Roll No. 519231

(142) **4504**

Printed Pages—7] **4M.Sc.(IT)3(B)**

# Master of Science (IT) (Fourth Semester) Examination, May/June, 2015

## 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.**

Scanned by CamScanner

## इकाई I (Unit I)

1. (a) Passive तथा Active security attacks (सुरक्षा आक्रमण) क्या हैं ? 10

What are Passive and Active security attacks ?

(b) कौनसी Security Mechanism(s) निम्नलिखित में से प्रत्येक मामले में लागू होती है ? प्रत्येक मामले के लिए अपने उत्तर को न्याय-संगत भी कीजिए : 10

(i) एक बैंक को Withdrawal के लिए एक ग्राहक के हस्ताक्षर की आवश्यकता है।

(ii) Exam Server में login के निमित्त एक on-line exam centre अभ्यर्थी की पहचान तथा Password की माँग करता है।

Which Security Mechanism(s) are provided in each of the following cases ? Also, justify your answer for each case :

(i) A bank requires the customer's signature for a withdrawal.

(ii) An on-line exam center demands the identification and the password of the candidate in order to login into the exam server.

**अथवा (Or)**

2. (a) गोपनीयता, सुरक्षा का एक महत्वपूर्ण सिद्धांत क्यों है ? इसे प्राप्त करने के उपायों का वर्णन कीजिए। 10

Why is confidentiality an important principle of security ? Describe the ways of achieving it.



Scanned by CamScanner

a2z question papers visit http://www.a2zsubjects.com

(b) कौनसी सुरक्षा मैकेनिज्म निम्नलिखित में से प्रत्येक मामले में लागू होती है ? प्रत्येक मामले के लिए अपना उत्तर न्यायसंगत भी कीजिए : 10

(i) जब एक व्यक्ति एक क्रेडिट कार्ड के लिए आवेदन हेतु भरे गये फॉर्म पर हस्ताक्षर करता है।

(ii) एक कॉलेज सर्वर एक विद्यार्थी को डिसकनेक्ट करता है यदि वह दो घण्टे से अधिक के लिए Logged into the system है।

Which Security Mechanism(s) are provided in each of the following cases ? Also, justify your answer for each case :

(i) When a person signs a form he has filled out to apply for a credit card ?

(ii) A college server disconnects a student if he/she is logged into the system for more than two hours.

## इकाई II (Unit II)

3. (a) Block cipher तथा Stream cipher के बीच अन्तर कीजिए। 10

Distinguish between the Block cipher and stream cipher.

(b) Secure Hash Function में कौन-कौनसी विशेषताओं की आवश्यकता होती है ? SHA-1 को विस्तार से समझाइए। 10

What characteristics are needed in a Secure Hash Function ? Explain SHA-1 in detail.



Scanned by CamScanner

अथवा (*Or*)

4. (*a*) प्रचालन (Operations) के विभिन्न Block cipher modes की विस्तार से व्याख्या कीजिए। 10

Discuss the various block cipher modes of operations in detail.

(*b*) Encryption के लिए Single columnar transposition तकनीक को समझाइए तथा Keyword ADMIRAL का प्रयोग करके निम्नलिखित Plaintext के Encrypt के लिए इसका प्रयोग कीजिए। AIRCRAFT WILL GO TO NEW DELHI। 10

Explain single columnar transposition technique for encryption and use it to encrypt the following plaintext using the keyword ADMIRAL AIRCRAFT WILL GO TO NEW DELHI.

## इकाई III (Unit III)

5. (*a*) Common prime $q = 11$ तथा primitive root $\alpha = 2$ के साथ Diffe-Hellman स्कीम पर विचार कीजिए। यदि User A के पास Public key $Y_a = 9$ है तो A की प्राइवेट key $X_a$ क्या है ? 10

Consider a Diffie-Hellman scheme with a common prime $q = 11$ and primitive root $\alpha = 2$. If user A has public key $Y_a = 9$, what is A's private key $X_a$ ?



Scanned by CamScanner
a2z question papers visit http://www.a2zsubjects.com

(*b*) Direct Digital Signature तथा Arbitrated Digital Signature के बीच अंतर कीजिए। 10

Differentiate between the Direct Digital Signature and an Arbitrated Digital Signature.

अथवा (*Or*)

6. (*a*) निम्नलिखित डाटा के लिए RSA अल्गोरिथ्म का प्रयोग करके Encryption तथा Decryption का निष्पादन कीजिए : 10

$$p = 17,\ q = 31,\ e = 7,\ m = 2.$$

Perform encryption and decryption using the RSA algorithm for the following data :

$$p = 17,\ q = 31,\ e = 7,\ m = 2.$$

(*b*) X.509 सर्टीफिकेट format को समझाइए। 10

Explain the X.509 certificate format.

## इकाई IV (Unit IV)

7. (*a*) IP security तथा Security association का क्या अर्थ ? 10

What is meant by IP security and security association ?



Scanned by CamScanner

अथवा (*Or*)

10. (*a*) प्रमुख Cyber कानूनों को परिभाषित तथा सूचीबद्ध कीजिए। 10

Define and list important Cyber Laws.

(*b*) Ethical Hacking के विभिन्न Phases को समझाइए। 10

Explain the different phases of ethical hacking.



Scanned by CamScanner

a2z question papers visit http://www.a2zsubjects.com