorithm with block diagram. [2019, 2021, 2022] ⭐⭐⭐⭐⭐
30. What is message authentication? [2018–2022] ⭐⭐⭐⭐⭐
31. What is message authentication code (MAC)? How does secure hash algorithm work? [2019, 2021] ⭐⭐⭐
32. What is message authentication? What are the requirements for message authentication? [2018, 2021] ⭐⭐⭐

33. What is message authentication? Draw an analogy between MD5 and SHA algorithm. [2020, 2021] ⋆ ⋆ ⋆
34. Can a MAC provide authentication? Justify your answer. [2018, 2020, 2022] ⋆ ⋆ ⋆ ⋆
35. Explain the general approaches to attack a conventional encryption scheme. [2020, 2021, 2022] ⋆ ⋆ ⋆ ⋆ ⋆
36. What are the requirements for secure use of conventional encryption? [2019, 2020, 2022] ⋆ ⋆ ⋆ ⋆

B. Network Security Concepts & Attacks

37. What do you understand by Computer Security, Network Security, and Internet Security? [2018, 2020, 2021] ⋆ ⋆ ⋆
38. What do you mean by network security? [2018, 2019, 2020, 2022] ⋆ ⋆ ⋆ ⋆ ⋆
39. What do you mean by information system security? Discuss major goals of information system security. [2021, 2022] ⋆ ⋆ ⋆ ⋆
40. Draw and explain Network Security model. [2018, 2020, 2021, 2022] ⋆ ⋆ ⋆ ⋆ ⋆
41. List and briefly define the categories of security mechanism. [2020, 2022] ⋆ ⋆ ⋆ ⋆
42. What are the different types of attacks on network? Describe them with block diagram. [2018, 2019, 2020, 2022] ⋆ ⋆ ⋆ ⋆ ⋆
43. Explain different types of security attacks on messages. [2018–2022] ⋆ ⋆ ⋆ ⋆ ⋆
44. Explain different types of attacks on plain text with diagram. [2019, 2021, 2022] ⋆ ⋆ ⋆ ⋆ ⋆
45. Explain various types of non-cryptanalytic attacks with example. [2020, 2022] ⋆ ⋆ ⋆ ⋆
46. Differentiate between active and passive attacks. [2018, 2019, 2021] ⋆ ⋆ ⋆
47. “A network security can be threatened by different types of security attacks” — Explain with example. [2021, 2022] ⋆ ⋆ ⋆ ⋆
48. What is brute force attack? [2020, 2021, 2022] ⋆ ⋆ ⋆ ⋆ ⋆
49. Explain Brute-force attack and middle-man attack with example. [2021, 2022] ⋆ ⋆ ⋆ ⋆
50. Define threat and attack. [2019, 2020, 2022] ⋆ ⋆ ⋆ ⋆
51. What is cryptography? What are the cryptographic algorithms used in security purposes? [2018, 2019, 2021, 2022] ⋆ ⋆ ⋆ ⋆ ⋆
52. What is steganography? [2020, 2021, 2022] ⋆ ⋆ ⋆ ⋆ ⋆
53. What is data security? Describe OSI security services. [2019, 2020, 2022] ⋆ ⋆ ⋆ ⋆
54. What is e-commerce security? Why is it important? [2021, 2022] ⋆ ⋆ ⋆ ⋆
55. Describe key distribution process in brief. [2020, 2021, 2022] ⋆ ⋆ ⋆ ⋆ ⋆
56. What do you mean by Trusted Third Party? When is it required? [2020, 2022] ⋆ ⋆ ⋆ ⋆
57. What are the key components of a wireless network? Describe in brief. [2019, 2020, 2021, 2022] ⋆ ⋆ ⋆ ⋆ ⋆
58. Define SET. Write down the features of SET. [2018, 2019, 2020, 2022] ⋆ ⋆ ⋆ ⋆ ⋆
59. What is remote access and explain various types of technologies used for secure remote access. [2020, 2021, 2022] ⋆ ⋆ ⋆ ⋆ ⋆
60. What is VPN? Why network security policy and management are needed? [2021, 2022] ⋆ ⋆ ⋆ ⋆
61. What do you mean by Denial of Service (DoS)? Discuss different types of distributed DoS attacks. [2021, 2022] ⋆ ⋆ ⋆ ⋆
62. What is IP security? [2018–2022] ⋆ ⋆ ⋆ ⋆ ⋆
63. Describe IPSec protocol for authentication and data integrity. [2021, 2022] ⋆ ⋆ ⋆ ⋆
64. Explain the IPSec architecture. [2020, 2022] ⋆ ⋆ ⋆ ⋆
65. Differentiate tunnel mode and transport mode of IPSec. [2019, 2020, 2021, 2022] ⋆ ⋆ ⋆ ⋆ ⋆

