Total No. of Questions : 8] *[Total No. of Printed Pages : 4*

Roll No .....

CS-703 (A) (GS)

B.Tech., VII Semester

Examination, November 2022

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) How do you convert a block cipher into a stream cipher by using the Cipher Feedback (CFB) mode? Explain.
सिफर फीडबैक (CFB) मोड का उपयोग करके आप किसी ब्लॉक सिफर को स्ट्रीम सिफर में कैसे बदलते हैं? समझाइए।

   b) Explain the concept of Cryptanalysis and Brute force attack.
क्रिप्टोनालिसिस और ब्रुट फोर्स अटैक का अवधारणा की व्याख्या करें।

2. a) Explain the steps for the Key Generation of DES algorithms.
DES एल्गोरिथम की कुंजी पीढ़ी के चरणों की व्याख्या करें।

   b) Give the structure of AES. Explain how Encryption/ Decryption is done in AES.
AES की संरचना दें। बताएं कि AES में एन्क्रिप्शन/डिक्रिप्शन कैसे किया जाता है?

3. a) State Chinese Remainder theorem and find X for the given set of congruent equations using CRT.
चीनी शेष प्रमेय को बताएं और CRT का उपयोग करके दिए गए सर्वांगसम समीकरणों के लिए X ज्ञात करें।

$X=1 \pmod 5$

$X=2 \pmod 7$

$X=3 \pmod 9$

$X=4 \pmod{11}$

   b) Explain in short different method of distribution of public key management.
सार्वजनिक कुंजी प्रबंधन के वितरण की विभिन्न विधियों को संक्षेप में समझाइए।

4. a) User A and B exchange the key using Diffie-Hellman algorithm. Assume á = 5, q = 11, $X_A = 2$ and $X_B = 3$. Find Y_A, Y_B and K.
उपयोगकर्ता A और B डिफी हेलमैन एल्गोरिथम का उपयोग करके कुंजी का आदान-प्रदान करते हैं। मान लीजिए á = 5, q = 11, $X_A = 2$ और $X_B = 3$। Y_A, Y_B और K खोजें।

   b) What is MD5? Explain MD5 with neat and clean diagram.
MD5 क्या है? MD5 को नीट और स्वच्छ चित्र द्वारा समझाइए।

5. a) Explain the Secure Hash Algorithm (SHA) with their Merit and Demerit.

सिक्योर हैश एल्गोरिथम (SHA) को उनकी योग्यता और अवगुण के साथ समझाइए।

b) Why does PGP compress the message? What are the reasons for compressing the signature but before encryption?

PGP मैसेज को कंप्रेस क्यों करता हैं? संपीड़ित करने के कारण क्या हैं हस्ताक्षर लेकिन एन्क्रिप्शन से पहले?

6. a) Explain the sequence of steps used in Secure Socket Layer handshake Protocol for establishing a new session. Draw a diagram which shows the action of Handshake Protocol.

एक नया सत्र स्थापित करने के लिए सिक्योर सॉकेट लेयर हैंडशेक प्रोटोकॉल में प्रयुक्त चरणों के अनुक्रम की व्याख्या करें। एक आरेख बनाएं जो हैंडशेक प्रोटोकॉल की क्रिया को दर्शाता है।

b) What is a Honeypot? Explain types of honeypot.

एक मधुशाला क्या है? हनीपोट के प्रकार समझाइए।

7. a) Explain in short different types of DoS Attack Understanding Tools.

विभिन्न प्रकार के DoS अटैक अंडरस्टैंडिंग टूल्स को संक्षेप में समझाइए।

b) Explain in short different types of Trojans detection tools.

विभिन्न प्रकार के ट्रोजन डिटेक्शन टूल्स को संक्षेप में समझाइए।

8. Write short notes on following(Any two):

a) Firewall and its types.

b) Digital Signature Standard (DSS)

c) Triple DES

d) Schnorr Identification Scheme with the discrete logarithm

निम्नलिखित पर संक्षिप्त टिप्पणी लिखिए। (कोई दो)

अ) फ़ायरवॉल और उसके प्रकार

ब) डिजिटल हस्ताक्षर मानक (DSS)

स) ट्रिपल डेस

द) असतत लघुगणक के साथ Schnorr पहचान योजना

******