



Reg No.: _____

Name: _____

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY
SEVENTH SEMESTER B.TECH DEGREE EXAMINATION, DECEMBER 2018

Course Code: CS409

Course Name: CRYPTOGRAPHY AND NETWORK SECURITY

Max. Marks: 100

Duration: 3 Hours

PART A

Answer all questions, each carries 4 marks.

Marks

- | | | |
|----|---|-----|
| 1 | Differentiate between computationally secure cipher and unconditionally secure cipher. Write examples with reasoning. | (4) |
| 2 | Encrypt the message "this is an exercise" using the additive Cipher with key=20 | (4) |
| 3 | What is the necessity of block cipher modes of operation? List out the advantages and disadvantages of <i>output feedback</i> mode. | (4) |
| 4 | Generate the key attributes for the values $p = 11$ and $q = 3$. Also encrypt the message $m = 2$ with the generated keys. | (4) |
| 5 | Find gcd (1970, 1066) | (4) |
| 6 | Discuss digital signature scheme using RSA | (4) |
| 7 | Write the general structure of Private Key Ring used in Pretty Good Privacy (PGP). | (4) |
| 8 | What are the functionalities provided by Secure MIME (S/MIME)? | (4) |
| 9 | What is the significance of Alert Protocol in Transport Layer Security? | (4) |
| 10 | Why the attacker is not able to recognize the actual sender of the message in encrypted tunnels? | (4) |

PART B

Answer any two full questions, each carries 9 marks.

- | | | |
|----|--|-----|
| 11 | a) Use Playfair Cipher with key COMPUTER to encrypt the message "CRYPTOGRAPHY". | (5) |
| | b) How key generation is done in DES. | (4) |
| 12 | a) Discuss the stream cipher RC4 in detail | (4) |
| | b) Illustrate the round transformation of IDEA. | (5) |
| 13 | a) Encrypt the text "LOVE" using Hill Cipher with the key $\begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}$ | (4) |
| | b) Illustrate S box creation in AES | (5) |

PART C

Answer any two full questions, each carries 9 marks.

- 14 a) Define Euler's Totient Function. Prove that, $\phi(pq) = (p-1)(q-1)$, where p and q are prime numbers. (5)
- b) Demonstrate Diffie Hellman Key exchange algorithm. (4)
- 15 Illustrate the working of SHA-1 with diagrams. (9)
- 16 a) What are the Security Requirements of message authentication? (4)
- b) Give the encryption/decryption procedures using Elliptic Curve Cryptography. (5)

PART D

Answer any two full questions, each carries 12 marks.

- 17 a) Explain the sequence of steps involved in the message generation and reception in Pretty Good Privacy (PGP) with block diagrams. (8)
- b) List out the security association (SA) parameters in IPSec. (4)
- 18 a) Illustrate the working of Secure Electronic Transaction (SET) in detail. (8)
- b) Compare Packet filter and Application Level Gateways. (4)
- 19 a) Explain the method of protecting IP datagram from replay attack using IPsec. (6)
- b) Explain the sequence of steps used in Secure Socket Layer handshake Protocol for establishing a new session. Draw a diagram which shows the action of Handshake Protocol. (6)
