1. Define data access control.
2. What is disaster on network?
3. What is open source concept?
4. What is cryptography?
5. Define operational issues on computer security.
6. What is link encryption?
7. Define MD5.
8. Define worms.
9. What is spoofing?
10. What is cryptanalysis?
11. How computer security differs from network security?
12. What do you mean by software vulnerabilities?
13. Why passive attack is difficult to detect? Explain
14. What do you mean by trusted system?
15. What do you mean by digital certificate?
16. What do you mean by malicious code? Give examples
17. What is hash function?
18. What is reply attack?
19. What do you mean by authentication protocols?
20. List advantages and disadvantages of open source software.
21. What do you mean by computer security?
22. List security threats.
23. What do you mean by digital signature?
24. What are the security goals?
25. What is Trojan horse?
26. What is a Bastion host?
27. What is hash function?
28. What do you mean by a trusted system?
29. Define the term session key.
30. List advantages of open source code.
31. How does network security differ from computer security?
32. Differentiate between active and passive attacks.
33. What do you mean by direct digital signature?
34. What are the security services?
35. What do you mean by Trojan horse attack?
36. Define VPN.
37. How is message digest generated?
38. What do you mean by trusted operating system?
39. What do you mean by logic bomb?
40. Define IPSec.
41. What do you mean by Trojan horse?

42. What are security threats?
43. Define digital certificate.
44. What is security policy?
45. Define cipher text.
46. What is a Bastion host?
47. What is the use of message authentication code?
48. What do you mean by a trusted system?
49. Define cyber law.
50. List features of open source software.
51. Define security policies.
52. What is digital crime?
53. Define the term threat.
54. What is disclosure on network?
55. What is spoofing?
56. Define public key.
57. What is message digest?
58. What is cryptology?
59. Define biometric security.
60. Define the term IPS.
61. What is certificate of authority? Differentiate it with digital certificate. Discuss about X.509 certificate. Are there any possibilities of using digital signature in Nepal?
62. What is web security? Write the use of SSL with its structure. Discuss about the PGP and S/MIME.
63. What is DES Algorithm? Define its use and role for security management.
64. What is malicious program? Explain its types
65. What is UNIX? List some flavors of UNIX. Discuss the security issues.
66. What is SET? Explain with operational process diagram.
67. What is Open Source Code? Explain some flavors of UNIX. Discuss them in terms of security issues.
68. What is firewall? Explain its use and types.
69. Differentiate between link and point to point encryption with example.
70. Write short notes on:
    a. Password management system
    b. Double and Triple DES
    c. Hash function
    d. VeriSign
    e. Triple-DES
    f. IT Policy of Nepal (Mission, Vision and Action plan)
    g. Secure Electronic Transaction (SET)
    h. RSA Algorithm.

i. Data Encryption Standard (DES)
j. ETO 2061
k. Kerberos V4
l. X.509
m. IT policy of Nepal.
n. Kerberos.
o. Triple-DES.
p. Types of firewall
q. Intrusion Response
r. X.509
s. VeriSign
t. Hash function
u.

71. What is dual signature and how is it formed? Explain the payment processing steps used in SET.
72. What is firewall? What are the different types of firewall? Explain three different ways of firewall configuration.
73. What is an encryption? Explain the various types of encryption with example.
74. Discuss various methods of computer security.
75. What do you mean by IDS? Explain the rule-based intrusion detection system.
76. What is Open Source Code? Explain some flavors of UNIX. Discuss them in terms of security issue.
77. What is malicious logic? Discuss its types.
78. Differentiate between transport and tunnel mode.
79. Why PGP is popular? How does it provide authentication services? Explain.
80. What is hash function? Define message digest? Explain its use on security.
81. What is IPSec? Explain its architecture.
82. What is digital signature? Explain its types with examples.
83. How is UNIX perceived by different communities with different flavor? How will you advocate the use of open source in our own country?
84. What is malicious logic? Discuss its types.
85. Discuss the structure of virus. Also explain briefly the generations of antivirus.
86. Discuss various types of security policies. List the main strategies and action plans of IT policy 2000 Nepal. Discuss the role of Electronic Transaction Act 2061 for digital data processing.
87. What are authentication protocols? Explain about mutual authentication with the concept of replay attacks, symmetric and public key cryptography approach.
88. What is e-mail security? How PGP provides authentication service in email security? Explain.
89. What is SET? What are the key features of SET? Briefly explain the role of participants of the SET system.
90. Write RSA Algorithm and verify the algorithm for the given message (M) = 12, and two prime numbers p = 5 and q = 7.

91. What do you mean by PGP? How does PGP provide the authentication and confidentiality services in e-mail security? Explain.
92. What are the types of firewall? How does packet filtering firewall work? Explain.
93. Differentiate between DSS approach and RSA approach.
94. What is IDS? Explain the rule-based intrusion detection system.
95. What is computer virus? Explain the types of virus.
96. Define system security. Explain the UNIX system security.
97. What are different types of security policies? Explain the commercial security policy with an example.
98. What are web threats? Explain SSL handshake protocol with example.
99. What is PGP? What are the PGP Services? How PGP provide the confidentiality and authentication services in email system. Explain.
100. What do you mean by link encryption? How link encryption differs from end-to-end encryption? Explain with example.
101. What are security threats? Explain with examples.
102. Differentiate between direct digital signature and Arbitrated digital signature.
103. Compare IPSec with VPN.
104. What is UNIX? Why open source code programs are popular? Write the some general security rule.
105. What is IPS and IDS? Discuss some methods for intrusion detection.
106. What is Firewall? Explain its types with examples.
107. What is X.509 certificate? List some areas where X.509 certificates are used along with the details of the certificate.
108. What is an encryption? Write about its types with example.
109. Define cyber law. Write about the process of getting license as a Certification Authority according to Electronic Transaction Act of Nepal.
110. Define security and its components. What are the operational issues that should be considered to get full benefits from the security policy and corresponding mechanisms?
111. What would a secure email contain? Explain how PGP sends a signed and encrypted message.
112. In which scenario does Kerberos finds its use? Draw a neat diagram to illustrate the scenario. Also write about Ticket Granting Service and Authentication Serer. You may support your answer with certain dialogues.
113. List the types of malicious code. Compare macro virus, polymorphic virus, Boot sector virus and zombie.
114. As a technical person how will you define UNIX? Write about the password management in UNIX.
115. How can security be provided in transport layer? Explain how it works in brief.
116. What is e-mail security? Explain the PGP Services in details.

117. Write RSA algorithm. Show all the steps of the algorithm and verify the algorithm for the given message (M) = 9, and two prime numbers p=7 and q=11.

118. What are the web security approaches? Explain the SSL record protocol services and operations with example.

119. What do you mean by payment processing? Explain the payment processing for purchase requests.

120. What are the applications of firewalls? How firewall protect network? Explain.

121. What is Kerberos? Explain the steps of Kerberos version 4.

122. What is IDS? Explain the rule-based intrusion detection system.

123. What do you mean by malicious program? Explain the taxonomy of the malicious program.

124. What are the circumstances for certifying authority suspend and revoke the certificate according to ETA 2063 (2008)?

125.