Roll No:-

SEM-VI Diploma Exam 2023 (Even)
(Computer Science & Engineering) (Theory)
Computer Network Security (2018604A)

[Time: 3:00 Hours] [Max. Marks: 70]

- All questions are compulsory. (सभी प्रश्न अनिवार्य है।)
- Marks are mentioned on the right side of each question. (अंक सभी प्रश्न के दाई ओर अंकित किये है।)

Group (A) (ग्रुप -ए)

Q.1 Choose the most suitable answer from the following options. (सर्वाधिक उपर्युक्त विकल्प को चुनकर लिखें।) :- (1*20=20)

i. Which of the following is not an approach to computer security?
(निम्नलिखित में कौन सा कंप्यूटर सुरक्षा के लिए एक दृष्टिकोण नहीं है ?)
(a) Reactive approach (प्रतिक्रियाशील दृष्टिकोण)
(b) Proactive approach (पूर्वाग्रही दृष्टिकोण)
(c) Anticipatory approach (पूर्वानुमानित दृष्टिकोण)
(d) All of the above (उपरोक्त सभी)

ii. Which is the operational model of network security? (नेटवर्क सुरक्षा का संचालनिक मॉडल क्या है ?)
(a) CIA Triad (CIA त्रिकोण)
(b) Access Control Model (पहुंच नियंत्रण मॉडल)
(c) Bell - La Padula Model (बेल - लापाडुला मॉडल)
(d) None of the above (उपरोक्त में से कोई नहीं)

iii. Symmetric key cryptography uses the same key for which of the following?
(सिमेट्रिक कुंजी गुप्तिविज्ञान, निम्नलिखित में से किसके लिए समान कुंजी का उपयोग करता है?)
(a) Encryption and decryption (एन्क्रिप्शन और डिक्रिप्शन)
(b) Data compression (डेटा संक्षेपण)
(c) Data transmission (डेटा ट्रांसमिशन)
(d) Data storage (डेटा स्टोरेज)

iv. Assymetric key cryptography uses different keys for which of the following?
(असिमेट्रिक कुंजी गुप्तिविज्ञान निम्नलिखित में किसके लिए अलग- अलग कुंजी का उपयोग करता है?)
(a) Encryption and decryption (एन्क्रिप्शन और डिक्रिपशन)
(b) Data compression (डेटा संक्षेपण)
(c) Data transmission (डेटा ट्रांसमिशन)
(d) Data storage (डेटा स्टोरेज)

v. What is the mathematics of cryptography used for? (गुप्तिविज्ञान का गणित किसके लिए उपयोग किया जाता है?)
(a) To encrypt data (डेटा का एन्क्रिप्ट करने के लिए)
(b) To crock encryption (एन्क्रिप्शन को क्रैक करने के लिए)
(c) To analyze encrypted data (एन्क्रिपटेड डेटा का विश्लेषण करने के लिए)
(d) All of the above (उपरोक्त सभी)

vi. Which of the following is a block cipher mode used in DFS?
(निम्नलिखित में से कौन सा DFS में उपयोग किया जाने वाला ब्लॉक चाइफर मोड है?)
(a) ECB (b) CBC (c) CFB (d) OFB

vii. Blowfish is used in pratlice for which of the following?
(ब्लोफ़िश का व्यावासायिक उपयोग निम्नलिखित में से किसके लिए किया जाता है?)
(a) Data encryption (डेटा एन्क्रिप्शन)
(b) Data transmission (डेटा ट्रांसमिशन)
(c) Data compression (डेटा संक्षेपण)
(d) Data storage (डेटा स्टोरेज)

471F7640B45A230F7511C3438ED4809A

viii. Rcu is a symmetric- key encryption algorithm used for what purpose?
(Rcu सिमेट्रिक कुंजी एनक्रिप्शन -एल्गोरीदम का किस उद्देश्य के लिए उपयोग किया जाता है?)
(a) Data encryption(डेटा एन्क्रिप्शन)
(b) Data transmission (डेटा ट्रांसमिशन)
(c) Data compression (डेटा संक्षेपण)
(d) Data storage (डेटा स्टोरेज)

ix. What are Digital Certificates used for? (डिजिटल प्रमाणपत्र का उपयोग क्या होता है?)
(a) Data encryption (डेटा एन्क्रिप्शन)
(b) Data transmission (डेटा ट्रांसमिशन)
(c) Key generation (कुंजी उत्पादन)
(d) Authentication (प्रामाणीकरण)

x. What are cryptographic hash functions used for? (गुप्तिविज्ञानी हैश फंक्शन का उपयोग क्या किया जात
(a) Data encryption (डेटा एन्क्रिप्शन)
(b) Data transmission (डेटा ट्रांसमिशन)
(c) Data compression (डेटा संक्षेपण)
(d) Data integrity veri (डेटा की अखंडता के

