No. of Printed Pages : 8

333

CS 308/IT 308

Roll No. : .....

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) _____ हमलों को सुरक्षित और प्रतिरक्षा बनाने के लिए संदेशों को बदलने का विज्ञान और कला है ।

(a) क्रिप्टोग्राफी (b) क्रिप्टोएनालिसिस

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

_____ is the science and art of transforming messages to make them secure and immune to attacks.

(a) Cryptography (b) Cryptoanalysis

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

(2) संदेश की गोपनीयता में, प्रेषित संदेश का मतलब केवल इच्छित _____ के लिए होना चाहिए ।

(a) प्राप्तकर्ता (b) भेजने वाले

(c) मॉड्युलर (d) अनुवादक

In message confidentiality, transmitted message must make sense to only intended _____.

(a) Receiver (b) Sender

(c) Modulor (d) Translator

P.T.O.

(3) जब डेटा रिसीवर पर पहुँचना चाहिए ठीक उसी तरह जैसे कि वे भेजे गए थे, यह कहलाता है

(a) संदेश गोपनीयता (b) संदेश अखंडता

(c) संदेश स्प्लैशिंग (d) संदेश भेजना

When data must arrive at receiver exactly as they were sent, it is called

(a) Message Confidentiality (b) Message Integrity

(c) Message Splashing (d) Message Sending

(4) _____ यह आश्वासन है कि कोई व्यक्ति किसी चीज की वैधता को अस्वीकार नहीं कर सकता है ।

(a) संदेश गैर-परित्याग (b) संदेश अखंडता

(c) संदेश गोपनीयता (d) संदेश भेजना

_____ is the assurance that someone cannot deny the validity of something.

(a) Message Non-repudiation (b) Message Integrity

(c) Message Confidentiality (d) Message Sending

(5) _____ का अर्थ है किसी और के होने का दिखावा करना ।

(a) सूँघना (b) स्पूफिंग

(c) फार्मिंग (d) फिशिंग

_____ means to pretend to be someone else.

(a) Sniffing (b) Spoofing

(c) Pharming (d) Phishing

(6) निम्नलिखित में से कौन सा सक्रिय हमला है ?

(a) मेस्कुएरेड (b) यातायात विश्लेषण

(c) ईवसड्रोपिंग (d) संदेश सामग्री जारी करना

Which one of the following is an active attack ?

(a) Masquerade (b) Traffic analysis

(c) Eavesdropping (d) Release of message content

(7) निम्नलिखित में से कौन सा निष्क्रिय हमला है ?

(a) रीप्ले हमला (b) मेस्कुएरेड

(c) ट्रैफ़िक विश्लेषण (d) सेवा से वंचित

Which of the following is passive attack ?

(a) Replay attack (b) Masquerade

(c) Traffic analysis (d) Denial of service

(8) एक कंप्यूटर _____ एक दुर्भावनापूर्ण कोड है जो स्वयं को अन्य प्रोग्रामों में कॉपी करके प्रतिकृति बनाता है ।

(a) कीड़ा (b) प्रोग्राम

(c) वायरस (d) इनमें से कोई नहीं

A computer _____ is a malicious code which self-replicates by copying itself to their programs.

(a) worm (b) program

(c) virus (d) none of these

(9) मोनो-अल्फाबेटिक सिफर में प्लेटेक्स्ट के प्रत्येक अक्षर को सिफरटेक्स्ट बनाने के लिए _____ द्वारा प्रतिस्थापित किया जाता है ।

(a) कुंजी (b) दूसरे अक्षर

(c) मल्टी पार्टीज़ (d) एकल पक्ष

In mono-alphabetic cipher each letter of the plaintext is substituted by _____ to form the ciphertext.

(a) key (b) other letter

(c) multi parties (d) single party

(10) _____ परिवर्तन के बाद का संदेश है ।

(a) सिफरटेक्स्ट (b) प्लेनटेक्स्ट

(c) गुप्त-टेक्स्ट (d) उपरोक्त में से कोई नहीं

The _____ is the message after transformation.

(a) ciphertext (b) plaintext

(c) secret-text (d) none of the above

(11) _____ एल्गोरिदम प्लेनटेक्स्ट को सिफरटेक्स्ट में बदल देता है ।

(a) एन्क्रिप्शन (b) डिक्रिप्शन

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

_____ algorithm transforms plaintext to ciphertext.

(a) Encryption (b) Decryption

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

(12) एक _____ सिफर एक वर्ण को दूसरे वर्ण से बदल देता है ।

(a) प्रतिस्थापन (b) ट्रांस्पोजीशन

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

A _____ cipher replaces one character with another character.

(a) substitution (b) transposition

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

(13) _____ सिफर एक सिफरटेक्स्ट बनाने के लिए प्लेनटेक्स्ट करेक्टरों को फिर से सेट करता है ।

(a) प्रतिस्थापन (b) ट्रांस्पोजीशन

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

The _____ cipher reorders the plaintext characters to create a ciphertext.

