Roll No:-_____

(Sem - VI) Diploma Exam 2024 (Even)

(C.S.E) (Theory)

[Time: 3 Hours] **Computer Network Security (2018604A)** **[Full. 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)

		Marks	CO	BL
Q.1	**Answer all questions as directed. (2x10=20)** **(निर्देशानुसार सभी प्रश्नों के उत्तर दें)**			
a)	Match the following terms with their descriptions: 1. Symmetric Key Cryptography — A. Encryption using the same key for both encryption and decryption 2. Asymmetric Key Cryptography — B. Encryption using a pair of public and private keys 3. DES (Data Encryption Standard) — C. A symmetric key encryption algorithm 4. RSA — D. An asymmetric encryption algorithm Digital Signature नीचे दिए गए शब्दों को उनके विवरण से मिलाएं: 1. सममित कुंजी क्रिप्टोग्राफी — A. एन्क्रिप्शन और डिक्रिप्शन के लिए एक ही कुंजी का उपयोग करना 2. असममित कुंजी क्रिप्टोग्राफी — B. सार्वजनिक और निजी कुंजियों की एक जोड़ी का उपयोग करके एन्क्रिप्शन 3. डीईएस (डाटा एन्क्रिप्शन स्टैंडर्ड) — C. एक सममित कुंजी एन्क्रिप्शन एल्गोरिथ्म 4. आरएसए — D. एक असममित एन्क्रिप्शन एल्गोरिथ्म	2	-	3
b)	SSL and TLS are protocols used for securing internet communications. (True/False) एसएसएल और टीएलएस इंटरनेट संचार को सुरक्षित करने के लिए उपयोग किए जाने वाले प्रोटोकॉल हैं। (सही/गलत)	2	-	2
c)	ECC stands for Elliptic Curve Cryptography. (True/ False) ईसीसी का मतलब एलिप्टिक कर्व क्रिप्टोग्राफी है। (सही/गलत)	2	-	2
d)	_____ is a cryptographic technique where the same key is used for both encryption and decryption.(Symmetric Key Cryptography /Asymmetric Key Cryptography /Hashing) _____ एक क्रिप्टोग्राफिक तकनीक है जहां एन्क्रिप्शन और डिक्रिप्शन के लिए एक ही कुंजी का उपयोग किया जाता है। (सममित कुंजी क्रिप्टोग्राफी/असममित कुंजी क्रिप्टोग्राफी/ हैशिंग)	2	-	2

e) The _____ is a widely used symmetric key block cipher. (DES/ RSA /ECC) _____ एक व्यापक रूप से उपयोग किया जाने वाला सममित कुंजी ब्लॉक सिफर है। (डीईएस/ आरएसए/ ईसीसी)	2	-	1
f) _____ is a public-key cryptosystem that is widely used for secure data transmission. (RSA / AES /Blowfish) _____ एक सार्वजनिक-कुंजी क्रिप्टोसिस्टम है जो सुरक्षित डेटा ट्रांसमिशन के लिए व्यापक रूप से उपयोग किया जाता है। (आरएसए/ एईएस/ब्लोफिश)	2	-	1
g) The _____ algorithm is used for creating a cryptographic hash value. (SHA / DES / SSL) _____ एल्गोरिथ्म का उपयोग एक क्रिप्टोग्राफ़िक हैश वैल्यू बनाने के लिए किया जाता है।(एसएचए/डीईएस/एसएसएल)	2	-	1
h) Viruses and worms are the same and cause the same type of damage. (True/False) वायरस और वर्म एक जैसे होते हैं और एक ही प्रकार की क्षति करते हैं। (सही/गलत)	2	-	2
i) Match the following terms with their descriptions: **1.** Digital Signature — A. A method for ensuring data integrity and authenticity **2.** SHA (Secure Hash Algorithm) — B. A cryptographic hash function **3.** Firewall — C. A network security device that monitors and controls incoming and outgoing network traffic नीचे दिए गए शब्दों को उनके विवरण से मिलाएं: **1.** डिजिटल हस्ताक्षर — A. डेटा की अखंडता और प्रामाणिकता सुनिश्चित करने की विधि **2.** एसएचए (सिक्योर हैश एल्गोरिथ्म) — B. एक क्रिप्टोग्राफ़िक हैश फ़ंक्शन **3.** फ़ायरवॉल — C. एक नेटवर्क सुरक्षा उपकरण जो इनकमिंग और आउटगोइंग नेटवर्क ट्रैफ़िक की निगरानी और नियंत्रण करता है	2	-	3
j) _____ is a security protocol that provides secure communications on the internet. (SSL/ IPsec /DES) _____ एक सुरक्षा प्रोटोकॉल है जो इंटरनेट पर सुरक्षित संचार प्रदान करता है। (एसएसएल/आईपीसेक/ डीईएस)	2	-	2

Group (B) (ग्रुप -बी)

Answer all five questions. (सभी पाँच प्रश्नों के उत्तर दें|) **4x5=20**

Q.2 Describe the different types of attacks on computer systems and networks. कंप्यूटर सिस्टम और नेटवर्क पर विभिन्न प्रकार के हमलों का वर्णन करें।	4	-	2
OR (अथवा)	4	-	2

