Roll No. .....

(127) **4504**

Printed Pages—**4**] **4M.Sc.(IT)3(B)**

Master of Science (IT) (Fourth Semester) Examination, May/June, 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*) सुरक्षा आक्रमण से आप क्या समझते हैं ? उपयुक्त उदाहरण सहित समझाइए। 8

What do you understand by Security Attacks ? Explain with suitable example.

(*b*) सिलेक्टिव फील्ड गोपनीयता और सिलेक्टिव फ्लो गोपनीयता में अन्तर बताइये। 8

Differentiate between Selective Field Confidentiality and Selective Flow Confidentiality.

(**अथवा**/*Or*)

2. (*a*) मोडीफिकेशन और फेब्रीकेशन सुरक्षा आक्रमणों को उपयुक्त उदाहरण सहित समझाइये। 8

Explain Modification and Fabrication types of Security attacks with suitable examples.

(*b*) सुरक्षा के Non-Repudiation सिद्धांत से आप क्या समझते हैं ? Non-Repudiation Origin सिद्धांत Non-Repudiation Destination सिद्धांत से किस प्रकार भिन्न है ? 8

What do you understand by Non-Repudiation principle of security ? How does Non-Repudiation Origin principle differ than Non-Repudiation Destination principle ?

(इकाई II/Unit II)

3. (*a*) Mono-Alphabetic Cipher और Poly-Alphabetic Cipher से आप क्या समझते हैं ? उदाहरण सहित समझाइये। 8

What do you understand by Mono-Alphabetic Cipher and Poly-Alphabetic Cipher ? Explain with examples.

(*b*) ECB (Electronic Code Book) और CBC (Cipher Block Chaining) ऑपरेशन मोड्स में अन्तर बताइये।

Differentiate between ECB (Electronic Code Book) and CBC (Cipher Block Chaining) cipher modes of operation.

(अथवा/*Or*)

4. (*a*) One Time Pad cipher को उचित उदाहरण सहित समझाइये। 8
Explain One Time Pad cipher with suitable example.

(*b*) Secure Hash Function के कार्यकारी सिद्धान्त को समझाइये। 8
Explain working principle of Secure Hash Function.

(इकाई III/Unit III)

5. (*a*) RSA (Rivest-Shamir-Adleman) क्रिप्टोग्राफी एल्गोरिथ्म से आप क्या समझते हैं ? 8
What do you know about RSA (Rivest-Shamir-Adleman) cryptography algorithm ?

(*b*) डिजिटल सिग्नेचर क्या हैं ? डिजिटल सिग्नेचर डिजिटल हस्ताक्षर (सर्टिफिकेट्स) से किस तरह भिन्न हैं ? समझाइये। 8
What are digital signatures ? How do they differ from digital certificates ? Explain.

(अथवा/*Or*)

6. (*a*) Symmetric Key Cryptography और Asymmetric Key Cryptography में अन्तर बताइये। 8
Distinguish between Symmetric Key Cryptography and Asymmetric Key Cryptography.

(*b*) X.509 directory authentication डिजिटल सर्टीफिकेट्स के विभिन्न संस्करणों का वर्णन कीजिये। 8
Describe different versions of X.509 directory authentication digital certificates.

(इकाई IV/Unit IV)

7. (*a*) E-Mail सुरक्षा से आप क्या समझते हैं ? PEM (Privacy Enhanced Mail) e-mail सुरक्षा मानक को समझाइये। 8
What do you know about E-Mail Security ? Explain PEM (Privacy Enhanced Mail) e-mail security standard.

(*b*) IP सुरक्षा की विभिन्न विशेषताएँ लिखिये। 8
Write down the different features of IP Security.

(अथवा/*Or*)

8. (*a*) PGP (Pretty Good Privacy) e-mail सुरक्षा मानक को समझाइये। PEM (Privacy Enhanced Mail) e-mail सुरक्षा मानक से यह किस प्रकार भिन्न है ? 8

Explain the PGP (Pretty Good Privacy) e-mail security standard. How does it differ from PEM (Privacy Enhanced Mail) e-mail security standard ?

(*b*) IP सुरक्षा की संरचना का वर्णन कीजिये। 8

Describe the architecture of IP Security.

(इकाई V/Unit V)

9. (*a*) साइबर अपराध को विस्तार से समझाइये। 8

Describe the Cyber Crime in detail.

(*b*) साइबर अपराध से संबंधित Insurgents और Extremist groups को समझाइये। 8

Explain Insurgents and Extremist groups related to cyber crime.

(अथवा/*Or*)

10. (*a*) विभिन्न साइबर अपराध आक्रमण के प्रकारों के नाम लिखिये। 8

Write down the names of different Cyber Crime attacks.

(*b*) "White hat hackers को ethical hackers भी कहते हैं।" व्याख्या कीजिये। 8

"White hat hackers are ethical hackers". Justify.