Total No. of Questions : 8] [Total No. of Printed Pages : 3

Roll No ...

IS-304 (GS)

B.Tech., III Semester

Examination, November 2022

Grading System (GS)

Introduction to Information Security

Time : Three Hours

Maximum Marks : 70

Note: i) Answer any five questions.
किन्हीं पाँच प्रश्नों को हल कीजिए।

ii) All questions carry equal marks.
सभी प्रश्न के समान अंक हैं।

iii) In case of any doubt or dispute the English version question should be treated as final.
किसी भी प्रकार के संदेह अथवा विवाद की स्थिति में अंग्रेजी भाषा के प्रश्न को अंतिम माना जायेगा।

1. a) What are the different factors on which Cryptography depends?
क्रिप्टोग्राफ़ी किन विभिन्न कारकों पर निर्भर करती है?

b) Find GCD (1970, 1066) by using Euclid's Algorithm.
यूक्लिड एल्गोरिथम का प्रयोग करके GCD (1970, 1066) ज्ञात कीजिए।

2. a) What is prime and relative prime numbers in cryptography and network security.
क्रिप्टोग्राफ़ी और नेटवर्क सुरक्षा में अभाज्य और सापेक्ष अभाज्य संख्याएँ क्या हैं?

b) Draw the block diagram of DES algorithm. Also explain its functionality.
DES एल्गोरिथम का ब्लॉक आरेख बनाइए। इसकी कार्यप्रणाली भी स्पष्ट कीजिए।

3. a) Describe IDEA encryption and decryption in brief.
आईडिया एन्क्रिप्शन और डिक्रिप्शन का संक्षेप में वर्णन करें।

b) Discuss the Message Authentication Codes. Also give the use of Authentication requirements in MAC.
संदेश प्रमाणीकरण कोड पर चर्चा करें। MAC में प्रमाणीकरण आवश्यताओं के उपयोग के बारे में भी बताइए।

4. a) List the strength of DES in brief. Also explain the Triple DES.
DES की ताकत को संक्षेप में सूचीबद्ध करें। ट्रिपल DES को भी समझाइए।

b) Explain the Chinese Remainder theorem with example. How Chinese Remainder theorem provide the security to online sharing transactions?
चायनीज शेष प्रमेय को उदाहरण सहित समझाइए। कैसे चायनीज शेष प्रमेय ऑनलाइन साझाकरण लेनदेन को सुरक्षा प्रदान करता है?

5. a) What do you understand from Hash Functions? Discuss the working of secure hash algorithm in Message Authentication.
हैश फंक्शन से आप क्या समझते हैं? संदेश प्रमाणीकरण में सुरक्षित हैश एल्गोरिथम की कार्यप्रणाली पर चर्चा करें।

b) Explain the Digital Signatures. Also give a detail description of Elgamal Digital Signature Techniques.
डिजिटल सिग्नेचर को समझाइए। एलगामल डिजिटल सिग्नेचर तकनीक का भी विस्तृत विवरण दें।

6. a) What do mean by System security? Also discuss Viruses and related threats to system security.

सिस्टम सुरक्षा से क्या तात्पर्य है? सिस्टम सुरक्षा के लिए वायरस और संबंधित खतरों पर भी चर्चा करें।

b) Discuss X.509 Certificates in detail. What is the role of X.509 in cryptography?

X.509 प्रमाणपत्रों पर विस्तार से चर्चा करें। क्रिप्टोग्राफी में X.509 की क्या भूमिका है?

7. a) Discuss Diffie Hellman key exchange method. Let $q = 353$, $\alpha = 3$, $X_A = 97$ and $X_B = 233$. Then compute Y_A, Y_B, K_A and K_B using Diffie Hellman.

डिफी हेलमैन की एक्सचेंज विधि की चर्चा करें। दिया गया है $q = 353$, $\alpha = 3$, $X_A = 97$ और $X_B = 233$। फिर डिफी हेलमैन का उपयोग करके Y_A, Y_B, K_A और K_B की गणना करें।

b) What is Block Cipher? Discuss Block Cipher Mode of Operations.

ब्लॉक सिफर क्या है? संचालन के ब्लॉक सिफर मोड पर चर्चा करें।

8. Write short notes on any Two of the followings.

i) Web Security

ii) S/MIME

iii) AES

निम्नलिखित में से किन्हीं दो पर संक्षिप्त टिप्पणियाँ लिखिए।

i) वेब सुरक्षा

ii) S/MIME

iii) AES

******