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.

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)
   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 = ?

3. 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

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

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

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 $23x^2 + 4x + 3$ 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 **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? (5)

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 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. 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 $\mathbf{Z_{11}}$.
   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. (3x2=6)
   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)
   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)
   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)
   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)
   b) Determine whether the integers 105 and 294 are relatively prime. Explain your answer using Euclidean algorithm. (4)

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 $\mathbf{Z_n}$ 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)

Institute of Science and Technology
2071
✡

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. Suppose a key logger program intercepts user password and is used to modify the user account. Now, justify whether it's a violation of confidentiality, integrity, or availability or some of combination of them.
   b. How zombies differ from logic bombs?
   c. Mention the advantages of using stream ciphers over block ciphers.
   d. What does Euler Totient Theorem states? What is the value of Totient(15)?
   e. Differentiate session keys from interchange keys.
   f. How Message Authentication Codes differ from Hash Functions?
   g. Briefly describe SubBytes and ShiftRows in AES.

2. a) In public key cryptosystem, each of the communicating parties, in general, should know the public keys of each other before attempting security encryptions. How this can be achieved? Write a Public Key Authority Protocol for Public-key distribution among any two users. [4]
   b) How Kerberos Version 4 differs from Kerberos Version 5? How once per type of service approach is ensured by Kerberos Protocol. [6]

3. a) Configure a Vigenere table for the characters from A-H. Use the table to encrypt the text DAD CAFE EACH BABE using the key FADE. [4]
   b) Mention the details of logical operations used in MD4. How the Majority function in Pass 1 of MD4 works? [6]

4. a) Encrypt the message "help" using the Hill cipher with the key $\begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix}$. Show your calculations and the result. [4]
   b) What do you mean by arbitrated digital signature? How signatures are generated using Digital Signature System? [6]

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)

Institute of Science and Technology
2072
✡

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. What does Euler Totient function means? What will be the value of PHI (119)?
   b. What properties does a good hash function should have?
   c. What is the purpose of S-Box in DES?
   d. Define each of the terms confidentiality, integrity and availability.
   e. What do you mean by primitive root of a prime number p? Is 3 a primitive root of 7?
   f. Describe the concept behind public key infrastructure.
   g. What are the possible phases that a virus can go through, during its life cycle?

2. a) In a RSA system, a user has chosen the primes 5 and 19 to create a key pair. The public key is {e=5, n=?} and the private key is {d=?, n=?}. Decide the private key {d, n}. Show encryption and decryption process for the message "TOGA" [6]
   b) Encrypt the message "MEET ME TONIGHT" using the Hill cipher with the key $\begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}$. Show your calculations and the result. [4]

3. a) Differentiate between SSL Session and SSL Connection. How SSL Record protocol provides confidentiality and message integrity. [2+3]
   b) What basic arithmetic and logical functions are used in SHA-1? [5]

4. a) Briefly describe about MixColumns and AddRoundKey stages in AES. How many bytes in a state are affected by ShiftRows round? [5+1]
   b) List the participants of Secured Electronic Transaction (SET). Discuss the key features of SET. [4]

5. a) In which situation using Kerberos system seem to be good? Describe what the major components of Kerberos system are. [2+4]
   b) Given the plaintext "LOST IN PARADISE", compute the ciphertext for
      i. The Ceaser cipher with key = 5
      ii. The Railfence cipher with rails = 4 [4]

6. a) Differentiate between direct digital signature and arbitrated digital signature. How signing and verifying process is done in Digital Signature Standard. [2+4]
   b) What do you mean by Man-in-Middle attack? Is man in middle attack possible in Diffie-Hellman algorithm for key exchange? How? [4]

Institute of Science and Technology
2073
✡

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. 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? [4]
   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. [6]

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? [6]
   b) Construct a playfair matrix with the key *EXAMPLE*. Using this matrix encrypt the message "Hide the Gold" [4]

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". [6]
   b) How SSL Record Protocol provides security in Secure Socket Layer Protocol? [4]

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? [6]
   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. [4]
   c) 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 [6]
   d) Define authentication system. How hardware based challenge response systems can be used as authentication approach. [4]