Roll No:-_____

Sem-VI Diploma Exam 2024 (Even)
(C.S.E)(Theory)

[Time: 3 Hours] **Computer Network Security (2018604A)** **[Full. Marks: 70]**

(1) प्रश्न में कुल III खण्ड है। जिनका उत्तर उत्तर-पुस्तिका में लिखना अनिवार्य है।

(2) खण्ड I से सभी 10. II से सभी ५ एवं III से सभी ५ प्रश्न का उत्तर अनिवार्य है।

(3) खण्ड I के प्रत्येक प्रश्न का मान २, खण्ड II के प्रत्येक प्रश्न का मान ४ एवं खण्ड III के प्रत्येक प्रश्न का मान 6 अंको का है।

Group (A) (ग्रुप -ए)

Q.1	**Answer all questions as directed.** **(निर्देशानुसार सभी प्रश्नों के उत्तर दें)** **(2x10=20)**	Marks	CO	BL
a)	Identify the odd one out: a) Need for security b) Cryptography concepts and techniques c) Key range size d) Substitution transposition इनमें से बेजोड़ को पहचानें: ए) सुरक्षा की आवश्यकता बी) क्रिप्टोग्राफी अवधारणाएं और तकनीकें सी) कुंजी श्रेणी का आकार डी) प्रतिस्थापन स्थानान्तरण	2	-	2
b)	Find the odd one out: a) Symmetric key cryptography b) Asymmetric key cryptography c) Types of attacks d) Key range size बेजोड़ का पता लगाएं: ए) सममित कुंजी क्रिप्टोग्राफी बी) असममित कुंजी क्रिप्टोग्राफी सी) हमलों के प्रकार डी) कुंजी श्रेणी का आकार	2	-	2
c)	The Data Encryption Standard (DES) is a _____ cipher that operates on _____-bit blocks of plaintext. (block, 64/block, 32/block, 16) डेटा एन्क्रिप्शन स्टैंडर्ड (डीईएस) एक _____ सिफर है जो प्लेनटेक्स्ट के _____-बिट ब्लॉक पर काम करता है। (ब्लॉक, 64/ब्लॉक, 32/ब्लॉक, 16)	2	-	2
d)	The working of DES involves multiple rounds of permutation, substitution, and _____ operations. (XNOR/XOR/OR) DES की कार्यप्रणाली में क्रमपरिवर्तन, प्रतिस्थापन और _____ संचालन के कई दौर शामिल हैं। (XNOR/XOR/OR)	2	-	1

e) Match the following symmetric ciphers with their names: a. Rijndael 1) AES b. RC5 2) Block cipher in RC series c. RC6 3) Successor of RC5, developed by RSA Security निम्नलिखित सममित सिफरों को उनके नामों से मिलाएँ: ए। रिजेंडेल 1) एईएस बी। आरसी5 2) आरसी श्रृंखला में ब्लॉक सिफर सी। आरसी6 3) आरएसए सिक्योरिटी द्वारा विकसित आरसी5 का उत्तराधिकारी	2	-	3
f) In Asymmetric-Key Cryptography, _____ is a widely-used algorithm based on the difficulty of factoring large prime numbers. (RSA/DSA/SSA) असममित-कुंजी क्रिप्टोग्राफी में, _____ बड़े अभाज्य संख्याओं के गुणनखंडन की कठिनाई पर आधारित एक व्यापक रूप से उपयोग किया जाने वाला एल्गोरिदम है। (आरएसए/डीएसए/एसएसए)	2	-	2
g) _____ are used to verify the authenticity of digital entities and facilitate secure communication over networks. (Digital certificates/Digital signature/Digital pen) _____ का उपयोग डिजिटल संस्थाओं की प्रामाणिकता को सत्यापित करने और नेटवर्क पर सुरक्षित संचार की सुविधा के लिए किया जाता है। (डिजिटल प्रमाणपत्र/डिजिटल हस्ताक्षर/डिजिटल पेन)	2	-	1
h) DSA stands for _____. (Digital Signature Algorithm/Digital Signature Analysis/Digitally Signature Algorithm) DSA का मतलब _____ है। (डिजिटल हस्ताक्षर एल्गोरिदम/डिजिटल हस्ताक्षर विश्लेषण/डिजिटल हस्ताक्षर एल्गोरिदम)	2	-	1
i) In Network Security, _____ is a protocol used to provide secure communication over the internet, often used for securing websites. (SSL (Secure Sockets Layer)/DSA(Digital Signature Algorithm)) नेटवर्क सुरक्षा में, _____ एक प्रोटोकॉल है जिसका उपयोग इंटरनेट पर सुरक्षित संचार प्रदान करने के लिए किया जाता है, जिसका उपयोग अक्सर वेबसाइटों को सुरक्षित करने के लिए किया जाता है। (एसएसएल (सिक्योर सॉकेट लेयर)/डीएसए (डिजिटल सिग्नेचर एल्गोरिथम))	2	-	1
j) _____ are security mechanisms designed to attract and detect unauthorized access attempts on a network. (Honeypots/Honeyballs/Mudpots) _____ सुरक्षा तंत्र हैं जो किसी नेटवर्क पर अनधिकृत पहुंच प्रयासों को आकर्षित करने और उनका पता लगाने के लिए डिज़ाइन किए गए हैं। (हनीपोट/हनीबॉल/मडपोट)	2	-	1

