No. of Printed Pages : 8

1018

CS308/IT308

Roll No. : .....

Spl. 2020

INTRODUCTION TO NETWORK SECURITY AND CRYPTOGRAPHY

निर्धारित समय : तीन घंटे] [अधिकतम अंक : 70

Time allowed : Three Hours] **[Maximum Marks : 70**

नोट : (i) *प्रथम प्रश्न अनिवार्य है, शेष में से किन्हीं* ***चार*** *के उत्तर दीजिये ।*

Note : *Question No. 1 is compulsory, answer any* ***FOUR*** *questions from the remaining.*

(ii) *प्रत्येक प्रश्न के सभी भागों को क्रमवार एक साथ हल कीजिये ।*
Solve all parts of a question consecutively together.

(iii) *प्रत्येक प्रश्न को नये पृष्ठ से प्रारम्भ कीजिये ।*
Start each question on fresh page.

(iv) *दोनों भाषाओं में अन्तर होने की स्थिति में अंग्रेजी अनुवाद ही मान्य है ।*
Only English version is valid in case of difference in both the languages.

1. (1) सीज़र सिफर इसका एक उदाहरण है

(a) पॉली-अल्फाबेटिक सिफर (b) मोनो – अल्फाबेटिक सिफर

(c) मल्टी-अल्फाबेटिक सिफर (d) द्वि-अल्फोबेटिक सिफर

Caesar cipher is an example of

(a) Poly-alphabetic Cipher (b) Mono-alphabetic Cipher

(c) Multi-alphabetic Cipher (d) Bi-alphabetic Cipher

(2) क्रिप्टानालिसिस का उपयोग किया जाता है

(a) क्रिप्टोग्राफिक स्कीम में कुछ असुरक्षा का पता लगाने के लिए

(b) गति बढ़ाने के लिए

(c) डेटा एन्क्रिप्ट करने के लिए

(d) नये सिफर बनाने के लिए

Cryptanalysis is used _____.

(a) to find some insecurity in a cryptographic scheme.

(b) to increase the speed.

(c) to encrypt the data.

(d) to make new ciphers.

(3) प्लेन टक्स्ट को अपठनीय टेक्स्ट में बदलने की प्रक्रिया

(a) एन्क्रिप्शन (b) डिक्रिप्शन

(c) नेटवर्क सुरक्षा (d) सूचना छिपाना

The process of transforming plain text into unreadable text

(a) Encryption (b) Decryption

(c) Network Security (d) Information Hiding

(4) _____ एक संख्या या संख्याओं का एक समूह है जिस पर सिफर संचालित होता है ।

(a) सिफर (b) सीक्रेट

(c) कुंजी (d) उपरोक्त में से कोई नहीं

The _____ is a number or a set of numbers on which the cipher operates.

(a) Cipher (b) Secret

(c) Key (d) None of the above

(5) _____ सिफर में, एक ही कुंजी का उपयोग प्रेषक और रिसीवर दोनों द्वारा किया जाता है ।

(a) सममित-कुंजी (b) असममित-कुंजी

(c) या तो (a) या (b) (d) न (a) और ना ही (b)

In a(n) _____ cipher, the same key is used by both the sender and receiver.

(a) Symmetric key (b) Asymmetric key

(c) either (a) or (b) (d) Neither (a) nor (b)

(6) निम्नलिखित में से कौन डेटा सुरक्षा का सिद्धान्त नहीं है ?

(a) डेटा की गोपनीयता (b) डेटा अखंडता

(c) प्रमाणीकरण (d) इनमें से कोई नहीं

Which of the following is not a principle of data security ?

(a) Data Confidentiality (b) Data Integrity

(c) Authentication (d) None of the above

(7) असममित-कुंजी में, प्रेषक _____ कुंजी का उपयोग करता है ।

(a) निजी कुंजी (b) सार्वजनिक कुंजी

(c) या तो (a) या (b) (d) ना (a) और ना ही (b)

In an asymmetric-key, the sender uses the _____ Key.

(a) Private Key (b) Public Key

(c) Either (a) or (b) (d) Neither (a) nor (b)

(8) एक असममित-कुंजी में, रिसीवर _____ कुंजी का उपयोग करता है ।

(a) निजी कुंजी (b) सार्वजनिक कुंजी

(c) या तो (a) या (b) (d) न (a) और ना ही (b)

In an asymmetric-key, the receiver uses the _____ key.

(a) Private Key (b) Public Key

(c) Either (a) or (b) (d) Neither (a) nor (b)

(9) निम्नलिखित में से कौन सा हमला एक निष्क्रिय हमला है ?

