Roll No. .....

(192) **9335**

Printed Pages—4] **4MCA7/CCE8**

Master of Computer Application (Fourth Semester)

(CBCS) Examination, May/June 2019

NETWORK & 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*) Block cipher क्या है ? Mode of opreations पर संक्षिप्त नोट लिखिए।

What is block cipher ? Write a short note on mode of opreations.

(*b*) Modern cipher के confusions और diffusions में गुण क्या हैं ?

What are confusions and diffusions properties of modern cipher ?

अथवा/(*Or*)

2. (*a*) उदाहरणों के साथ one-way function पर चर्चा कीजिए।

Discuss the one-way function with an example.

(*b*) निम्नलिखित को समझाइए :

Explain the following :

(*a*) Blowfish

(*b*) IDEA

(*c*) RCS.

इकाई II/(Unit II)

3. (*a*) DES round क्या है ? 'IDEA' DES से अलग कैसे है ?

What is DES round ? How is IDEA different from DES ?

(*b*) Middle attack में आदमी क्या है ? एलिस और बॉब ने जी = 7 का उपयोग करके डिफी हेलमैन key एक्सचेंज का उपयोग करके सीक्रेट स्थापित किया; एन = 13. एलिस एक्स को 3 के रूप में लेता है और बॉब 9 के रूप में वाई लेता है। टॉम और घुसपैठिए X को 8 और Y को 6 के रूप में चुनते हैं। Middle attack में आदमी के काम को दिखाइए।

What is man in the middle attack ? Alice and Bob establish secrete using Diffie Hellman key exchange using g = 7; n=13. Alice takes X as 3 and Bob takes Y as 9. Tom and intruder select X as 8 and Y as 6. Show the working of the man in the middle attack.

अथवा/(*Or*)

4. (*a*) DES सिंहावलोकन और DES round के संदर्भ में DES एल्गोरिद्म का वर्णन कीजिए।

Describe the algorithm with reference to its overview and DES round.

(*b*) Diff-hell Key वितरण एल्गोरिद्म और इसकी हानि के बारे में बताइए।

Explain diff-hell key distribution algorithm and list disadvantages of it.

इकाई III/(Unit III)

5. (*a*) यदि सादा पाठ 63 और public key 13 है, तो सिफर टेक्स्ट क्या है ? RSA एल्गोरिद्म का प्रयोग कीजिए।

What is the cipher text if the plain text is 63 and public key is 13 ? Use RSA algorithm.

(*b*) IPSec द्वारा प्रदान की जाने वाली सेवाएँ क्या हैं ? नेटवर्क पर स्थित IPSec कहाँ हो सकता है ?

Waht are the services provided by IPSec ? Where can be the IPSec located on a network ?

अथवा/(*Or*)

6. (*a*) Digital Signature को परिभाषित कीजिए। नेटवर्क सुरक्षा में अपनी भूमिका की व्याख्या कीजिए।

Define digital signature. Expalin its role in network security.

(*b*) उपयुक्त उदाहरणों के साथ RSA के बारे में वर्णन कीजिए।

Describe about the RSA with suitable examples

इकाई IV/(Unit IV)

7. (*a*) Secure Hash Algorithm के compression की व्याख्या कीजिए।

Explain the compression of Secure Hash Algorithm.

(*b*) GUI-KGPG के बारे में चर्चा कीजिए।

Discuss about the GUI-KGPG.

अथवा/(*Or*)

8. (*a*) Frontends-Kleopatra पर एक संक्षिप्त नोट लिखिए।

Write a short note on Frontends-Kleopatra?

(*b*) SHA-256 क्या है ? नेटवर्क को सुरक्षित रखने के लिए इसका उपयोग कैसे किया जाता है ?

What is SHA-256 ? How is it used for secure the network ?

इकाई V/(Unit V)

9. (*a*) चार public key cryptography एल्गोरिद्म सूचीबद्ध कीजिए। एल्गोरिद्म में से एक को समझाइए जहाँ public key cryptography का उपयोग किया जाता है ?

List *four* public key cryptography algorithms. Explain *one* of the algorithms where public key cryptography are used.

(*b*) Seahorse क्या है ? Modular Square roots पर संक्षिप्त नोट लिखिए।

What is seahorse ? Write a short note on modular square roots ?

अथवा/(*Or*)

10. (*a*) Steganography से आपका क्या मतलब है ? आप मल्टीमीडिया फाइल में डेटा कैसे छिपाते हैं ?

What do you mean by steganography ? How do you hide data in a mutlimedia file ?

(*b*) इंटरनेट प्रोटोकॉल की transport layer पर सुरक्षा सेवाओं की क्या आवश्यकता है ?

What is the need for security services at transport layer of Internet Protocol ?