

Introduction to Cyber Security 14IT605
B.Tech.,(Semester- VI) Section A

Date : January 05, 2019

Alternate Assessment Test : II

Duration : 45 mts.

Maximum Marks : 30

Set-I ($Rno \bmod 5 == 0$)

I Describe Cipher Block Chaining mode of operation along with its merits and demerits **(5 M)**

II Describe Output Feedback mode of operation along with its merits and demerits **(5 M)**

Introduction to Cyber Security 14IT605
B.Tech.,(Semester- VI) Section A

Date : January 05, 2019
Duration : 45 mts.

Alternate Assessment Test : II
Maximum Marks : 30

Set-II (Rno mod 5 == 1)

- I What is multiple encryption? **(3 M)**
- II Describe Electronic Code Book mode of operation along with its merits and demerits **(5 M)**
- III Why is the middle portion of 3DES a decryption rather than an encryption? **(2 M)**

Introduction to Cyber Security 14IT605
B.Tech.,(Semester- VI) Section A

Date : January 05, 2019
Duration : 45 mts.

Alternate Assessment Test : II
Maximum Marks : 30

Set-III (Rno mod 5 == 2)

- I What is a meet-in-the-middle attack? **(5 M)**
- II Describe Cipher Feedback mode of operation along with its merits and demerits **(5 M)**

Introduction to Cyber Security 14IT605
B.Tech.,(Semester- VI) Section A

Date : January 05, 2019
Duration : 45 mts.

Alternate Assessment Test : II
Maximum Marks : 30

Set-III (Rno mod 5 == 3)

- I How asymmetric encryption provides confidentiality service? **(5 M)**
- II How asymmetric encryption provides authentication service? **(5 M)**

Introduction to Cyber Security 14IT605
B.Tech.,(Semester- VI) Section A

Date : January 05, 2019
Duration : 45 mts.

Alternate Assessment Test : II
Maximum Marks : 30

Set-III (Rno mod 5 == 4)

- I Describe Counter mode of operation along with its merits and demerits **(4 M)**
- II Describe RSA cryptosystem **(6 M)**