Code No: **R204105Y** **R20** **Set No. 1**

IV B.Tech I Semester Regular Examinations, January – 2024

CRYPTOGRAPHY & NETWORK SECURITY

(PE-III: CSE-AIML, CSE-AI, AIML & CSE-CSD) (OE-IV: CE, EEE, ME, ECE, AME, MM, AGE, CSE-CS, CSE-IOTCSIBCT, CSE- IOT, FE, PHARM & CS)

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

Answer any FIVE Questions
ONE Question from Each unit
All Questions Carry Equal Marks
*****

Unit - I

1 a) Describe Denial of Service (DOS), Spoofing & Phishing with suitable examples? [7]
b) Describe different types of attacks and explain in detail? [7]

(OR)

2 a) Explain in detail different passive and active attacks. [7]
b) Discuss examples from real life where the confidentiality is needed? Suggest suitable security mechanisms to achieve them. [7]

Unit - II

3 a) Explain in detail the key generation in AES algorithm and its expansion format? [7]
b) Explain single round DES with neat sketch? [7]

(OR)

4 a) Explain AES encryption and decryption in detail. [7]
b) Compare the substitution method in DES and AES. Why do we need only one substitution table in AES, but several in DES? [7]

Unit - III

5 a) Explain RSA algorithm and give example of generation of public and private keys and generation of cipher text through RSA. [7]
b) Identify the possible threats for RSA algorithm and list their counter measures. [7]

(OR)

Code No: **R204105Y** **R20** **Set No. 1**

6 a) Perform encryption and decryption using the RSA algorithm for p = 3; q = 11, e = 7; M = 5. [7]

b) Perform encryption and decryption using the RSA algorithm for p = 5; q = 11, e = 3; M = 9. [7]

Unit - IV

7 a) Describe digital signature algorithm and show how signing and verification is done using Digital signature scheme? [7]

b) What is importance Chinese Remainder Theorem in cryptography? Explain. [7]

(OR)

8 a) User Alice & Bob exchange the key using Diffie Hellman algorithm Assume α=5 q=83 X_A=6 X_B=10. Find Y_A, Y_B, K. [7]

b) What is Kerberos? Explain how it provides authenticated service. [7]

Unit - V

9 a) Write the general format of PGP Message. Explain the PGP message generation from User A to User B with no compression. [7]

b) How do you provide security at application layer? [7]

(OR)

10 a) Explain how email messages are protected using S/MIME signing and encryption? [7]

b) Explain the authentication services provided by X.509. [7]

Code No: **R204105Y** **R20** **Set No. 2**

IV B.Tech I Semester Regular Examinations, January – 2024

CRYPTOGRAPHY & NETWORK SECURITY

(PE-III: CSE-AIML, CSE-AI, AIML & CSE-CSD) (OE-IV: CE, EEE, ME, ECE, AME, MM, AGE, CSE-CS, CSE-IOTCSIBCT, CSE- IOT, FE, PHARM & CS)

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

Answer any FIVE Questions
ONE Question from Each unit
All Questions Carry Equal Marks
*****

Unit - I

1 a) Explain in details different categories of security threats? [7]
b) Describe various types of cryptographic attacks. [7]

(OR)

2 a) What is a security attack? Explain different security mechanism. [7]
b) Discuss examples from real life where the Integrity is needed? Suggest suitable security mechanisms to achieve them. [7]

Unit - II

3 a) Explain the following operations used in AES?
i) Substitute bytes
ii) Shift Rows [7]
b) Explain the following different modes of operation in DES?
i) Electronic Code Book (ECB)
ii) Cipher Block Chaining (CBC) [7]

(OR)

4 a) In AES, how the encryption key is expanded to produce keys for the 10 rounds? [7]
b) Draw the general structure of DES and explain the encryption decryption process. [7]

Unit - III

5 a) Explain about Rivest Shamir Adleman (RSA) Algorithm with example. [7]
b) Explain in detail EIGamal Public key cryptosystem. [7]

(OR)

Code No: **R204105Y** **R20** **Set No. 2**

6 a) State and prove Chinese remainder theorem. Using Chinese remainder theorem, solve for x for the following $x \equiv 2 \pmod 3$; $x \equiv 3 \pmod 5$; $x \equiv 2 \pmod 7$. [7]

b) In a public-key system using RSA, you intercept the cipher text C = 10 sent to a user whose public key is e = 5, n = 35. What is the plaintext M? [7]

Unit - IV

7 a) How man in middle attack can be performed in Diffie Hellman algorithm? [7]

b) Explain Fermat's theorem and Euler totient function with an example each. [7]

(OR)

8 a) Users A and B use the Diffie Hellman key exchange technique, a common prime q=11 and a primitive root alpha=7. If user A has private key XA=3.What is A's public key YA? If user B has private key XB=6 What is B's public key YB? What is the shared secret key? Also write the algorithm. [7]

b) Explain how authentication is performed in Kerberos. [7]

Unit - V

9 a) Write and explain various PGP cryptographic functions and services in detail. [7]

b) How does PGP provide confidentiality and authentication service for e-mail and file storage applications? Draw the block diagram and explain its components. [7]

(OR)

10 a) Evaluate the different protocols of SSL. Explain Handshake protocol in detail. Describe the SSL Architecture in detail with a neat diagram? [7]

b) Explain Secure Electronic Transaction with neat diagram? [7]

