Roll No. .....

(87) **8330**

Printed Pages—**4**] **4M.Sc.(CS)3(C)**

Master of Science (CS) (Fourth Semester) Examination, Dec. 2018/Jan. 2019

INFORMATION SECURITY

अवधि/Duration : 3 घंटे/Hours] [पूर्णांक/Max. Marks : 80

[न्यूनतम उत्तीर्णांक/Min. Pass Marks : 32

निर्देश :

1. प्रश्न-पत्र पाँच इकाइयों में विभाजित है । प्रत्येक इकाई में आन्तरिक विकल्प दिया गया है ।
2. प्रत्येक इकाई से **एक** प्रश्न का उत्तर दीजिए । इस प्रकार कुल **पाँच** प्रश्नों के उत्तर दीजिए ।
3. **सभी** प्रश्नों के लिए समान अंक नियत हैं ।
4. जहाँ आवश्यकता हो वहाँ उपयुक्त डाटा माना जा सकता है ।
5. अनुवाद में विसंगति होने पर अंग्रेजी स्वरूप को सही माना जाए ।
6. प्रश्न-पत्र में परीक्षार्थी निर्धारित स्थान पर अपना रोल नम्बर अंकित करें ।

Instructions :

1. The Question Paper is divided in five Units. Each unit carries an internal choice.
2. Attempt *one* question from each Unit. Thus attempt *five* questions in all.
3. *All* questions carry equal marks.
4. Assume suitable data wherever necessary.
5. English version should be deemed to be correct in case of any anomaly in translation.
6. Candidate should write his/her Roll Number at the prescribed space on the question paper.

P.T.O.

इकाई I (Unit I)

1. (*a*) क्रिप्टोग्राफी और अन्य सुरक्षा तंत्र द्वारा गोपनीयता और उपलब्धता कैसे प्राप्त करेंगे ? 8

How to achieve confidentiality and availability by Cryptography and other security mechanisms ?

(*b*) Spoofing और Sniffers में उदाहरण सहित अन्तर स्पष्ट कीजिए। 8

Differentiate between spoofing and sniffers with examples.

अथवा (*Or*)

2. (*a*) गैर-अस्वीकार क्या है ? डेटा ट्रांसमिशन में हमें प्रमाणीकरण की आवश्यकता क्यों होती है ? 8

What is Non-Repudiation ? Why do we need authentication in data transmission ?

(*b*) Malicious Code और Backdoors में उदाहरण सहित अन्तर स्पष्ट कीजिये। 8

Differentiate between Malicious Code and Backdoors with examples.

इकाई II (Unit II)

3. (*a*) शास्त्रीय एन्क्रिप्शन तकनीकों को परिभाषित कीजिये। 8

Define Classical Encryption Techniques.

(*b*) Confusion और Diffusion की उदाहरण सहित व्याख्या कीजिये। 8

Explain Confusion and Diffusion with examples.

अथवा (*Or*)

4. (*a*) आई.डी.ई.ए. (इंटरनेशनल डेटा एन्क्रिप्शन एल्गोरिद्म) को समझाइए। 8

Explain IDEA (International Data Encryption Algorithm).

(*b*) Feistel Cipher Structure के बारे में विस्तार से समझाइए। 8

Explain in detail about Feistel Cipher Structure.

इकाई III (Unit III)

5. (*a*) आर.एस.ए. एल्गोरिद्म को समझाइए। 8

Explain RSA algorithm.

(*b*) Digital Signature Algorithm में Parameter Generation की व्याख्या कीजिये। 8

Explain Parameter Generation in Digital Signature Algorithm.

अथवा (*Or*)

6. (*a*) Simple Hash Function और Secured Hash Function में अंतर स्पष्ट कीजिये। 8

Differentiate between Simple Hash Function and Secured Hash Function.

(*b*) X.509 में प्रमाणन प्रक्रियाओं को परिभाषित कीजिये। 8

Define authentication procedure in X.509.

इकाई IV (Unit IV)

7. (*a*) हमें कुंजी प्रबंधन की आवश्यकता क्यों है ? विभिन्न कुंजी प्रबंधन तकनीकों को समझाइए। 8

What do we need Key Management ? Explain various key management techniques.

(*b*) IP Sec (IP Security) Architecture की व्याख्या कीजिये। 8

Explain IP Sec (IP Security) Architecture.

अथवा (*Or*)

8. (*a*) Security Association से आप क्या समझते हैं ? SA (Security Association) के सन्दर्भ में Key Management को समझाइए। 8

What do you understand by Security Associations ? Explain Key Management in the context of SA (Security Association).

(*b*) e-mail Security में प्रयुक्त S/MIME की व्याख्या कीजिये। 8

Explain S/MIME used in e-mail Security.

इकाई V (Unit V)

9. (*a*) Cyber Crimes की श्रेणियाँ बताइये तथा संक्षेप में उनके विभिन्न वर्गीकरण समझाइये। 8

Classify Cyber Crimes and briefly explain its different categories.

(*b*) सूचना युद्ध से आप क्या समझते हैं ? आतंकवादी सूचना का उपयोग खुफिया हथियार के रूप में कैसे कर सकते हैं ? 8

What do you understand by Information Warfare ? How can terrorist use information as an intelligence weapon ?

अथवा (*Or*)

10. (*a*) "Information as an Intelligence Weapon" पर टिप्पणी कीजिये। 8

Comment on "Information as an Intelligence Weapon".

(*b*) निम्न पर संक्षिप्त टिप्पणी लिखिए : 8

Write short notes on :

(1) Hackers

(2) Insurgents

(3) Extremist Groups

(4) Attack and Retaliation

(5) Attack and Defense.