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)**