Code No: **R204105Y** **R20** **Set No. 3**

IV B.Tech I Semester Regular Examinations, January – 2024

CRYPTOGRAPHY & NETWORK SECURITY

(PE-III: CSE-AIML, CSE-AI, AIML & CSE-CSD) (OE-IV: CE, EEE, ME, ECE, AME, MM, AGE, CSE-CS, CSE-IOTCSIBCT, CSE- IOT, FE, PHARM & CS)

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

Answer any FIVE Questions
ONE Question from Each unit
All Questions Carry Equal Marks

*****

Unit - I

1 a) What is Cryptography? Explain types and features of Cryptography? [7]
b) Describe in detail about security attacks and security services? [7]

(OR)

2 a) Define threat and attack. What is the difference between both? List some examples of attacks which have arisen in real world cases. [7]
b) Discuss examples from real life, where the Non- repudiation is needed? Suggest suitable security mechanisms to achieve them. [7]

Unit - II

3 a) Explain the following operations used in AES?
i) Mix Columns
ii) Add Round Key [7]
b) Explain Cipher Feedback (CFB) and Output Feedback (OFB) modes of operation in DES? [7]

(OR)

4 a) Draw the general structure of DES and explain the encryption decryption process. [7]
b) Compare the substitution method in DES and AES. Why do we need only one substitution table in AES, but several in DES? [7]

Unit - III

5 a) Explain about public key algorithm with example. [7]
b) Define some Elliptic curves on real numbers. Give the description of addition on those elliptic curves. [7]

(OR)

Code No: **R204105Y** **R20** **Set No. 3**

6 a) Alice chooses 173 and 149 as two prime numbers and 3 as public key in RSA. Check whether the chosen prime numbers are valid or not? [7]

b) In a public-key system using RSA, you intercept the cipher text C = 20 sent to a user whose public key is e = 13, n = 77. What is the plaintext M? [7]

Unit - IV

7 a) In what way Diffie Hellman key exchange algorithm prone to man in the middle attack? [7]

b) Explain in detail Digital Signature Standard approach and its algorithm? [7]

(OR)

8 a) What are the services provided by digital signatures? Explain if the following are provided

i) Source Authentication

ii) Data Integrity

iii) Source Non-Repudiation [7]

b) Explain the process involved in message digest generation and processing of single block inSHA-512. [7]

Unit - V

9 a) Illustrate hot PGP encryption is implemented through suitable diagram? [7]

b) Draw IPSec Authentication Header and write short notes on each element of the Header. [7]

(OR)

10 a) What is the use of SSL protocol? Explain SSL record protocol operation with SSL record format. [7]

b) Write and explain TLS functions and alert codes of Transport Layer Security. [7]

Code No: **R204105Y** **R20** **Set No. 4**

IV B.Tech I Semester Regular Examinations, January – 2024

CRYPTOGRAPHY & NETWORK SECURITY

(PE-III: CSE-AIML, CSE-AI, AIML & CSE-CSD) (OE-IV: CE, EEE, ME, ECE, AME, MM, AGE, CSE-CS, CSE-IOTCSIBCT, CSE- IOT, FE, PHARM & CS)

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

Answer any FIVE Questions
ONE Question from Each unit
All Questions Carry Equal Marks
*****

Unit - I

1	a)	Explain in details different categories of security threats?	[7]
	b)	Describe in detail about Security attacks and security services?	[7]

(OR)

2	a)	What is a security attack? Explain different security mechanism.	[7]
	b)	Define Euler's theorem and it's application also Find gcd (24140, 16762), gcd (1970,1066) using Euclid's algorithm?	[7]

Unit - II

3	a)	Explain in detail the key generation in AES algorithm and its expansion format?	[7]
	b)	Explain the Counter Mode of operation in DES?	[7]

(OR)

4	a)	Explain in detail the sub key generation and round function of DES algorithm in detail.	[7]
	b)	What are the merits of Output-Feedback (OFB. as compared to Cipher Feedback (CFB)?	[7]

Unit - III

5	a)	Explain about RSA asymmetric algorithm.	[7]
	b)	Illustrate Encryption, Decryption and Security of Elliptic Curve Cryptography (ECC).	[7]

(OR)

Code No: **R204105Y** **R20** **Set No. 4**

6	a)	A Box contains gold coins. If the coins are equally divided among three friends, two coins are left over, If the coins are equally divided among five friends, three coins are left over If the coins are equally divided among seven friends, two coins are left over. If the box holds smallest number of coins that meets these conditions, how many coins are there?	[7]
	b)	In an RSA system, the public key of a given user is e = 65, n = 2881, What is the private key of this user?	[7]

Unit - IV

7	a)	Describe the MD5 message digest algorithm with necessary block diagrams.	[7]
	b)	What is the purpose of digital signature? Explain its properties and requirements.	[7]

(OR)

8	a)	What is Birthday Attack on Digital Signatures? Can it be performed by an 'Outsider'?	[7]
	b)	What is Message Authentication code? Explain its functions and basic uses.	[7]

Unit - V

9	a)	Explain the architecture of IPSec in detail with neat diagram?	[7]
	b)	Discuss the seven types of MIME content type?	[7]

(OR)

10	a)	What are the similarities and differences between S/MIME and PGP?	[7]
	b)	With a neat sketch explain the IPSec scenario and IPSec Services.	[7]