(a) छद्मवेष हमला (b) संदेश का संशोधन

(c) सेवा से इनकार (d) ट्रेफिक विश्लेषण

Which of the following attacks is a passive attack ?

(a) Masquerade attack (b) Modification of message

(c) Denial of service (d) Traffic analysis

(10) निम्नलिखित में से कौन सा विकल्प ब्रूट बल हमले को सही ढ़ंग से परिभाषित करता है ?

(a) पिन और पासवर्ड जैसी उपयोगी जानकारी साझा करने के लिए उपयोगकर्ता को क्रूरता से मजबूर करना ।

(b) संदेश को डिक्रिप्ट करने के लिए हर मुमकिन कोशिश करना ।

(c) एक इकाई कुछ अन्य इकाई होने का दिखावा करती है ।

(d) रिसीवर को भेजने से पहले संदेश या सूचना को संशोधित किया जाता है ।

Which of the following options correctly defines the Brute Force attack ?

(a) Brutally forcing the user to share the useful information like pins and passwords.

(b) Trying every possible key to decrypt the message.

(c) One entity pretends to be some other entity.

(d) The message or information is modified before sending it to the receiver.

(11) संदेश _____ का अर्थ है कि रिसीवर सुनिश्चित करता है कि संदेश किसी अन्य प्रेषक से नही, बल्कि इच्छित प्रेषक से ही आ रहा है ।

(a) गोपनीयता (b) अखंडता

(c) प्रमाणीकरण (d) उपरोक्त में से कोई नहीं

Message _____ means that the receiver is ensured that message is coming from the intended sender, not an impostor.

(a) Confidentiality (b) Integrity

(c) Authentication (d) None of the above

(12) एक _____ का उपयोग किसी दस्तावेज या संदेश की अखंडता को बनाये रखने के लिए किया जा सकता है ।

(a) संदेश डाइजेस्ट (b) संदेश सारांश

(c) एन्क्रिप्टेड संदेश (d) उपरोक्त में से कोई नहीं

A(n) _____ can be used to preserve the integrity of a document or message.

(a) Message Digest (b) Message Summary

(c) Encrypted Message (d) None of the above

(13) संदेश _____ का अर्थ है कि प्रेषक और रिसीवर गोपनीयता की अपेक्षा करते हैं ।

(a) गोपनीयता (b) अखंडता

(c) प्रमाणीकरण (d) उपरोक्त में से कोई नहीं

Message _____means that the sender and the receiver expect privacy.

(a) Confidentiality (b) Integrity

(c) Authentication (d) None of the above

(14) निम्न में से कौन सा एक एंटी–वायरस प्रोग्राम है ।

(a) नॉर्टन (b) के 7

(c) क्विक हील (d) उपरोक्त सभी

Which of the following is an anti-virus program ?

(a) Norton (b) K7

(c) Quick Heal (d) All of above

(15) यह एक प्रोग्राम या हार्डवेयर डिवाइस है जो इन्टरनेट कनेक्शन के माध्यम से आने वाली सूचनाओं को किसी नेटवर्क या कम्प्यूटर सिस्टम में फिल्टर करता है ।

(a) एंटी–वायरस (b) कुकीज़

(c) फायरवॉल (d) साइबर सुरक्षा

It is a program or hardware device that filters the information coming through an internet connection to a Network or Computer System

(a) Anti-Virus (b) Cookies

(c) Firewall (d) Cyber Safety

(16) यह विज़िट की गई वेबसाइट को उपयोगकर्ता के कम्प्यूटर पर उपयोगकर्ता के बारे में अपनी जानकारी संग्रहित करने की अनुमति देता है

(a) स्पैम (b) कुकीज़

(c) मालवेयर (d) एडवेयर

It allows a visited website to store its own information about a user on the user's computer

(a) Spam (b) Cookies

(c) Malware (d) Adware

(17) यदि कम्प्यूटर सिस्टम सुलभ नहीं है, तो निम्न में से किस सिद्धान्त का उल्लंघन किया गया है ?

(a) गोपनीयता (b) उपलब्धता

(c) अभिगम नियंत्रण (d) प्रमाणीकरण

Which of the following principle is violated if computer system is not accessible ?

