Roll No .....

CY-302 (GS)

B.Tech., III Semester

Examination, June 2023

Grading System (GS)

Fundamental of Cryptography

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 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 is Perfect Secrecy in Crypto System? Explain. 9
क्रिप्टो सिस्टम में परफेक्ट सेक्रेसी क्या है? व्याख्या करें।

   b) Explain the purpose of One-Time Pad encryption? 5
वन–टाइम पैड एन्क्रिप्शन का उद्देश्य बताएं।

2. a) How does the DES algorithm work in cryptography? Discuss with suitable example. 10
क्रिप्टोग्राफी में DES एल्गोरिथम कैसे काम करता है? उपयुक्त उदाहरण सहित चर्चा कीजिए।

   b) What is Message Authentication Code (MAC)? Discuss about secure MAC. 4
मैसेज ऑथेंटिकेशन कोड (MAC) क्या है। सुरक्षित मैक के बारे में चर्चा करें।

3. a) What is Random Oracle Model in cryptography? Explain. 9
क्रिप्टोग्राफी में रैंडम ओरेकल मॉडल क्या है? व्याख्या करें।

   b) What do you mean by trapdoor attacks? Explain. 5
ट्रैपडोर अटैक से आपका क्या मतलब है? व्याख्या कीजिए।

4. a) Write the importance of Discrete Logarithms in Cryptography? 7
क्रिप्टोग्राफी में असतत लघुगणक का महत्व लिखिए।

   b) Explain the following? 7
   i) Authenticate
   ii) Confidentiality
   iii) Authorization
   निम्नलिखित की व्याख्या करें।
   i) प्रमाणीकरण
   ii) गोपनीयता
   iii) प्राधिकार

5. a) What is a SSL protocol? How many protocols are there in SSL discuss in detail. 9
SSL प्रोटोकॉल क्या है? SSL में कितने प्रोटोकॉल हैं विस्तार से चर्चा करें।

   b) Discuss the role of number theory used in Cryptography? 5
क्रिप्टोग्राफी में प्रयुक्त संख्या सिद्धांत की भूमिका पर चर्चा करें।

6. a) What is Symmetric vs. Asymmetric Encryption? Discuss. 6
सममित बनाम असममित एन्क्रिप्शन क्या है? चर्चा करना।

   b) Explain about AES algorithm with suitable example. 8
AES एल्गोरिथम के बारे में उपयुक्त उदाहरण सहित समझाइए।

7. a) Give an overview of Diffie-Hellman problem? Discuss about the main problem that Diffie-Hellman key exchange faces? 8

डिफी–हेलमैन समस्या का अवलोकन करें। मुख्य समस्या के बारे में चर्चा करें जिसका सामना डिफी–हेलमैन कुंजी एक्सचेंज करता है?

b) Write about One-way vs Two-way hash functions? 6

वन–वे बनाम टू–वे हैश फंक्शन के बारे में लिखें।

8. Explain any two of the following? 14

a) Transport Layer Security

b) Interactive protocols in Cryptography

c) Hybrid Cryptosystem

d) Hill Cipher

निम्नलिखित में से किन्हीं दो की व्याख्या करें।

अ) ट्रांसपोर्ट लेयर सुरक्षा

ब) क्रिप्टोग्राफी में इंटरएक्टिव प्रोटोकॉल

स) हाइब्रिड क्रिप्टोसिस्टम

द) हिल सिफर

******