Tribhuvan University

Faculty of Humanities & Social Sciences

OFFICE OF THE DEAN

2024

Bachelor in Computer Applications
Course Title: Information Security
Code No: CACS 459
Semester: VIII

Full Marks: 60
Pass Marks: 24
Time: 3 hours

Candidates are required to answer the questions in their own words as far as possible.

Group B

Attempt any SIX questions. [6×5 = 30]

2. What is security services? Explain four fundamental security design principle. [1+4]
3. What do you mean by transportation cipher? Decrypt the cipher text UIESTNVRIY using the Rail fence cipher using rail size is 2. [2+3]
4. What is Euler's totient function? Find multiplicative inverse of 87 in Z_{100} using Extended Euclidean algorithm. [1+4]
5. What is Abelian group? Find whether 561 is prime or not using Miller-Rabin algorithm. [2+3]
6. What is Password aging? Explain process of biometric authentication. [1+4]
7. What is malicious software? How worms are different from Trojan horses? [1+4]
8. What is security Audit? Explain the architecture of security auditing. [1+4]

Group C

Attempt any TWO questions. [2×10 = 20]

9. How key generation, encryption and decryption is done in RSA. In a RSA cryptosystem, given p=5 and q=19, determine private key, public key and perform encryption and decryption for the message m=4. [5+5]
10. Explain properties of hash functions. How hash value is generated using SHA-1 algorithm, explain with suitable diagram. [3+7]
11. What is difference between Access Control List (ACL) and Access Control Matrix (ACM)? Explain five services provided by PGP protocol to secure email. [5+5]