(a) Confidentiality (b) Availability

(c) Access Control (d) Authentication

(18) फ़ायरवॉल लागू किया जा सकता है

(a) राउटर्स जो इंट्रानेट को इंटरनेट से जोड़ते हैं ।

(b) इंट्रानेट में उपयोग किये जाने वाले ब्रिड्ज

(c) महँगा मोडेम

(d) उपयोगकर्ता के एप्लीकेशन प्रोग्राम

A firewall may be implemented in

(a) Routers which connect Intranet to Internet

(b) Bridges used in an Intranet

(c) Expensive Modem

(d) User's application programs

(19) PGP को _____ के रूप में संक्षिप्त किया गया है ।

(a) Powerful Good Privacy (b) Protocol Giving Privacy
(c) Pretty Good Protocol (d) Pretty Good Privacy

PGP is abbreviated as _____

(a) Powerful Good Privacy (b) Protocol Giving Privacy
(c) Pretty Good Protocol (d) Pretty Good Privacy

(20) निम्न में से कौन सी एक सुरक्षित मेल ट्रांसफरिंग कार्यप्रणाली नहीं है ?

(a) POP3 (b) SSMTP
(c) PGP का उपयोग करके मेल (d) S/MIME

Which of the following is not a secured mail transferring methodology ?

(a) POP3 (b) SSMTP
(c) Mail using PGP (d) S/MIME

(21) SSL मुख्य रूप से _____ पर केंद्रित है ।

(a) अखंडता और प्रामाणिकता (b) अखंडता और गैर-प्रत्यावर्तन
(c) प्रामाणिकता और गोपनीयता (d) गोपनीयता और अखंडता

SSL primarily focuses on _____

(a) integrity and authenticity (b) integrity and non-repudiation
(c) authenticity and privacy (d) confidentiality and integrity

(22) _____ का उपयोग नेटवर्क स्तर पर डेटा एन्क्रिप्ट करने के लिए किया जाता है ।

(a) IPSec (b) HTTPS (c) SMTP (d) S/MIME

_____ is used for encrypting data at network layer.

(a) IPSec (b) HTTPS (c) SMTP (d) S/MIME

(23) S/MIME को _____ के रूप में संक्षिप्त किया गया है ।

(a) सुरक्षित/मल्टीमीडिया इंटरनेट मेलिंग एक्सटेंशन
(b) सुरक्षित / बहुउद्देशीय इंटरनेट मेलिंग एक्सटेंशन
(c) सुरक्षित / मल्टीमीडिया इंटरनेट मेल एक्सटेंशन
(d) सुरक्षित / बहुउद्देशीय इंटरनेट मेल एक्सटेंशन

S/MIME is abbreviated as _____.

(a) Secure/Multimedia Internet Mailing Extensions
(b) Secure/Multipurpose Internet Mailing Extensions
(c) Secure/Multimedia Internet Mail Extensions
(d) Secure/Multipurpose Internet Mail Extensions

(24) वीपीएन सिस्टम को वर्गीकृत करने के लिए कौन से कथन सही नहीं हैं ?

(a) ट्रैफिक को टनल करने के लिए उपयोग किये जाने वाले प्रोटोकॉल ।
(b) वीपीएन साइट-टू-साइट या रिमोट एक्सेस कनेक्शन प्रदान कर रहे हैं ।
(c) बॉट और मालवेयर से नेटवर्क को सुरक्षित करना ।
(d) निजी रूप से डेटा भेजने और प्राप्त करने के लिए प्रदान की गई सुरक्षा के स्तर ।

Which of the statements are not true to classify VPN Systems ?

(a) Protocols used for tunnelling the traffic.
(b) VPNs are providing site-to-site or remote access connection.
(c) Securing the network from bots and malwares.
(d) Levels of security provided for sending and receiving data privately.

(25) डिजिटल हस्ताक्षर एक गणितीय तकनीक है जो मान्य होती है

(a) प्रामाणिकता (b) अखंडता (c) गैर-प्रतिक्षेप (d) उपरोक्त सभी

A digital signature is a mathematical technique which validates

(a) Authenticity (b) Integrity
(c) Non-repudiation (d) All of the above

(26) SSL की ऊपरी परत पर, प्रारंभिक प्रमाणीकरण और एन्क्रिप्शन कुंजी के हस्तांतरण के लिए एक प्रोटोकॉल, जिसे _____ कहा जाता है ।

(a) SSL Handshake Protocol (b) SSL Authentication Protocol
(c) SSL Record Protocol (d) SSL Cipher Protocol

On the upper layer of SSL, a protocol for initial authentication and transfer of encryption keys, called the _____.

(a) SSL Handshake Protocol (b) SSL Authentication Protocol
(c) SSL Record Protocol (d) SSL Cipher Protocol

(27) नेटवर्क स्तर पर एक पैकेट के लिए सुरक्षा प्रदान करने के लिए इंटरनेट इंजीनियरिंग टास्क फोर्स (IETF) द्वारा डिज़ाइन किये गये प्रोटोकॉल का एक संग्रह _____ है ।

(a) IPsec (b) नेटसेक (c) पैकेटसेक (d) प्रोटोकॉलसेक

The _____ is a collection of protocols designed by Internet Engineering Task Force (IETF) to provide security for a packet at the network level.

