



CRYPTOGRAPHY AND SYSTEM SECURITY

May 2019

Computer Engineering (Semester 6)

Total marks: 80

Total time: 3 Hours

INSTRUCTIONS

- (1) Question 1 is compulsory.
- (2) Attempt any **three** from the remaining questions.
- (3) Draw neat diagrams wherever necessary.

- 1.a. Enlist security goals. Discuss their significance. (5 marks)
- 1.b. Compare AES and DES. Which one is bit oriented? Which one is byte oriented? (5 marks)
- 1.c. What is authentication header (AH)? How does it protect against replay attacks? (5 marks)
- 1.d. List various Software Vulnerabilities. How vulnerabilities are exploited to launch an attack. (5 marks)
- 2.a. Encrypt the plaintext message "SECURITY" using affine cipher with the key pair (3, 7). Decrypt to get back original plaintext. (10 marks)
- 2.b. Explain different types of Denial of Service attacks. (10 marks)
- 3.a. Users A and B use the Diffie-Hellman key exchange technique with a common prime 71 and primitive root 7. Show that 7 is primitive root of 71. If user A has private key $x=5$, what is A's Public Key R_1 ? If user B has private key $y=12$, what is B's public key R_2 ? What is the shared secret key? (10 marks)
- 3.b. What are traditional ciphers? Discuss any one substitution and transposition cipher with example. List their merits and demerits. (10 marks)



- 4.a.** Alice chooses public key as (7, 33) and B chooses public key as (13, 221). Calculate their private keys. A wishes to send message $m=5$ to B. Show the message signing and verification using RSA digital signature. (10 marks)
- 4.b.** Discuss in detail block cipher modes of operation. (10 marks)
- 5.a.** What is the need of SSL? Explain all phases of SSL Handshake protocol in detail. (10 marks)
- 5.b.** What are the requirements of the cryptographic hash functions? Compare MD5 and SHA Hash functions. State real world applications of hash functions. (10 marks)
- 6.** Write short notes on any FOUR: (20 marks)
- a. Kerberos
 - b. Buffer Overflow
 - c. 3DES
 - d. X.509
 - e. IDS