Tribhuvan University
Institute of Science and Technology
2068

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.

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

a. All classical ciphers are based on symmetric key encryption. What does that mean?
b. What makes Vigenere cipher more secure than say, the Playfair cipher?
c. AES is a block cipher. What sized blocks are used by AES?
d. When does a set become a group?
e. What is the difference between the notation a mod n and the notation a ≡ b (mod n)?
f. What is the difference between a virus and a worm?
g. How do you define a prime number? When are two numbers A and B considered to be coprimes?

2. a) What do you mean by a "Feistel Structure for Block Ciphers"? Explain. (5)
b)Divide 23x2 + 4x + 3 by 5x + c, assuming that the polynomials are over the field Z7. (5)

OR

What are the asymmetries between the modulo n addition and modulo n multiplication over Zn?

3. a) Describe the ''mix columns'' transformation that constitutes the third step in each round of AES. (5)
b)What is the difference between algorithmically generated random numbers and true random numbers? (5)

4. a) Miller-Rabin algorithm for primality testing is based on a special decomposition of odd numbers. What is that? Explain (5)
b)In RSA algorithm, the necessary condition for the encryption key e is that it be coprime to the totient of the
modulus. But, in practice, what is e typically set to and why? (5)

5. a) What is meant by the strong collision resistance property of a hash function? (5)
b)How can public-key cryptography be used for document authentication? (5)

OR

What seems so counterintuitive about the counter mode (CTR) for using a block cipher?

6. a) What is the role of the SSL Record Protocol in SSL/TLS? Explain. (5)

OR

How many layers are in the TCP/IP protocol suite for internet communications? Name the layers. Name some of the protocols in each layer.
b)What does PGP stand for? What is it used primarily for? And what are the five services provided by the PGP protocol?