xi. Which hashing scheme belongs to the SHA family? (कौन - सा हैशिंग स्कीम SHA-परिवार का है?)
(a) SHA-1 (b) SHA-256 (c) SHA-512 (d) All of the above (उपरोक्त सभी)

xii. Which security protocol is used to secure web communication?
(कौन -सा सुरक्षा प्रोटोकॉल वेब संचार को सुरक्षित करने के लिए उपयोग किया जाता है?)
(a) SSL (b) TLS (c) TSP (d) WAP Security (WAP सुर

xiii. Hashing Authentication & signature schemes are used for what purpose in network security?
(नेटवर्क सुरक्षा में हैशिंग प्रमाणीकरण और सिग्नेचर स्कीम का उपयोग किस उद्देश्य के लिए किया जाता है?)
(a) Data encryption (डेटा एन्क्रिपशन)
(b) Data transmission (डेटा ट्रांसमिशन)
(c) Data authentication (डेटा प्रमाणीकरण)
(d) Data compression (डेटा संक्षेपण)

xiv. What is SSL used for in network security?(नेटवर्क सुरक्षा SSL का उपयोग क्या होता है?)
(a) Secure data storage (सुरक्षित डेटा स्टोरेज)
(b) Secure data transmission (सुरक्षित डेटा ट्रांसमिशन)
(c) Secure data encryption (सुरक्षित डेटा एन्क्रिपशन
(d) Secure data compression (सुरक्षित डेटा संक्षेपण

xv. Firewall architecture is implemented for what purpose in systems security?
(सिस्टम सुरक्षा में फायरवॉल विन्यास का उद्देश्य क्या होता है?)
(a) To detect viruses and worms
(वायरस और कीड़े का पता लगाने के लिए)
(b) To protect against intruder
(चाकूबाज के खिलाफ सुरक्षा प्रदान करने के लिए)
(c) To encrypt data
(डेटा को एन्क्रिप्ट करने के लिए)
(d) To control network traffic
(नेटवर्क ट्रैफिक को नियंत्रित करने के लिए)

xvi. Trusted systems are used to ensure what in systems security?
(सिस्टम सुरक्षा में विश्वसनीय सिस्टम का उपयोग क्या सुनिश्चित करने के लिए किया जाता है?)
(a) Data encryption (डेटा एन्क्रिप्शन)
(b) Data transmission (डेटा ट्रांसमिशन)
(c) Data authentication (डेटा प्रमाणीकरण)
(d) Data integrity (डेटा की अखंडता)

xvii. Wireless security in Adhoc -networks is implemented for what purpose?
(ऐडहॉक - नेटवर्क में वायरलेस सुरक्षा का विन्यास किस उद्देश्य के लिए किया जाता है?)
(a) To detect viruses and worms
(वायरस और कीड़े का पता लगाने के लिए)
(b)To protect against intruders
(चाकूजबाज़ के खिलाफ सुरक्षा प्रदान करने के लिए)
(c) To encrypt data
(डेटा को एन्क्रिप्ट करने के लिए)
(d) To control network traffic
(नेटवर्क ट्रैफिक को नियंत्रित करने के लिए)

xviii. Which encryption algorithm is compared with AES in the overview of Rijndael?
(रिज़न्डेल के अवलोकन में AES के साथ तुलना मे कौन - सा एन्क्रिपशन एल्गोरिदम है?)

(a)RSA (b) DES (c) Blowfish (ब्लो फिश) (d) RC4

xix. Internet security protocols include which of the following?
(इंटरनेट सुरक्षा प्रोटोकॉल में निम्नलिखित में से कौन - सा शामिल है?)

(a) SSL (b) TSL (c) TSP (d) All of the above (उपरोक्त सभी)

xx. What are the types of attacks on computers and computer security?
(कंप्यूटरों और कंप्यूटर सुरक्षा पर होने वाले हमले किस प्रकार के होते है?)

(a) Physical attacks (भौतिक हमले) (b) cyber attacks (साइबर हमले) (c) Both (a) and (b) ((अ) और (ब) दोनों) (d) None of the above (उपरोक्त में से कोई नहीं)

Group (B) (ग्रुप -बी)

Q.2 What is SSL (Secure Socket Layer) and how does it provide security for web communication? 4
(SSL (सुरक्षित सॉकेट लेयर) क्या है, और यह वेब संचार के लिए सुरक्षा कैसे प्रदान करता है?)

OR (अथवा)

What are the challenges faced in cracking DES encryption and how does differential cryptanalysis help in this process? 4
(DES एन्क्रिपशन को क्रैक करने के लिए कौन सी चुनौतियों का सामना किया जाता है और इस प्रक्रिया में, डिफरेंशियल क्रिप्टएनालिसिस कैसे मदद करता है?)

