Roll No. .....

(173) **9335**

Printed Pages—**4**] **4MCA7/CCE8**

Master of Computer Application (Fourth Semester)

(CBCS) Examination, Dec. 2018/Jan. 2019

NETWORK AND CYBER 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*) Public key cryptography को परिभाषित कीजिए और cryptography में उनके एप्लिकेशन की व्याख्या कीजिए।

Define public key cryptography and explain their application in cryptography.

(*b*) Threat क्या है ? Threats के स्रोतों को सूचीबद्ध कीजिए।

What is threat ? Enlist sources of threats.

अथवा (*Or*)

2. (*a*) हमें Cyber security की आवश्यकता क्यों है ? उदाहरणों के साथ CIA की व्याख्या कीजिए।

Why do we need cyber security ? Explain the CIA with an example.

(*b*) Blowfish में महत्वपूर्ण विस्तार कैसे किया जाता है ?

How is key expansion done in Blowfish ?

इकाई II (Unit II)

3. (*a*) DES में S-Box की भूमिका क्या है ? व्याख्या कीजिये।

What is the role of S-Box in DES ? Explain.

(*b*) विभिन्न block cipher डिजाइन सिद्धांत क्या हैं ?

What are the various block cipher design principles ?

अथवा (*Or*)

4. (*a*) Diffie Hellman न तो एन्क्रिप्ट करता है और न ही संकेत देता है। यह क्या करता है ?

Diffie Hellman neither encrypts nor signs. What does it do ?

(*b*) समझाइए कि विभिन्न cryptographic एल्गोरिदम Fiestel Cipher Structure का उपयोग कैसे करते हैं ?

Explain how different cryptographic algorithms use Fiestel Cipher structure ?

इकाई III (Unit III)

5. (*a*) निम्नलिखित के लिए RSA का उपयोग करके एन्क्रिप्शन और डिक्रिप्शन कीजिए :

Perform encryption and decryption using RSA for the following :

$$p = 3;\ q = 11;\ e = 7;\ m = 5$$

(*b*) Secure Socket Layer द्वारा परिभाषित **चार** प्रोटोकॉल समझाइए।

Explain the *four* protocols defined by Secure Socket Layer.

अथवा (*Or*)

6. (*a*) Digital signatures पर हमलों का वर्णन कीजिए।

Describe the attacks on digital signatures.

(*b*) IPSec द्वारा कौनसी सेवाएँ प्रदान की जाती हैं ? IPSec की architecture का वर्णन कीजिए।

What services are provided by IPSec ? Describe the architecture of IPSec.

इकाई IV (Unit IV)

7. (*a*) Hash function क्या है ? HMAC से MAC अलग कैसे है ?

What is hash function ? How is MAC different from HMAC ?

(*b*) MD5 क्या है ? नेटवर्क को सुरक्षित रखने के लिए इसका उपयोग कैसे किया जाता है ?

What is MD5 ? How is it used for secure the network ?

अथवा (*Or*)

8. (*a*) Trap door प्रणाली को समझाइये।

Explain the trap door system.

(*b*) GPG को परिभाषित कीजिए। GPG ट्रस्ट मॉडल पर चर्चा कीजिए।

Define GPG. Discuss the GPG trust model.

इकाई V (Unit V)

9. (*a*) उदाहरण के साथ PKI का वर्णन कीजिए।

Describe the PKI with an example.

(*b*) Kerberos की क्या आवश्यकताएँ हैं ? "Is Ethical hacking legal" पर टिप्पणी कीजिए।

What are the requirements of Kerberos ? Comment on "Is Ethical hacking legal" ?

अथवा (*Or*)

10. (*a*) सिद्धांत और विधियों का उपयोग करके आप efficient authentication कैसे प्राप्त करते हैं ?

How do you achieve efficient authentication using principle and methods ?

(*b*) Audit क्या है ? Security audit की आवश्यकता पर चर्चा कीजिए।

What is an audit ? Discuss the necessity of security audit.