(a) substitution (b) transposition

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

(14) एक असममित-कुंजी (या सार्वजनिक-कुंजी) सिफर _____ का उपयोग करता है ।

(a) 1 कुंजी (b) 2 कुंजी

(c) 3 कुंजी (d) 4 कुंजी

An asymmetric-key (or public-key) cipher uses _____

(a) 1 key (b) 2 key

(c) 3 key (d) 4 key

(15) एक _____ सिफर में, एक ही कुंजी प्रेषक और रिसीवर दोनों द्वारा उपयोग की जाती है ।

(a) सममित-कुंजी (b) असममित-कुंजी

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

In a _____ 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)

(16) एक हैश फ़ंक्शन किसी संदेश की अखंडता की गारंटी देता है । यह गारंटी देता है कि संदेश _____ नहीं है ।

(a) उल्लंघन किया गया (b) ओवर व्यू

(c) बदला हुआ (d) उपरोक्त में से कोई नहीं

A hash function guarantees integrity of a message. It guarantees that message has not be _____.

(a) Violated replaced (b) Over view

(c) Changed (d) None of the above

(17) एक डिजिटल हस्ताक्षर एक हस्ताक्षर का एक इलेक्ट्रॉनिक रूप है जिसका उपयोग किसी संदेश के _____ की पहचान को प्रमाणित करने के लिए किया जाता है ।

(a) प्राप्तकर्ता (b) प्रेषक

(c) प्राप्तकर्ता और प्रेषक दोनों (d) उपरोक्त में से कोई नहीं

A digital signature is an electronic form of a signature that can be used to authenticate the identity of the _____ of a message.

(a) receiver (b) sender

(c) both receiver and sender (d) none of the above

(18) _____ एक क्रिप्टोग्राफिक प्रोटोकॉल है जिसका उपयोग HTTP/HTTPS आधारित कनेक्शन को सुरक्षित करने के लिए किया जाता है ।

(a) एस.एस.एल. (सिक्योर सॉकेट लेयर) (b) एच.टी.एम.एल.

(c) एस.ई.टी. (d) उपरोक्त में से कोई नहीं

_____ is a cryptographic protocol used for securing HTTP/HTTPS based connection.

(a) SSL (Secure Socket Layer) (b) HTML

(c) SET (d) None of the above

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

(a) हाइपरटेक्स्ट ट्रांसमिशन प्रोटोकॉल सुरक्षित

(b) सुरक्षित हाइपरलिंकड टेक्स्ट ट्रांसफर प्रोटोकॉल

(c) हाइपरलिंकड टेक्स्ट ट्रांसफर प्रोटोकॉल सुरक्षित

(d) हाइपरटेक्स्ट ट्रांसफर प्रोटोकॉल सुरक्षित

HTTPS is abbreviated as _____ .

(a) Hypertext Transmission Protocol Secured

(b) Secured Hyperlinked Text Transfer Protocol

(c) Hyperlinked Text Transfer Protocol Secured

(d) Hypertext Transfer Protocol Secure

(20) निम्नलिखित में से कौन एक मजबूत सुरक्षा प्रोटोकॉल नहीं है ?

(a) HTTPS (b) SSL

(c) SMTP (d) SET

Which of the following is not a strong security protocol ?

(a) HTTPS (b) SSL

(c) SMTP (d) SET

(21) आईपी प्रोटोकॉल है

(a) अविश्वसनीय प्रोटोकॉल (b) विश्वसनीय प्रोटोकॉल

(c) मेल सुरक्षा प्रोटोकॉल (d) उपरोक्त में से कोई नहीं

IP protocol is

(a) Unreliable Protocol (b) Reliable Protocol

(c) Mail Security Protocol (d) None of the above

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

(a) सुरक्षित/मल्टीमीडिया इंटरनेट मेलिंग एक्सटेंशनस

(b) सुरक्षित/बहुउद्देशीय इंटरनेट मेलिंग एक्सटेंशनस

(c) सुरक्षित/मल्टीमीडिया इंटरनेट मेल एक्सटेंशनस

(d) सुरक्षित/बहुउद्देशीय इंटरनेट मेल एक्सटेंशनस

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

(23) _____ ई-मेल सिस्टम के लिए एक सुरक्षा प्रोटोकॉल है।

(a) आईपी सेक (b) एस.एस.एल.

(c) पी.जी.पी. (d) उपरोक्त में से कोई नहीं

_____ is one security protocol for the e-mail system.

(a) IPSec (b) SSL

(c) PGP (d) None of the above

(24) सुंदर अच्छी गोपनीयता (PGP) में _____ का प्रयोग किया जाता है।

(a) ब्राउज़र सुरक्षा (b) ई-मेल सुरक्षा

(c) एफ़टीपी सुरक्षा (d) उल्लेखित कोई भी नहीं

In Pretty good privacy (PGP) _____ is used.

