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 answer in their own words as for 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. List and briefly define types of cryptanalytic attacks based on what is known to the attacker.
   b. The larger the size of the key space, the more secure a cipher? Justify your answer.
   c. Explain the concepts of diffusion and confusion as used in DES.
   d. What are the characteristics of a stream cipher?
   e. How afraid should you be of viruses and worms?
   f. What do you mean when we say that a pseudorandom number generator is cryptographically secure?
   g. How many rounds are used in AES and what does the number of rounds depend on?

2.a) The notation $\mathbf{Z_n}$ stands for the set of residues. What does that mean? Why is $\mathbf{Z_n}$ not a finite field? Explain. (5)

2.b) Find the multiplicative inverse of each nonzero element in $\mathbf{Z_n}$. (5)

OR

Complete the following equalities for the numbers in GG(2):

1+1 = ?
1-1 = ?
-1 = ?
1*1 = ?
1*-1 = ? (5)

3.a) What are the steps that go into the construction of the 16 × 16 S-box lookup table for AES algorithm? (5)

3.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

How is the sender authentication carried out in PGP? (5)

4.a) What sort of secure communication applications is the Kerberos protocol intended for? Explain. (5)

4.b) What is Fermat's Little Theorem? What is the totient of a number? (5)

5.a) Miller-Robin test for primality is based on the fact that there are only two numbers in $\mathbf{Z_p}$ 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)

5.b) What is the Diffie-Hellman algorithm for exchanging a secret session key? (5)

6.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)

6.b) What is the relationship between "hash" as in "hash code" or "hashing function" and "hash" as in a "hash table" ? (5)

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 answer in their own words as for as practicable.
The figures in the margin indicate full marks.

Attempt all the questions.

1. Answer the following questions in short **(Any Five)**. (5 X 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 $a \equiv b \pmod{n}$?
   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)

2.b) Divide $23x^2 + 4x + 3$ by $5x + c$. assuming that the polynomials are over the field $\mathbf{Z}_7$. (5)

OR

What are the asymmetries between the modulo n addition and modulo n multiplication over $\mathbf{Z}_n$? (5)

3.a) Describe the "mix columns" transformation that constitutes the third step in each round of AES. (5)

3.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)

4.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)

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.

6.b) What does PGP stand for? What is it used primarily for? And what are the five services provided by the PGP protocol? (5)

Tribhuvan University
Institute of Science and Technology
2069
✡

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 answer in their own words as for as practicable.
The figures in the margin indicate full marks.

Attempt all the questions.

1. Answer the following questions in short (**any five**): (5 x 2=10)

   a. How monoalphabetic substitution differs from polyalphabetic. Briefly define with suitable example.
   b. What are the components of authentication system? Give an example of authentication system.
   c. What do you mean by avalanche effect?
   d. How chosen plaintext attack differs from chosen ciphertext attack?
   e. What do you mean by multiplicative inverse? Find multiplicative inverse of each nonzero elements in Z_{11}.
   f. Even though we have a strong algorithm like 3-DES, still AES is preferred as a reasonable candidate for long term use. Why?
   g. Give an example for a situation that compromise in confidentiality leads to compromise in integrity.

2.a) Consider a Deffie-Hellman scheme with a common prime p = 11 and a primitive root g = 2.

   i. Show that 2 is a primitive root of 11.
   ii. If user A has public key $Y_a = 9$, what is A's private key X_a?
   iii. If user B has public key $Y_b = 3$, what is shared key K, shared with A. (2 X 3=6)

2.b) Construct a playfair matrix with the key "*KEYWORD*". Using this matrix encrypt the message "*WHY DON'T YOU*". (4)

3.a) How Trojan horse differs from viruses? Discuss about possible types of Trojan horses. (2+3)

3.b) Does Kerberos protocol ensures authentication and confidentiality in secure system? Explain. (5)

4.a) How Hash functions differ from MAC? Given a message m, discuss what arithmetic and logical functions are used by MD4 to produce message digest of 128 bits. (2+4)

4.b) Discuss the five principle services provided by PGP protocol. (4)

5.a) What is the purpose of S-Boxes in DES? Prove that DES satisfies complementation property. (6)

5.b) Given the plaintext "ABRA KA DABRA", compute the ciphertext for (4)

i. The Ceaser cipher with key = 8
ii. The Railfence cipher with rails = 3

6.a) What do you mean by digital signature? How digital signatures can be enforced using encryptions? Illustrate with an example. (1+5)

6.b) Determine whether the integers 105 and 294 are relatively prime. Explain your answer using Euclidean algorithm. (4)