66. What is transport layer security? Describe in brief. [2020, 2021, 2022] ⋆ ⋆ ⋆ ⋆ ⋆
67. What is firewall? Mention some merits and demerits of using firewall. [2018–2022] ⋆ ⋆ ⋆ ⋆ ⋆
68. What is Kerberos? Briefly describe the working procedure of KDC. [2019, 2020, 2021, 2022] ⋆ ⋆ ⋆ ⋆ ⋆
69. What four requirements were defined for Kerberos? [2021, 2022] ⋆ ⋆ ⋆ ⋆
70. What are the security attacks? [2018, 2020, 2022] ⋆ ⋆ ⋆ ⋆
71. What is an authentication service? Describe S-box and X.509 authentication service. [2020, 2021, 2022] ⋆ ⋆ ⋆ ⋆ ⋆
72. What are the requirements for message authentication? [2018, 2021, 2022] ⋆ ⋆ ⋆ ⋆

C. Protocols & Applications

73. Explain the secure socket layer handshake protocol action. [2021, 2022] ⋆ ⋆ ⋆ ⋆
74. List and define the parameters that define secure socket layer connection state. [2021, 2022] ⋆ ⋆ ⋆ ⋆
75. What are the benefits of using Secured Socket Layer (SSL)? [2019, 2021, 2022] ⋆ ⋆ ⋆ ⋆ ⋆
76. How does Security Socket Layer (SSL) algorithm work? [2018–2022] ⋆ ⋆ ⋆ ⋆ ⋆
77. Explain the authentication service provided by X.509 certificate. [2018–2022] ⋆ ⋆ ⋆ ⋆ ⋆
78. Why is certificate authority required and how does it work? [2019, 2020, 2021, 2022] ⋆ ⋆ ⋆ ⋆ ⋆
79. What is Secure Shell (SSH)? For what purpose is it useful? [2021, 2022] ⋆ ⋆ ⋆ ⋆
80. Define certificate authority. [2019, 2021, 2022] ⋆ ⋆ ⋆ ⋆
81. What is secure electronic transaction? Mention its features. [2020, 2021, 2022] ⋆ ⋆ ⋆ ⋆ ⋆
82. Write short notes on secure electronic transaction and web security. [2019–2022] ⋆ ⋆ ⋆ ⋆ ⋆
83. What is PKI? Is it possible to operate encryption technique without PKI? [2020, 2022] ⋆ ⋆ ⋆ ⋆
84. What is remote access? Explain various technologies used for secure remote access. [2020, 2021, 2022] ⋆ ⋆ ⋆ ⋆ ⋆

D. Short Notes

1. Firewall [2018–2022] ⋆ ⋆ ⋆ ⋆ ⋆
2. Digital Immune System [2018–2022] ⋆ ⋆ ⋆ ⋆ ⋆
3. E-mail Security [2020, 2021, 2022] ⋆ ⋆ ⋆ ⋆ ⋆
4. Feistel Cipher [2020, 2022] ⋆ ⋆ ⋆ ⋆
5. RSA Algorithm [2020, 2021, 2022] ⋆ ⋆ ⋆ ⋆ ⋆
6. IPSec Architecture [2018–2022] ⋆ ⋆ ⋆ ⋆ ⋆
7. White Box Cryptography [2018–2022] ⋆ ⋆ ⋆ ⋆ ⋆
8. S/MIME [2018–2022] ⋆ ⋆ ⋆ ⋆ ⋆
9. SSL [2018–2022] ⋆ ⋆ ⋆ ⋆ ⋆
10. UNIX Password Scheme [2018–2022] ⋆ ⋆ ⋆ ⋆ ⋆
11. Key Management System [2019–2022] ⋆ ⋆ ⋆ ⋆ ⋆
12. Generic Encryption [2019–2022] ⋆ ⋆ ⋆ ⋆ ⋆
13. Web Security Threat [2019–2022] ⋆ ⋆ ⋆ ⋆ ⋆
14. Block Chain [2019–2022] ⋆ ⋆ ⋆ ⋆ ⋆
15. SSN Protocol [2021, 2022] ⋆ ⋆ ⋆ ⋆
16. Public Key Infrastructure (PKI) [2020, 2021, 2022] ⋆ ⋆ ⋆ ⋆ ⋆
17. Network Security Services [2021, 2022] ⋆ ⋆ ⋆ ⋆
18. Authentication Service (X.509) [2018–2022] ⋆ ⋆ ⋆ ⋆ ⋆

19. Tunnel Mode and Transport Mode of IPSec [2019–2022] ⭑ ⭑ ⭑ ⭑ ⭑

✅ **Total Questions:** 109 🏆 **Tip for 2023:** Focus heavily on ⭑ ⭑ ⭑ ⭑ ⭑ questions — these are most likely to repeat, especially those from **X.509, SSL, RSA, Firewall, Kerberos, IPSec, DES, AES, PKI, SET, and Hash Functions.**