Roll No .....

IT-801 (GS)

B.Tech., VIII Semester

Examination, May 2024

Grading System (GS)

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) Explain fabrication, interception, Non-Repudiation and Integrity in terms of security.
सुरक्षा के संदर्भ में निर्माण, अवरोधन, गैर–अस्वीकार और अखंडता की व्याख्या करें।

   b) Encrypt the following message using Caesar cipher with key = 1. Plaintext is "Laughter is the best medicine".
कुंजी = 1 के साथ सीज़र सिफर का उपयोग करके निम्न संदेश को एन्क्रिप्ट करें। प्लेनटेक्स्ट "Laughter is the best medicine"

2. a) Consider a plain text alphabet G. Using RSA algorithm and the value as $e=3$, $d=11$ and $n=15$, find out what this plain text alphabet encrypt to, and verify that upon decryption it transform back to G.

एक सादे पाठ वर्णमाला G पर विचार करें। RSA एल्गोरिथम और $e=3$, $d=11$ और $n=15$ के रूप में मान का उपयोग करके, यह पता लगाइए कि यह प्लेनटेक्स्ट वर्णमाला क्या एन्क्रिप्ट करता है, और सत्यापित करें कि डिक्रिप्शन पर यह वापस G में बदल जाता है।

   b) To find
पता लगाना
   i) 75 mod 119
   ii) 89 mod 119
   iii) Primitive root of 11
   iv) Primitive root of 5

3. a) Explain in detail the key generation in AES algorithm and its expansion format.
AES एल्गोरिथम में प्रमुख पीढ़ी और उसके विस्तार प्रारूप को विस्तार से समझाइए।

   b) Give the five modes of operation of Block cipher. Explain any two.
ब्लॉक सिफर के संचालन के पाँच तरीके दें। किन्हीं दो को समझाइए।

4. Evaluate using Diffie-Hellman key exchange technique. Users A and B use a common prime $q = 11$ and a primitive root alpha = 7.
   i) If user A has private key XA = 3. What is A's public key YA?
   ii) If user B has private key XB = 6. What is B's public key YB?
डिफी–हेलमैन की एक्सचेंज तकनीक का उपयोग करके मूल्यांकन करें। उपयोगकर्ता A और B एक सामान्य प्राइम $q = 11$ और एक आदिम रूट alpha = 7 का उपयोग करते हैं।
   i) यदि उपयोगकर्ता A के पास निजी कुंजी XA = 3 है। A की सार्वजनिक कुंजी YA क्या है?
   ii) यदि उपयोगकर्ता B के पास निजी कुंजी XB = 6 है। B की सार्वजनिक कुंजी YB क्या है?

5. a) Formulate what are the requirements of Kerberos? Explain about Kerberos version.
   तैयार करें कि केर्बेरोज (Kerberos) की आवश्यकताएं क्या हैं? केर्बेरोज वर्जन के बारे में बताइए।
   b) How does PGP provide confidentiality and authentication service for e-mail and file storage applications? Draw the block diagram and explain its components.
   PGP ई–मेल और फ़ाइल संग्रहण अनुप्रयोगों के लिए गोपनीयता और प्रमाणीकरण सेवा कैसे प्रदान करता है? ब्लॉक डायग्राम बनाइए और इसके घटकों को समझाइए।

6. a) Estimate what is the role of intrusion detection system. What are the three benefits that can be provided by the intrusion detection system?
   अनुमापन लगाइए कि घुसपैठ का पता लगाने वाली प्रणाली की क्या भूमिका है? घुसपैठ का पता लगाने वाली प्रणाली द्वारा प्रदान किए जा सकने वाले तीन लाभ क्या हैं?
   b) Illustrate the three common types of firewalls with diagrams.
   तीन सामान्य प्रकार के फायरवॉल को रेखाचित्रों की सहायता से समझाइए।

7. a) What are Viruses? Explain the virus related threats and the counter measures applied.
   वायरस क्या होते हैं? वायरस से संबंधित खतरों और लागू किए गए काउंटर उपायों की व्याख्या करें।
   b) What is secure electronic transaction and how it can be achieved?
   सुरक्षित इलेक्ट्रॉनिक लेनदेन क्या है और इसे कैसे प्राप्त किया जा सकता है?

8. Write a short notes (any three)
   संक्षिप्त टिप्पणियां लिखें (कोई तीन)
   a) DOS and DDOS attack
   b) Hash function
   c) Secure Socket Layer
   d) Steganography

******