Q.3 Discuss the mathematics of cryptography and its role in secure communication 4
(क्रिप्टोग्राफी की गणित और सुरक्षित संचार में इसकी भूमिका पर चर्चा करें।)

OR (अथवा)

What are the different types of attacks that can be launched on computer 4
(कंप्यूटर सिस्टमों पर शुरू किए जाने वाले विभिन्न प्रकार के हमलों क्या है?)

Q.4 Explore the application of DSS (Digital Signature Algorithm)and DSA (Digital Signature Algorithm) in secure communication 4
(सुरक्षित संचार में DSS (डिज़िटल सिग्नेचर एल्गोरिदम) और DSA (डिज़िटल सिग्नेचर एल्गोरिदम) के अनुप्रयोगों का पता करें ।)

OR (अथवा)

Compare the SHA family hashing schemes with MAC (Message Authentication Code) for data integrity verification. 4
(डेटा अखंडता सत्यापन के लिए SHA- परिवार हैशिंग योजनाओं को MAC (मैसेज प्रमाणीकरण कोड) के साथ तुलना करें)

Q.5 Explain the concept of cryptographic hash functions and their applications in data security. 4
(क्रिप्टोग्राफिक हैश फंक्शन की अवधारणा और डेटा सुरक्षा में इसके अनुप्रयोगों को समझाए ।)

OR (अथवा)

Explain the concept of internet security protocols and the role of SSL/TLS in secure web communication. 4
(इंटरनेट सुरक्षा प्रोटोकॉल की अवधारणा और सुरक्षित वेब संचार में SSL/TLS की भूमिका को समझाए ।)

Q.6 Explain the concept of symmetric key cryptography and its application in secure communication (सिमेट्रिक -की क्रिप्टोग्राफी की अवधारणा और सुरक्षित संचार में इसके अनुप्रयोगों की व्याख्या करें) 4

OR (अथवा)

Explain the working of DES (Data Encryption Standard) and its significances in cryptography? (DES (डेटा एन्क्रिप्शन स्टैंडर्ड) का काम कैसे होता है, और क्रिप्टोग्राफी में इसका महत्त्व क्या है ।) 4

Group (C) (ग्रुप - सी)

Q.7 Explain the operational model of network security and its components. (नेटवर्क सुरक्षा के संचालन मॉडल और इसके घटकों की व्याख्या करें ।) 6

OR (अथवा)

Explain the concept of computer security and the need for security in computer systems. (कंप्यूटर सुरक्षा अवधारणा और कंप्यूटर सिस्टम में सुरक्षा की आवश्यकता को समझाएं ।) 6

Q.8 Explain the concept of honeypots in systems security and their role in detecting and mitigating attacks. (सिस्टम सुरक्षा में हनीपोट्स की अवधारणा और हमलों का पता लगाने और इन्हें रोकने में उनकी भूमिका को समझाएं ।) 6

OR (अथवा)

Explore the practical applications of Blowfish in symmetric-key cryptography. (सिमेट्रिक-की क्रीप्टोग्राफी में ब्लोफिश के व्यावहारिक अनुप्रयोगों का पता करें ।) 6

Q.9 Discuss the different approaches and principles of computer security. (कंप्यूटर सुरक्षा के विभिन्न दृष्टिकोण और सिद्धांतों पर चर्चा करें) 6

OR (अथवा)

Discuss the concept of trusted systems and multilevel security in ensuring data confidentiality and integrity. (डेटा गोपनीयता और अखंडता सुनिश्चित करने मे विश्वसनीय सिस्टम और बहुस्तरीय सुरक्षा की अवधारणा पर चर्चा करें) 6

Q.10 Discuss the RSA encryption algorithm and its significance in asymmetric-key cryptography. (RSAएन्क्रिप्शन एल्गोरिदम पर चर्चा करें और एसिमेट्रिक की क्रिप्टोग्राफी में इसका महत्व समझाएं) 6

OR (अथवा)

Discuss the concept of digital signatures and their role in ensuing message authencity. (डिजिटल सिग्नेचर की अवधारणा और संदेश की प्रमाणिकता सुनिश्चित करने में इसकी भूमिका पर चर्चा करें।) 6

Q.11 Discuss the role of TLS (Transport Layer Security) in securing data transmission over a network (नेटवर्क पर डेटा ट्रांसमिशन को सुरक्षित करने में (ट्रांसपोर्ट लेयर सुरक्षा) की भूमिका पर चर्चा करें।) 6

OR (अथवा)

Explain the concept of wireless security and the measures taken to secure wireless networks and communication (वायरलेस सुरक्षा की अवधारणा और वायरलेस नेटवर्क और संचार को सुरक्षित करने के लिए उठाए गए उपयों की व्याख्या करें ।) 6

*****