

**TCS/TIT-606****B. TECH. (CS/IT) (SIXTH SEMESTER)  
MID SEMESTER EXAMINATION, 2018  
NETWORK AND CYBER SECURITY****Time : 1 : 30 Hours****Maximum Marks : 50**

**Note :**(i) This question paper contains two Sections.

(ii) Both Sections are compulsory.

**Section—A**

1. Fill in the blanks : (1×5=5 Marks)

- (a) S-DES uses \_\_\_\_\_ bit Cipher key.
- (b) In an “n” group of people wants to communicate with each other, they will need \_\_\_\_\_ keys to communicate using symmetric key cipher
- (c) Symmetric cipher uses \_\_\_\_\_ key(s).
- (d) DoS is a/an \_\_\_\_\_.
- (e) The key domain for multiplicative cipher is \_\_\_\_\_.

2. Attempt any *five* parts : (3×5=15 Marks)

- (a) Authentication Exchange mechanism.

(2)

TCS/TIT-606

- (b) Digital signature.
- (c) Encipherment and data integrity mechanism.
- (d) Define security goals.
- (e) Encrypt message "secure" using Additive cipher with key = 15.
- (f) Traffic padding and Routing control.

**Section—B**

3. Attempt any *two* parts of choice from (a), (b) and (c). (5×2=10 Marks)
- (a) Explain the S-DES structure with its complete architecture.
  - (b) Explain the different Block Cipher Modes of Operations. As well as explain the error propagation in each of them.
  - (c) Encrypt and decrypt the message "MESSAGE IS VERY SECURE" using Affine cipher, where key = (7, 2).
4. Attempt any *two* parts of choice from (a), (b) and (c). (5×2=10 Marks)
- (a) What is double DES ? What kind of attack makes it useless ? What is triple DES ? What is triple DES with two keys ?
  - (b) Explain the five security services defined by ITU-T (X.800).

(3)

- (c) Encrypt a message "this is an exercise" using the multiplicative cipher with key = 15.
5. Attempt any *two* parts of choice from (a), (b) and (c). (5×2=10 Marks)
- (a) Explain RSA Cryptosystem.
  - (b) Explain different types of Active and Passive attacks.
  - (c) Explain the concept of IPv6 authentication along with a short note on modes of IPsec.

TCS/TIT-606

420