No. of Printed Pages : 2

1116

CS308/IT308

Roll No. : .....

2018

INTRODUCTION TO NETWORK SECURITY AND CRYPTOGRAPHY

निर्धारित समय : तीन घंटे] **[अधिकतम अंक : 70**

Time allowed : Three Hours] **[Maximum Marks : 70**

नोट : *(i) प्रथम प्रश्न अनिवार्य है, शेष में से किन्हीं **पाँच** के उत्तर दीजिये ।*

Note : *Question No. 1 is compulsory, answer any **FIVE** questions from the remaining.*

(ii) प्रत्येक प्रश्न के सभी भागों को क्रमवार एक साथ हल कीजिये ।
Solve all parts of a question consecutively together.

(iii) प्रत्येक प्रश्न को नये पृष्ठ से प्रारम्भ कीजिये ।
Start each question on fresh page.

(iv) दोनों भाषाओं में अन्तर होने की स्थिति में अंग्रेजी अनुवाद ही मान्य है ।
Only English version is valid in case of difference in both the languages.

1. (i) क्रिप्टएनालिस्ट क्या है ?
What is Cryptanalyst ?

(ii) फायरवाल से आप क्या समझते हो ?
What do you understand by firewall.

(iii) ऐक्टिव हमलों से आप क्या समझते हो ?
What do you understand by active attack.

(iv) डिजिटल हस्ताक्षर को परिभाषित कीजिए ।
Define digital signature.

(v) नॉन रेप्यूडिएशन की अवधारणा क्या है ?
What is the concept of non repudiation ? **(2×5)**

2. (i) असममित कुंजी क्रिप्टोग्राफी को खण्ड आरेख की सहायता से समझाइये ।
Explain asymmetric key cryptography with the help of block diagram.

(ii) फिशिंग अटैक को समझाइये ।
Explain phishing attack. **(6+6)**

3. (i) मोनो अल्फाबेटिक साइफर क्या है, उदाहरण सहित समझाइये ।
What is mono alphabetic cipher, explain with example.
(ii) एनक्रिप्शन तथा डिक्रिप्शन को समझाइये ।
Explain encryption and decryption. (6+6)

4. इन्टरनेट सुरक्षा प्रोटोकोल से आप क्या समझते हैं ? एस एस एल क्या है ? यह किस प्रकार कार्य करती है ? विस्तार से समझाइये ।
What do you understand by Internet Security Protocol ? What is SSL ? How it works ? Explain in details. (12)

5. (i) ब्लॉक साइफर साधारण टेक्स्ट को साइफर टेक्स्ट में किस एल्गोरिथ्मिक विधि द्वारा परिवर्तित करता है, उदाहरण सहित समझाइये ।
How does block cipher convert plain text into cipher text ? Explain algorithmic mode with example.
(ii) प्रोग्राम अटैक से आप क्या समझते हो ? वोर्म एवं ट्रोजन हार्स अटैक को समझाइये ।
What do you meant by program attack ? Explain worm and trojan horse attack. (6+6)

6. (i) प्रेटी गुड प्राइवेसी द्वारा ईमेल सुरक्षा किस प्रकार प्रदान की जाती है ? समझाइये ।
How are the email security features offered by pretty good privacy ? Explain.
(ii) एस एम टी पी को समझाइये ।
Explain SMTP. (6+6)

7. (i) वर्चुअल प्राइवेट नेटवर्क क्या है ? समझाइये ।
What is virtual private network ? Explain.
(ii) पैकेट फिल्टरिंग राउटर की कार्य प्रणाली को समझाइये ।
Explain the working of packet filtering router. (6+6)

8. निम्न पर संक्षिप्त टिप्पणियाँ लिखिए :
Write short notes on the following :
(i) मैसेज डाइजेस्ट
Massage Diegest
(ii) सेक्योर इलेक्ट्रोनिक ट्रान्जेक्शन (SET) ।
Secure electronic transaction (SET). (6+6)