Group (B) (ग्रुप -बी)

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

Q.2 Discuss the primary goal of computer security, and why is it important. कंप्यूटर सुरक्षा के प्राथमिक लक्ष्य पर चर्चा करें और यह महत्वपूर्ण क्यों है?	4	-	2

	OR (अथवा) Discuss two common approaches to ensuring computer security. कंप्यूटर सुरक्षा सुनिश्चित करने के लिए दो सामान्य दृष्टिकोण पर चर्चा करें ।	4	-	2
Q.3	Explain three principles that underlies computer security practices. कंप्यूटर सुरक्षा प्रथाओं को रेखांकित करने वाले तीन सिद्धांतों की व्याख्या करें।	4	-	2
	OR (अथवा) Explain different types of cyberattack on computer systems. कंप्यूटर सिस्टम पर विभिन्न प्रकार के साइबर हमले की व्याख्या करें।	4	-	2
Q.4	Discuss the concept of Feistel ciphers in block ciphers. ब्लॉक सिफर में फिस्टेल सिफर की अवधारणा पर चर्चा करें ।	4	-	2
	OR (अथवा) Discuss the concept of DES and how does it work. डीईएस स्टैंड की अवधारणा पर चर्चा करें और यह कैसे काम करता है.	4	-	2
Q.5	Explain the purpose of the Triple DES (3DES) encryption method. ट्रिपल डीईएस (3डीईएस) एन्क्रिप्शन विधि का उद्देश्य बताएं.	4	-	1
	OR (अथवा) Mention one side channel attack on cryptographic systems. क्रिप्टोग्राफ़िक सिस्टम पर वन साइड चैनल हमले का उल्लेख करें।	4	-	1
Q.6	Compare between Symmetric Key Cryptography and Asymmetric Key Cryptography, सममित कुंजी क्रिप्टोग्राफी और असममित कुंजी क्रिप्टोग्राफी के बीच तुलना करें,	4	-	3
	OR (अथवा) Compare AES and Rijndael in terms of their cryptographic characteristics. उनकी क्रिप्टोग्राफ़िक विशेषताओं के संदर्भ में एईएस और रिजेंडेल की तुलना करें।	4	-	3
	Group (C) (ग्रुप - सी)			
	Answer all five questions. (सभी पाँच प्रश्नों के उत्तर दें ।) **6x5=30**	6	-	2
Q.7	Explain Side channel attack with examples. साइड चैनल अटैक को उदाहरण सहित समझाइये।			
	OR (अथवा)			
	Explain the working principle of the Mobile IPSec. मोबाइल आईपीएसईसी के कार्य सिद्धांत की व्याख्या करें।	6	-	2
Q.8	Compare the AES encryption algorithm with another symmetric cipher of your choice. एईएस एन्क्रिप्शन एल्गोरिदम की तुलना अपनी पसंद के किसी अन्य सममित सिफर से करें।	6	-	3
	OR (अथवा) Elaborate the working principle of Virtual Private Network. वर्चुअल प्राइवेट नेटवर्क के कार्य सिद्धांत को समझाइये।	6	-	3
Q.9	Explain Elliptic curve cryptography in detail. एलिप्टिक वक्र क्रिप्टोग्राफी को विस्तार से समझाइए।	6	-	2

	OR (अथवा)			
	Explain how RSA works in asymmetric-key cryptography. बताएं कि आरएसए असममित–कुंजी क्रिप्टोग्राफी में कैसे काम करता है।	6	-	3
Q.10	Discuss the concept of digital certificates and their role in Public Key Infrastructure (PKI). डिजिटल प्रमाणपत्रों की अवधारणा और सार्वजनिक कुंजी अवसंरचना (पीकेआई) में उनकी भूमिका पर चर्चा करें।	6	-	2
	OR (अथवा)			
	Describe the purpose and operation of hashing schemes, including SHA-family. SHA-परिवार सहित हैशिंग योजनाओं के उद्देश्य और संचालन का वर्णन करें।	6	-	2
Q.11	Compare various symmetric key cryptography algorithms. विभिन्न सममित कुंजी क्रिप्टोग्राफी एल्गोरिदम की तुलना करें।	6	-	4
	OR (अथवा)			
	Compare various Internet security protocols such as SSL, TLS, and IPsec. एसएसएल, टीएलएस और आईपीसेक जैसे इंटरनेट सुरक्षा प्रोटोकॉल की तुलना करें और अंतर बताएं।	6	-	4

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