LAST MOMENT TUITIONS

CRYPTOGRAPHY AND SYSTEM SECURITY
MAY 2019

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.

Q.1.(a) Enlist security goals. Discuss their significance. (05)
(b) Compare AES and DES. Which one is bit oriented? Which one is byte oriented? (05)
(c) What is authentication header (AH)? How does it protect against replay attacks? (05)
(d) List various Software Vulnerabilities. How vulnerabilities are exploited to launch an attack. (05)

Q.2.(a) Encrypt the plaintext message "SECURITY" using affine cipher with the key pair (3, 7). Decrypt to get back original plaintext. (10)
(b) Explain different types of Denial of Service attacks. (10)

Q.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 R1? If user B has private key y=12, what is B's public key R2? What is the shared secret key? (10)
(b) What are traditional ciphers? Discuss any one substitution and transposition cipher with example. List their merits and demerits. (10)

Q.4.(a) Alice chooses public key as (7, 33) and B chooses public key as (13, 221). Calculate their private keys. A wish to send message m=5 to B. Show the message signing and verification using RSA digital signature. (10)
(**b)** Discuss in detail block cipher modes of operation. (10)

Q.5.(a) What is the need of SSL? Explain all phases of SSL Handshake protocol in detail. (10)
(b) What are the requirements of the cryptographic hash functions? Compare MD5 (10)

Q.6. Write short note on any four. (20)
a. Kerberos
b. buffer Overflow
c. 3 DES
d. X.509
e. IDS