Code No: **R1641051** **R16** **Set No. 1**

IV B.Tech I Semester Regular Examinations, October/November - 2019

CRYPTOGRAPHY AND NETWORK SECURITY

(Common to Computer Science and Engineering and Information Technology)

Time: 3 hours **Max. Marks: 70**

Question paper consists of Part-A and Part-B
Answer ALL sub questions from Part-A
Answer any FOUR questions from Part-B
*****

PART–A *(14 Marks)*

1. a) Find the particular and the general solutions to the following linear Diophantine equation $19x + 13y = 20$. [3]
   b) A message has 2000 characters. If it is supposed to be encrypted using a block cipher of 64 bits, find the size of the padding and the number of blocks. [3]
   c) Define Euler's Phi-function. Find the value of $\Phi(240)$. [2]
   d) Write any two differences between message integrity and message authentication. [2]
   e) List limitation of simple electronic mail. [2]
   f) Define security association and explain its purpose. [2]

PART–B *(4x14 = 56 Marks)*

2. a) Explain security services and security mechanisms. [8]
   b) State and prove the properties of modular arithmetic binary operations. [6]

3. a) Distinguish between a Feistel and a non-Feistel block cipher. [4]
   b) Explain the DES algorithm in detail. [10]

4. (a) Explain the Miller – Rabin test for primatlity.
   (b) Explain the ElGamal cryptosystem method.
   (c) In ElGamal, what happens if C_1 and C_2 are swapped during the transition. [14]

5. a) Explain different schemes of iterated Hash functions. [6]
   b) Discuss about digital signature. [8]

6. a) What is PGP? Explain different packet formats of PGP. [7]
   b) Explain SSL architecture. [7]

7. a) What is IPSec? Explain the operation of IPSec in transport mode and tunnel mode. [7]
   b) Explain ISAKMP protocol. [7]

Code No: **R1641051** **R16** **Set No. 2**

IV B.Tech I Semester Regular Examinations, October/November - 2019

CRYPTOGRAPHY AND NETWORK SECURITY

(Common to Computer Science and Engineering and Information Technology)

Time: 3 hours **Max. Marks: 70**

Question paper consists of Part-A and Part-B
Answer ALL sub questions from Part-A
Answer any FOUR questions from Part-B
*****

PART–A *(14 Marks)*

1. a) Let us assign numeric values to the uppercase alphabet (A=0, B=1, . . ,Z=25). We can do modular arithmetic on the system using modulo 26
   (i) What is (A+N) mod 26 in this system?
   (ii) What is (C-10) mod 26 in this system? [3]
   b) Define a P-box and list its three variations. Which variation is invertible? [2]
   c) Define Fermat's Little theorem. Find the result of 6^{10} mod 11. [2]
   d) Give any two differences between MDC and a MAC. [2]
   e) List the four protocols defined in SSL. [2]
   f) Define ISAKMP and its relation to IKE. [3]

PART–B *(4x14 = 56 Marks)*

2. a) What is a Security attack? Explain taxonomy of attacks with relation to security goals [6]
   b) Explain the extended Euclidean algorithm. Find gcd(a, b) and the values of s and t for given a=161 and b=28 [8]

3. a) Define and explain the properties of the following algebraic structures:
   (i) Groups (ii) Rings (iii) Fields [9]
   b) What is a stream cipher? Define the feedback shift register and list the two variations used in stream ciphers. [5]

4. (a) Explain the Pollard rho Method for factorization.
   (b) Explain the RABIN cryptosystem in detail.
   (c) Using RABIN cryptosystem with P=47 and q=11, Encrypt P= 17 to find the ciphertext. [14]

5. (a) Explain Merkle-Damgard scheme.
   (b) Explain characteristics of Secure hash Algorithms.
   (c) Explain SHA-512 block diagram and compression function. [14]

6. a) Explain S/MIME protocol. [8]
   b) Explain Record Protocol of SSL. [6]

7. What is IPSec? Explain AH and ESP protocols of IPsec. [14]

Code No: **R1641051** **R16** **Set No. 3**

IV B.Tech I Semester Regular Examinations, October/November - 2019

CRYPTOGRAPHY AND NETWORK SECURITY

(Common to Computer Science and Engineering and Information Technology)

