Tribhuwan University
Institute of Science and Technology
2073

Bachelor Level / fifth-semester / Science — Full marks: 60
Computer Science and Information Technology(CSC316) — 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 questions.

1. Answer the following questions in short (Any Five).

a. Why the procedure used during encryption-decryption process of DES is often known as managing or criss-crossing?

b. What do you mean by reply attacks? Describe with an example.

c. Find Multiplicative inverse of each nonzero element in Z6.

d. Mention the image resistive properties of Hash functions.

e. How rabbits and bacterium can be malicious to a secure system?

f. What do you mean by one-time signatures?

g. How security at application layer can be achieved?

2. a) Describe Extended Euclidean Algorithm. Use this algorithm to test whether any two number n1, n2 are co-prime or not?

b) How IDEA operates on 64-bit blocks using 128-bit key? Describe each round of operations that IDEA follows to generate ciphertext of a 64-bit input message block.

3. a) How padding is done in SHA-1? How 160-bit of hash value is generated by taking an input message of variable size using SHA-1?

b) Construct a playfair matrix with the key *EXAMPLE*. Using this matrix encrypt the message "Hide the Gold".

4. a) In a RSA system, a user has chosen the primes 5 and 19 to create a key pair. The public key is (5, n) and the private key is (d, n). Decide the private key (d, n). Show encryption and decryption process for the message "Drogba".

b) How SSL Record Protocol provides security in Secure Socket Layer Protocol?

5. a) Why hash functions are known to be best option for digital signature schemes? How about the use of encryption paradigms for generating digital signatures?

b) Encrypt the message "NANI" using the Hill cipher with the key $\begin{pmatrix} 4 & 5 \\ 6 & 9 \end{pmatrix}$**. Show your calculations and the result.**

6. a) How Man-In-Middle attack is possible in Deffie-Hellman Algorithm. Support answer with a numerical computation. Chose the required parameters with your own assumptions.

b) Define authentication system. How hardware based challenge response systems can be used as authentication approach.

