Tribhuvan University
Institute of Science and Technology
2070

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. Difference between monoalphabetic substitution ciphers and polyalphabetic substitution ciphers.
b. What are the two building blocks of all classical ciphers?
c. Des encryption was broken in 1999. Does that make this an unimportant cipher? Why do you think that
happened?
d. What does a field have, that an integral domain does not? Why is Zn not an integral domain/
e. Does a field contain a multiplicative inverse for every element of the field?
f. What are the four steps that are executed in a single round of AES processing?
g. What is a hash code? Why can a hash function not be used for encryption?

2. a) What is Euclid's algorithm for finding the GCD of two numbers? Explain. (5)

OR

What is Euler's theorem? What is the totient of a prime number?
b)Calculate the result of the following if the polynomial are over GF(2): (5)
(x4 + x2 + x + 1) + (x3+1)
(x4 + x2 + x + 1) – (x3+1)
(x4 + x2 + x + 1) x (x3+1)
(x4 + x2 + x + 1) / (x3+1)

3. a) Let's go back to the first step of processing in each round of AES. How does one look up the 16x16 S-box table for the byte-by-byte substitution? (5)
b)What do you mean by man-in middle attack? Is man-in-middle attack possible in Deffie-Hellman? How?(5)

4. a) There are two aspects to a secure communication link: authentication and confidentiality. How do you understand these two words? Does the Kerberos protocol give us both? (5)
b)Miller-Rabin test says that if a candidate integer n is prime, it must satisfy one of two special conditions. What are those two conditions? (5)

5. a) How do you create public and private keys in the RSA algorithm for public-key cryptography? (5)

OR

What are the notions Public Key Ring and Private Key Ring in PGP?
b)What is the difference between a connection and a session in SSL/TLS? Can a session include multiple connections? Explain the notions "connection state" and "session sate" in SSL/TLS. What security features apply to each? (5)

6. a) How hash function differ from MAC? Discuss how data integrity can be achieved from either of them. (5)
b)What is a certificate and why are certificates needed in public key cryptography? (5)