Time: 3 hours **Max. Marks: 70**

Question paper consists of Part-A and Part-B
Answer ALL sub questions from Part-A
Answer any FOUR questions from Part-B

*****

PART–A *(14 Marks)*

1. a) Find the particular and the general solutions to the following linear Diophantine equation $25x + 10y = 15$. [3]
   b) Define a product cipher and list the two classes of product ciphers. [2]
   c) Define the Euler's totient function and its applications. [2]
   d) List the security services provided by a digital signature. [2]
   e) Name three types of messages in PGP and their purposes. [2]
   f) Define security policy and explain its purpose with relation to IPsec. [3]

PART–B *(4x14 = 56 Marks)*

2. a) Explain the Cryptography and Steganography security techniques. [8]
   b) Explain the Euclidian algorithm. Find the greatest common divisor of 25 and 60 using this. [6]

3. (a) List the parameters of three AES versions
   (b) Compare the substitution in DES and AES. Why do we have only one substitution table (S-table) in AES , but several in AES?
   (c) Compare the permutations in DES and AES. Why do we need expansion compression permutations in DES, but not in AES?
   (d) Compare the round keys in DES and AES. In which cipher is the size of the round key the same as the size of the block? [14]

4. (a) Define the Chinese remainder theorem and its applications.
   (b) Find the value of x for the following sets of congruence using Chinese remainder theorem $x \equiv 2 \bmod 7$ and $x \equiv 3 \bmod 9$.
   (c) Explain the Elliptic Curve Cryptosystem in detail. [14]

5. a) Explain RSA digital signature scheme. [7]
   b) Explain Diffie-Hellman Key agreement protocol for a symmetric key agreement. [7]

6. a) Make a table to compare and contrast the symmetric-key cryptographic algorithms, asymmetric-key cryptographic algorithms, hash algorithms and digital algorithms used in PGP and S/MIME. [8]
   b) Explain Cryptographic Parameter Generation in SSL. [6]

7. a) Explain Authentication Header protocol of IPSec. [7]
   b) Explain Security Policy of IPSec. [7]

Code No: **R1641051** **R16** **Set No. 4**

IV B.Tech I Semester Regular Examinations, October/November - 2019

CRYPTOGRAPHY AND NETWORK SECURITY

(Common to Computer Science and Engineering and Information Technology)

Time: 3 hours **Max. Marks: 70**

Question paper consists of Part-A and Part-B
Answer ALL sub questions from Part-A
Answer any FOUR questions from Part-B

*****

PART–A *(14 Marks)*

1. a) Let us assign numeric values to the uppercase alphabet (A=0, B=1, . . , Z=25). We can do modular arithmetic on the system using modulo 26
   (i) What is (A+6) mod 26 in this system?
   (ii) What is (C-10) mod 26 in this system? [3]
   b) Define an S-box and mention the necessary condition for an S-box to be invertible. [2]
   c) Define a trapdoor one-way function and explain its use in asymmetric-key cryptography. [3]
   d) Define the first and second criterion for a cryptographic hash functions . [2]
   e) List the services provided by SSL. [2]
   f) Distinguish two modes of IPsec. [2]

PART–B *(4x14 = 56 Marks)*

2. a) Define the three security goals. Explain the actual implementation techniques of these goals. [10]
   b) What is a multiplicative inverse? Find all multiplicative inverse pairs in Z_{11}. [4]

3. a) Explain why modern block ciphers are designed as substitution ciphers instead of transposition ciphers. [4]
   b) Explain multiple DES algorithms. List the advantages of multiple DES's compared to single DES. [10]

4. a) Explain the fast Exponentiation algorithm. [6]
   b) Explain the RSA algorithm and answer the following
   (i) What is the one-way function in this system?
   (ii) What is the trapdoor in this system?
   (iii) Define the public and private keys in this system.
   (iv) Describe the security of this system. [8]

5. a) What is digital signature? Explain Elliptic Curve Digital Signature Scheme. [7]
   b) Explain various public-key distribution methods. [7]

6. a) Explain different MIME data types and list the differences between MIME and S/MIME. [7]
   b) Explain the all phases of Handshake protocol in SSL. [7]

7. a) Explain ESP protocol and compare the services provided by IPSec in AH and ESP. [10]
   b) What is IKE? Explain the components of IKE. [4]