Tribhuvan University
Institute of Science and Technology
2067

Bachelor Level/ Third Year/ Fifth Semester/ Science — Full Marks: 60
Computer Science and Information Technology (CSc. 313) — Pass Marks: 24
(Cryptography) — Time: 3 hours

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

Attempt all the questions.
Answer the following questions in short (Any Five). (5 × 2 = 10)

1. List and briefly define types of cryptanalytic attacks based on what is known to the attacker.
2. The larger the size of the key space, the more secure a cipher? Justify your answer.
3 Explain the concepts of diffusion and confusion as used in DES.
4. What are the characteristics of a stream cipher?
5. How afraid should you be of viruses and worms?
6. What do you mean when we say that a pseudorandom number generator is cryptographically secure?
7. How many rounds are used in AES and what does the number of rounds depend on?

8 a. The notation Zn stands for the set of residues. What does that mean? Why is Zn not a finite field? Explain. (5)
b. Find the multiplicative inverse of each nonzero element in Zn. (5)

OR
Complete the following equalities for the numbers in GG(2):
1+1 = ?
1-1 = ?
-1 = ?
1*1 = ?
1 * -1 = ?
9. a) What are the steps that go into the construction of the 16 × 16 S-box lookup table for AES algorithm? (5)
b) In RSA algorithm, what is necessary condition that must be satisfied by the modulus n chosen for the generation of the public and private key pair? Also, is the modulus made public? (5)

OR

10. How is the sender authentication carried out in PGP? (5)
11. a) What sort of secure communication applications is the Kerberos protocol intended for? Explain. (5)
b) What is Fermat's Little Theorem? What is the totient of a number? (5)

12. a) Miller-Rabin test for primality is based on the fact that there are only two numbers in Zp that when squared give us 1. What are those two numbers? (5)

OR

What is discrete logarithm and when can we define it for a set of numbers? (5)
b) What is the Diffie-Hellman algorithm for exchanging a secret session key? (5)
13. a) We say that SSL/TLS is not really a single protocol, but a stack of protocols. Explain. What are the different protocols in the SSL/TLS stack? (5)
b) What is the relationship between "hash" as in "hash code" or "hashing function" and "hash" as in a "hash table"? (5)