(a) IPsec (b) Netsec (c) Packetsec (d) Protocolsec

(28) टनल मोड में IPsec _____ की सुरक्षा करता है ।

(a) संपूर्ण आइ पी पैकेट (b) आई पी हेडर
(c) आईपी पेलोड (d) आईपी ट्रेलर

In tunnel mode, IPsec protects the _____.

(a) Entire IP packet (b) IP header
(c) IP payload (d) IP trailer

(29) नेटवर्क लेयर फ़ायरवॉल में _____ नामक दो उप-श्रेणियाँ हैं ।

(a) स्टेटफुल फ़ायरवॉल और स्टेटलेस फ़ायरवॉल
(b) बिट-उन्मुख फ़ायरवॉल और बाइट-उन्मुख फ़ायरवॉल
(c) फ्रेम फ़ायरवॉल और पैकेट फ़ायरवॉल
(d) नेटवर्क फ़ायरवॉल और डेटा फ़ायरवॉल

Network layer firewall has two sub-categories called _____.

(a) Stateful firewall and stateless firewall
(b) bit-oriented firewall and byte-oriented firewall
(c) Frame firewall and packet firewall
(d) Network firewall and data firewall

(30) अपने इच्छित उपयोगकर्ताओं के लिए कम्प्यूटर संसाधन उपलब्ध नहीं करने का प्रयास _____ कहलाता है ।

(a) सेवा इनकार का हमला (b) वायरस का हमला
(c) कीड़े का हमला (d) बॉटनेट प्रक्रिया

An attempt to make a computer resource unavailable to its intended users is called _____.

(a) denial of service attack (b) Virus attack
(c) worms attack (d) botnet process **(1×30)**

2. निम्न को समझाइए :

Explain the following :

(i) क्रिप्टोग्राफी

Cryptography

(ii) एन्क्रिप्शन और डिक्रिप्शन

Encryption and Decryption

(iii) गोपनीयता की अवधारणा

Concept of confidentiality

(iv) कम्प्यूटर सुरक्षा की आवश्यकता

Need of computer security

(v) प्रीटी गुड प्राइवेसी (पीजीपी)

Pretty Good Privacy (PGP) **(2×5)**

3. (i) कम्प्यूटर सुरक्षा के सिद्धान्तों की व्याख्या कीजिए ।

Explain the principles of Computer Security.

(ii) सक्रिय और निष्क्रिय हमलों के बीच पाँच अंतर लिखिए ।

Write down the five differences between active and passive attacks. **(5+5)**

4. (i) स्निफ्फिंग एवं स्पूफिंग को समझाइए ।

Explain sniffing and spoofing.

(ii) कूकीज क्या है ? इसकी कार्यविधि समझाइए ।

What is cookies ? Explain working of it. **(5+5)**

5. (i) प्लेफेयर सिफर की उदाहरण के साथ व्याख्या कीजिए ।

Explain playfair cipher with example.

(ii) सममित कुंजी क्रिप्टोग्राफी की व्याख्या कीजिए ।

Explain symmetric key cryptography. **(5+5)**

6. (i) TCP/IP की विभिन्न सतहों को समझाइए ।

Explain various layers of TCP/IP.

(ii) सुरक्षित सॉकेट लेयर (SSL) की व्याख्या कीजिए ।

Explain Secure Socket Layer (SSL). **(5+5)**

7. (i) फ़ॉयरवॉल क्या है ? फायरवॉल के प्रकार बताइए ।

What is firewall ? Explain the types of firewalls.

(ii) घुसपैठ क्या है ? घुसपैठ पहचान प्रणाली के प्रमुख घटकों की व्याख्या करें ।

What is an intrusion ? Explain major components of intrusion detection system. **(5+5)**

8. (i) PEM (प्राइवेसी एनहान्सड मेल) के पदों को समझाइए ।

Explain the steps of PEM (Privacy Enhanced Mail).

(ii) ब्लॉक एवं स्ट्रीम सिफर को समझाइए । उनके मध्य अंतरों को लिखिए ।

Explain Block and Stream Cipher. Write down the differences between them. **(5+5)**

9. निम्न पर संक्षिप्त टिप्पणियाँ लिखिए :

Write short notes on the following :

(i) वर्चुअल प्राइवेट नेटवर्क (VPN)

Virtual Private Network (VPN)

(ii) संदेश संग्रह

Message Digest

(iii) डिजिटल हस्ताक्षर

Digital Signature **(3+4+3)**