# Introduction to Cyber Security 14IT605

## B.Tech.,(Semester- VI) Section A

| | | | | | |
|---|---|---|---|---|---|
| Date | : | December 26, 2018 | Alternate Assessment Test | : | I |
| Duration | : | 45 mts. | Maximum Marks | : | 30 |

***Set-I ( Rno mod 3 == 0 )***

---

| | | |
|---|---|---|
| I | What is the OSI security architecture? | **(3 M)** |
| II | What is steganography? | **(3 M)** |
| III | Briefly describe the Playfair cipher. | **(3 M)** |
| IV | Briefly describe the Hill cipher. | **(3 M)** |
| V | Briefly define types of cryptanalytic attacks based on what is known to the attacker. | **(3 M)** |
| VI | What are two problems with the one-time pad? | **(3 M)** |
| VII | What is the difference between diffusion and confusion? | **(3 M)** |
| VIII | What is a product cipher? | **(3 M)** |
| IX | What is the purpose of the S-boxes in DES? | **(3 M)** |
| X | Explain the avalanche effect. | **(3 M)** |

# Introduction to Cyber Security 14IT605

## B.Tech.,(Semester- VI) Section A

| | | | | | |
|---|---|---|---|---|---|
| Date | : | December 26, 2018 | Alternate Assessment Test | : | I |
| Duration | : | 45 mts. | Maximum Marks | : | 30 |

***Set-II ( Rno mod 3 == 1 )***

---

| | | |
|---|---|---|
| I | What is the difference between passive and active security threats? | **(3 M)** |
| II | Briefly define categories of security services. | **(3 M)** |
| III | What is the difference between an unconditionally secure cipher and a computationally secure cipher? | **(3 M)** |
| IV | Briefly describe the Caesar cipher. | **(3 M)** |
| V | Briefly describe the monoalphabetic cipher. | **(3 M)** |
| VI | What is the difference between a monoalphabetic cipher and a polyalphabetic cipher? | **(3 M)** |
| VII | Why is it important to study the Feistel cipher? | **(3 M)** |
| VIII | What is the difference between a block cipher and a stream cipher? | **(3 M)** |
| IX | Which parameters and design choices determine the actual algorithm of a Feistel cipher? | **(3 M)** |
| X | What is a singular transformation? Give one example. | **(3 M)** |

# Introduction to Cyber Security 14IT605

## B.Tech.,(Semester- VI) Section A

Date : December 26, 2018 Alternate Assessment Test : I

Duration : 45 mts. Maximum Marks : 30

***Set-III ( Rno mod 3 == 2 )***

---

| | | |
|---|---|---|
| I | Briefly define categories of passive and active security attacks. | **(3 M)** |
| II | Briefly define categories of security mechanisms. | **(3 M)** |
| III | What are the essential ingredients of a symmetric cipher? | **(3 M)** |
| IV | What are the two basic functions used in encryption algorithms? | **(3 M)** |
| V | How many keys are required for two people to communicate via a cipher? | **(3 M)** |
| VI | What is the difference between a block cipher and a stream cipher? | **(3 M)** |
| VII | What are the two general approaches to attacking a cipher? | **(3 M)** |
| VIII | What is a transposition cipher? | **(3 M)** |
| IX | Why is it important to study the Feistel cipher? | **(3 M)** |
| X | What is the difference between a block cipher and a stream cipher? | **(3 M)** |