

E

03000CS409122301

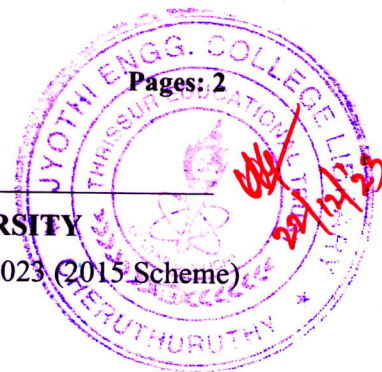
Pages: 2

Reg No.: _____

Name: _____

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

B.Tech Degree S7 (S, FE) / S7 (PT) (S, FE) Examination December 2023 (2015 Scheme)



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 substitution cipher and transposition cipher. | (4) |
| 2 | Use Vigenere cipher with the keyword "key" to encrypt the plain text "SECURITY". | (4) |
| 3 | Explain the key expansion procedure of IDEA. | (4) |
| 4 | Find $12^{102} \text{ mod } 101$ using Fermat theorem | (4) |
| 5 | Find $\text{gcd}(252, 105)$ using Euclidean algorithm. | (4) |
| 6 | What are the requirements of a good hash function? | (4) |
| 7 | List out any four benefits of IPSec. | (4) |
| 8 | What are the functionalities provided by Secure MIME (S/MIME)? | (4) |
| 9 | Differentiate between SSL and TLS | (4) |
| 10 | What are encrypted tunnels? | (4) |

PART B

Answer any two full questions, each carries 9 marks.

- | | | |
|----|--|-----|
| 11 | a) Explain the round function of DES in detail | (5) |
| | b) Differentiate between monoalphabetic ciphers and polyalphabetic ciphers and give one example for each. | (4) |
| 12 | a) Explain the single round transformations of AES with neat sketches. | (9) |
| 13 | a) a) Use Playfair Cipher, with key COMPUTER to encrypt the message "CRYPTOGRAPHY". List out the rules also. | (5) |
| | b) Explain the primitive operations of RC4 algorithm. | (4) |

PART C

Answer any two full questions, each carries 9 marks.

- 14 a) Explain RSA algorithm. In a system an RSA algorithm with $p=5$ and $q=7$, is implemented for data security. What is the value of decryption key if encryption key is 11? (6)
- b) Differentiate between Public key and Private key cryptosystem. (3)
- 15 Illustrate the working of SHA-1 algorithm. (9)
- 16 a) Explain Diffie Hellman Key exchange algorithm. In a Diffie-Hellman Key Exchange, Alice and Bob have chosen prime value $q = 17$ and primitive root = 5. If Alice's secret key is 3 and Bob's secret key is 5, what is the secret key they exchanged? (6)
- b) List different types of attacks addressed by message authentication. (3)

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 PGP with block diagrams. (8)
- b) Compare transport mode and tunnel mode functionalities in IPSec (4)
- 18 a) Compare the features of different types of firewalls. (8)
- b) What is dual signature? Explain the steps involved in generating dual signature. (4)
- 19 a) List and explain different S/MIME message content types (6)
- b) Explain the sequence of operations required for Secure Electronic Transaction. (6)