	Explain the principles of cryptography and how they contribute to secure communications. क्रिप्टोग्राफी के सिद्धांतों की व्याख्या करें और वे सुरक्षित संचार में कैसे योगदान करते हैं।			
Q.3	Discuss the operational model of network security with examples. उदाहरण सहित नेटवर्क सुरक्षा का परिचालन मॉडल समझाएँ।	4	-	2
	OR (अथवा)			
	Explain the concept of substitution and transposition in cryptography with examples. क्रिप्टोग्राफी में प्रतिस्थापन और स्थानांतरण की अवधारणा को उदाहरण के साथ समझाएं।	4	-	2
Q.4	Describe the working of the DES algorithm. डीईएस एल्गोरिथ्म के कार्य करने का तरीका बताएं।	4	-	3
	OR (अथवा)			
	Discuss the process and challenges of cracking DES. डीईएस को क्रैक करने की प्रक्रिया और चुनौतियों पर चर्चा करें।	4	-	2
Q.5	Describe the principles of differential cryptanalysis. डिफरेंशियल क्रिप्टानालिसिस के सिद्धांतों का वर्णन करें।	4	-	2
	OR (अथवा)			
	Explain the concept of a Feistel cipher and its role in DES. फिस्टेल सिफर की अवधारणा और डीईएस में इसकी भूमिका समझाएं।	4	-	2
Q.6	Compare and contrast AES with other symmetric key algorithms like Blowfish and RC4. एईएस की तुलना अन्य सममित कुंजी एल्गोरिदम जैसे ब्लोफिश और आरसी4 से करें।	4	-	3
	OR (अथवा)			
	Explain the working of RSA encryption and its use in digital communications. आरएसए एन्क्रिप्शन कैसे काम करता है**,** और इसे डिजिटल संचार में कैसे उपयोग किया जाता है**?**	4	-	2
	Group (C) (ग्रुप - सी)			
	Answer all five questions. (सभी पाँच प्रश्नों के उत्तर दें।) **6x5=30**	6	-	2
Q.7	Discuss the role of Galois Field theory in cryptography, including its applications in AES. गैलोइस फील्ड सिद्धांत और इसके क्रिप्टोग्राफी में अनुप्रयोगों की चर्चा करें, जिनमें एईएस भी शामिल है।			
	OR (अथवा)			
	Compare and contrast AES with other symmetric key algorithms highlighting their strengths and weaknesses. एईएस की तुलना अन्य सममित कुंजी एल्गोरिदम से करें, उनके मजबूत और कमजोर पक्षों को हाइलाइट करते हुए।	6	-	3
Q.8	Explain the working of RSA encryption, including its mathematical foundations and practical applications. आरएसए एन्क्रिप्शन के कार्य करने की विधि, इसके गणितीय आधार और व्यावहारिक अनुप्रयोगों की व्याख्या करें।	6	-	2
	OR (अथवा)			
	Discuss the importance of digital certificates and Public Key Infrastructure (PKI) in secure communications. सुरक्षित संचार में डिजिटल प्रमाणपत्र और सार्वजनिक कुंजी अवसंरचना (पीकेआई) के महत्व की चर्चा करें।	6	-	2

Q.9	Explain the SHA-family of hashing algorithms, including their design, applications, and vulnerabilities. एसएचए-परिवार के हैशिंग एल्गोरिदम का वर्णन करें, जिनमें उनका डिज़ाइन, अनुप्रयोग और कमजोरियां शामिल हैं।	6	-	3
	OR (अथवा)			
	Describe the process of creating and verifying a digital signature using RSA and DSS/DSA. आरएसए और डीएसएस/डीएसए का उपयोग करके डिजिटल हस्ताक्षर बनाने और सत्यापित करने की प्रक्रिया का वर्णन करें।	6	-	2
Q.10	Discuss the role of authentication protocols in network security. नेटवर्क सुरक्षा में प्रमाणीकरण प्रोटोकॉल की भूमिका की चर्चा करें|	6	-	2
	OR (अथवा)			
	Explain the architecture and working of IPsec, and how it secures data transmission over the internet. आईपीसेक की आर्किटेक्चर और कार्यप्रणाली की व्याख्या करें, और यह इंटरनेट संचार को कैसे सुरक्षित करता है।	6	-	2
Q.11	Compare SSL and TLS protocols, including their roles in securing web communications and their differences. एसएसएल और टीएलएस प्रोटोकॉल की तुलना करें, जिनमें उनकी भूमिका, वेब संचार को सुरक्षित करने में उनके योगदान और उनके अंतर शामिल हैं।	6	-	3
	OR (अथवा)			
	Discuss the importance of email security protocols and how they protect sensitive information. ईमेल सुरक्षा प्रोटोकॉल के महत्व की चर्चा करें और वे संवेदनशील जानकारी की सुरक्षा कैसे करते हैं।	6	-	3

----------*****----------