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

Roll No .....

CS-703 (A) (GS)

B.Tech., VII Semester

Examination, November 2023

Grading System (GS)

Cryptography and Information Security

Time : Three Hours

Maximum Marks : 70

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

ii) All questions carry equal marks.
सभी प्रश्नों 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) Describe Fermat's little theorem with an example. 7
फ़र्मेट के छोटे प्रमेय का उदाहरण सहित वर्णन करें।

   b) Define Cryptanalysis. Explain the concept of cryptanalysis on substitution cipher. 7
क्रिप्टएनालिसिस को परिभाषित करें। प्रतिस्थापन सिफर पर क्रिप्टएनालिसिस की अवधारणा समझाइए।

2. a) Illustrate DES algorithm with neat diagram. Explain S-box importance in DES. 7
साफ चित्र के साथ DES एल्गोरिथम का चित्रण करें। DES में एस–बॉक्स का महत्व बताइए।

   b) How to establish a shared secret between two parties using Diffie-Hellmann key exchange algorithm? Explain. 7
डिफी–हेलमैन कुंजी विनिमय एल्गोरिथम का उपयोग करके दो पक्षों के बीच एक साझा रहस्य कैसे स्थापित करें? व्याख्या करें।

3. a) Explain RSA algorithm? Give an example of encryption and decryption using RSA? 7
RSA एल्गोरिथम समझाइए। RSA का उपयोग करके एन्क्रिप्शन और डिक्रिप्शन का एक उदाहरण दें।

   b) Describe the Schnorr Identification Scheme in detail. 7
Schnorr पहचान योजना का विस्तार से वर्णन करें।

4. a) What are the types of attacks addressed by message authentication? What are the two levels of functionality the comprise a message authentication or digital signature mechanism? 7
संदेश प्रमाणीकरण द्वारा किस प्रकार के हमलों का समाधान किया जाता है? संदेश प्रमाणीकरण या डिजिटल हस्ताक्षर तंत्र में कार्यक्षमता के दो स्तर कौन से हैं?

   b) Describe the Digital Signature Standard (DSS) in detail. 7
डिजिटल हस्ताक्षर मानक (DSS) का विस्तार से वर्णन करें।

5. a) What is Firewall? Explain different types of firewalls in detail. 7
फ़ायरवॉल क्या है? विभिन्न प्रकार के फ़ायरवॉल के बारे में विस्तार से बताइए।

b) Write about the usage of Session keys, Public and Private keys in PGP. 7
PGP में सत्र कुंजियों, सार्वजनिक और निजी कुंजियों के उपयोग के बारे में लिखें।

6. a) Analyze the Cryptographic algorithms used in S-MIME. Explain S-MIME certification processing. 7
S-MIME में प्रयुक्त क्रिप्टोग्राफ़िक एल्गोरिथम का विश्लेषण करें। S-MIME प्रमाणन प्रसंस्करण के बारे में बताइए।

b) Discuss about Encapsulating Security Payload. 7
सुरक्षा पेलोड को एनकैप्सुलेट करने के बारे में चर्चा करें।

7. a) Explain different types of DoS attack understanding tools. https://www.rgpvonline.com 7
विभिन्न प्रकार के DoS आक्रमण समझने वाले उपकरणों की व्याख्या करें।

b) What is Steganography? Explain different types of Steganography. 7
स्टेग्नोग्राफ़ी क्या है? स्टेग्नोग्राफ़ी के विभिन्न प्रकार बताइए।

8. Write short notes on any Two: 14
i) Block Cipher
ii) Hash Function
iii) Transport Layer Security
iv) Foot Printing Tools

किन्हीं दो पर संक्षिप्त टिप्पणी लिखिए।
i) ब्लॉक सिफर
ii) हैश फ़ंक्शन
iii) परिवहन परत सुरक्षा
iv) फुट प्रिंटिंग उपकरण

******