

Reg No.: _____

00000CS409121901 Name: _____

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

Seventh Semester B.Tech Degree Examination (Regular and Supplementary), December 2020



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 | What are the two approaches to attack a cipher? Give example for each. | (4) |
| 2 | Use autokey system of Vigenere cipher to encrypt the message "meet me after the toga party" using the key " largest ". | (4) |
| 3 | Illustrate the key expansion procedure of IDEA. | (4) |
| 4 | Define Euler's Totient Function. Compute $\phi(41)$ and $\phi(115)$. | (4) |
| 5 | Distinguish between conventional encryption and public key encryption system. | (4) |
| 6 | Explain any two ways in which a hash code can be used to provide message authentication. | (4) |
| 7 | Why PGP generate a signature before applying compression | (4) |
| 8 | List out the security association parameters in IPSec. | (4) |
| 9 | What is the significance of Alert protocol in SSL and list out any three Alert messages and their use? | (4) |
| 10 | What are the key features provided by SET? | (4) |

PART B

Answer any two full questions, each carries 9 marks.

- | | | |
|----|---|-----|
| 11 | a) Encrypt the word "Semester Result" with the keyword "Examination" using play fair cipher. List the rules used | (5) |
| | b) Depict a block cipher mode that can be used to convert block cipher to stream cipher. | (4) |
| 12 | a) Explain AES key expansion procedure. | (4) |
| | b) Explain the primitive operations of RC4. | (5) |
| 13 | a) Using double stage columnar transposition technique, encrypt the text "Cryptography and Network Security" using the key "43125". | (4) |
| | b) Explain the construction of S-box in AES algorithm. | (5) |

PART C

Answer any two full questions, each carries 9 marks.

- 14 a) User A and B exchange the key using Diffie-Hellman algorithm. Assume $\alpha=5$, (3)
 $q=11$, $X_A=2$, $X_B=3$. Find the values of Y_A , Y_B , and K .
- b) Summarize the RSA algorithm with example. (6)
- 15 Illustrate MD5 hash algorithm in detail. (9)
- 16 a) State and prove Fermat's Theorem. Use Fermat's theorem to find $3^{62} \bmod 7$ (5)
b) Explain message authentication code based on DES. (4)

PART D

Answer any two full questions, each carries 12 marks.

- 17 a) What are the five principal services provided by PGP and explain how (6)
authentication and confidentiality are provided?
- b) Explain the functionalities provided by S/MIME. (6)
- 18 a) Compare the features of three types of Firewall. (9)
b) What is the significance of dual signature in SET? (3)
- 19 a) Define the parameters that define an SSL session state. (6)
b) Give the format of IPSec Authentication header. (6)

Ktunotes.in