



Reg No.: _____

Name: _____

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY
SEVENTH SEMESTER B.TECH DEGREE EXAMINATION(R&S), DECEMBER 2019

Course Code: CS409

Course Name: CRYPTOGRAPHY AND NETWORKSECURITY

Max. Marks: 100

Duration: 3 Hours

PART A

Answer all questions, each carries 4 marks.

		Marks
1	Explain confusion and diffusion properties of modern block ciphers	(4)
2	Differentiate between symmetric and asymmetric cryptosystem	(4)
3	Explain the mix column operation in AES algorithm	(4)
4	Compute $3^{61} \bmod 7$.	(4)
5	What are the requirements of a good hash function	(4)
6	How digital signature is implemented using RSA approach	(4)
7	What are the steps for preparing a SignedData MIME entity?	(4)
8	Give the format of Authentication Header in IPSec	(4)
9	Explain the handshake protocol in SSL	(4)
10	List the various attacks that can be made on packet filtering routers and mention appropriate counter measures	(4)

PART B

Answer any two full questions, each carries 9 marks.

- | | | |
|----|---|-----|
| 11 | a) Use Playfair cipher to encrypt the message 'THE HOUSE IS BEING SOLD TONIGHT' with the key 'GUIDANCE' | (4) |
| | b) Differentiate between monoalphabetic and polyalphabetic ciphers with example | (5) |
| 12 | a) Explain the S-box design of DES algorithm. | (4) |
| | b) Illustrate RC4 algorithm | (5) |
| 13 | a) Explain the key generation in AES algorithm | (5) |
| | b) How round transformation is performed in IDEA. | (4) |

PART C

Answer any two full questions, each carries 9 marks.

- | | | |
|----|--|-----|
| 14 | a) Explain the algorithm for generating keys in RSA algorithm. Perform encryption and decryption using RSA Alg. for the following. $P=7$; $q=11$; $e=13$; $M=8$ | (6) |
| | b) Illustrate man in the middle attack on Diffie Hellman key exchange algorithm | (3) |
| 15 | Illustrate the working of SHA-1 algorithm with diagram | (9) |

- 16 a) How signing and verification is done in Digital Signature algorithm. (5)
b) Illustrate Elliptic Curve Encryption/Decryption (4)

PART D

Answer any two full questions, each carries 12 marks.

- 17 a) Explain in details about the message generation and reception in Pretty Good privacy with neat diagram (8)
b) Explain the construction of dual signature in SET protocol (4)
- 18 a) Explain the various protocols used in SSL (8)
b) Draw and explain IPSec ESP Format (4)
- 19 a) Explain the role of Security Association and SA selectors in IPSec. (6)
b) Discuss about the various types of firewalls (6)
