Council for Technical Education and Vocational Training

Office of the Controller of Examinations

Sanothimi, Bhaktapur

Regular/Back Exam – 2082 Shrawan/Bhadra

Program:	**Diploma in Computer Engineering**	**Full Marks: 80**
Year/Part:	**III/II (2022)**	**Pass Marks: 32**
Subject:	**Information Security**	**Time: 3 hrs.**

Candidates are required to give their answers in their own words as far as practicable. The figures in the margin indicate full marks.

Attempt any EIGHT Questions.

1. a. What is information security? Explain different security mechanism in information security. (1+5)
   b. Differentiate between symmetric and asymmetric cryptography. (4)
2. Explain the implementation of Advance Encryption Standard (AES). (10)
3. a. Explain conventional substitution and transposition cipher. (5)
   b. Write about authentication and digital signature. (5)
4. What is application security? Describe mobile application security and cloud security. (2+4+4)
5. Define program security. Explain the concept of salani attack and how it can be prevented. (4+6)
6. What is an intrusion detection system? Explain. How does it differ from intrusion protection system? (5+5)
7. a. What is firewall? Explain e-mail security. (2+3)
   b. Discuss the importance of database security. (5)
8. Explain legal, privacy and ethical issues in computer security. (10)
9. Write short notes on: (any **TWO**) (5+5)
   a) Security planning
   b) Multi level security
   c) Steganography
   d) Man-in-the-middle attack

Good Luck !

Council for Technical Education and Vocational Training

Office of the Controller of Examinations

Sanothimi, Bhaktapur

Regular Exam – 2081 Kartik/Mangsir

Program:	**Diploma in Computer Engineering**	**Full Marks: 80**
Year/Part:	**III/II (2022)**	**Pass Marks: 32**
Subject:	**Information Security**	**Time: 3 hrs.**

Candidates are required to give their answers in their own words as far as practicable. The figures in the margin indicate full marks.

Attempt any EIGHT questions.

1. Define 'vulnerability' and 'attack' in information security. Explain different security mechanisms in information security. [3+7]
2. What is cryptography? Explain conventional substitution and transposition cipher. [2+8]
3. Differentiate between symmetric and asymmetric cryptography. Explain the implementation of Advanced Encryption Standard (AES). [2+8]
4. Define the terms 'authentication' and 'digital signature'. Explain the working of key management Kerberos. [8+2]
5. What is application security? Describe mobile application security and cloud security. [2+8]
6. What do you mean by incomplete mediation? Elaborate on your understanding of trapdoors and covert channels in the context of program security. [3+7]
7. Define network security. Describe the intrusion detection system and its types. [2+8]

8. What do you mean by database security? Explain the rights of employees and employers in the context of security administration. [10]
9. Write short notes on: (any **TWO**) [2×5]
   a. Software failure
   b. Multilevel database
   c. Honeypots
   d. Intrusion Protection System (IPS)

Good Luck !