(a) browser security (b) email security

(c) FTP security (d) None of the mentioned.

(25) SMTP _____ TCP पोर्ट का उपयोग करता है।

(a) 22 (b) 23

(c) 24 (d) 25

SMTP uses the _____ TCP port.

(a) 22 (b) 23

(c) 24 (d) 25

(26) नेटवर्क लेयर फ़ायरवॉल _____ के रूप में करता है।

(a) ई-मेल फ़िल्टर (b) पैकेट फ़िल्टर

(c) सामग्री फ़िल्टर (d) वायरस फ़िल्टर

Network layer firewall works as a/an _____.

(a) email filter (b) packet filter

(c) content filter (d) virus filter

(27) _____ पर एक प्रॉक्सी फ़ायरवॉल फ़िल्टर करता है।

(a) भौतिक परत (b) डेटा लिंक परत

(c) नेटवर्क लेयर (d) एप्लीकेशन लेयर

A proxy firewall filters at _____.

(a) Physical layer (b) Data link layer

(c) Network layer (d) Application layer

(28) फ़ायरवॉल का उपयोग _____ सुरक्षा के लिए किया जाता है ।

(a) होम नेटवर्क (b) कॉर्पोरेट नेटवर्क

(c) उपरोक्त दोनों (d) इनमें से कोई नहीं

Firewalls are used to protect _____ .

(a) Home Networks (b) Corporate Networks

(c) Both of Above (d) None of these

(29) NAT का पूर्ण रूप क्या है ?

(a) नेटवर्क एड्रेस ट्रांसलेशन (b) नेटवर्क एड्रेस ट्रांसफार्मेशन

(c) नेटवर्क एक्सेस ट्रांसलेशन (d) इनमें से कोई नहीं

What is the full form of NAT ?

(a) Network Address Translation

(b) Network Address Transformation

(c) Network Access Translation

(d) None of these

(30) फ़ायरवॉल _____ से रक्षा नहीं कर सकता है ।

(a) आंतरिक खतरे (b) बाहरी खतरे

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

The firewall cannot protect against the _____ .

(a) internal threats (b) external threats

(c) both (a) and (b) (d) neither (a) nor (b) (1×30)

2. (i) ट्रोजन हॉर्स से आप क्या समझते हैं ?

What do you understand by Trojan Horse ?

(ii) ब्लॉक साइफर से आप क्या समझते हैं ?

What do you understand by Block Cipher ?

(iii) साइफर टेक्स्ट क्या है ?

What is cipher text ?

(iv) डी.एम.ज़ेड. क्या है ?

What is DMZ ?

(v) क्रिप्टोग्राफी को परिभाषित कीजिए ।

Define cryptography. (2×5)

P.T.O.

3. (i) फार्मिंग अटैक को समझाइए।
Explain pharming attack.

(ii) वर्नम साइफर को उदाहरण सहित समझाइये।
Explain vernam cipher with example. (5+5)

4. (i) कूकीज क्या है ? यह किस प्रकार कार्य करती है ? समझाइये।
What is cookies ? How it works ? Explain.

(ii) डिजिटल हस्ताक्षर क्या है ? यह कैसे कार्य करता है ? समझाइये।
What is digital signature ? How it works ? Explain. (5+5)

5. (i) असममित कुंजी क्रिप्टोग्राफी को खण्ड आरेख की सहायता से समझाइये।
Explain asymmetric key cryptography with the help of block diagram.

(ii) पॉलीअल्फाबेटिक प्रतिस्थापन साइफर क्या है ? उदाहरण सहित समझाइये।
What is polyalphabetic substitution cipher ? Explain with example. (5+5)

6. (i) टाईम स्टैम्पिंग प्रोटोकॉल क्या है ? यह किस प्रकार उपयोगी है ? समझाइए।
What is time stamping protocol ? How it is useful ? Explain.

(ii) ऐप्लिकेशन गेटवे से आप क्या समझते हैं ? विस्तार से समझाइये।
What do you understand by application gateways ? Explain in details. (5+5)

7. (i) प्राइवेसी इन्हान्स्ड मेल क्या है ? समझाइये।
What is privacy enhanced mail ? Explain.

(ii) टी.सी.पी./आई.पी. को समझाइये।
Explain TCP / IP. (5+5)

8. (i) फ़ायरवॉल से आप क्या समझते हैं ? फ़ायरवॉल की सीमाएँ समझाइये।
What do you understand by firewall ? Explain the limitations of firewall.

(ii) कम्प्यूटर सुरक्षा के सिद्धांतो को समझाइये।
Explain principles of computer security. (5+5)

9. निम्न पर संक्षिप्त टिप्पणियाँ लिखिए :
Write short notes on the following :

(i) कम्प्यूटर सुरक्षा की आवश्यकता
Need of computer security.

(ii) सिक्योर मल्टीपरपज़ इन्टरनेट मेल इक्स्टेन्शॅन्स (एस.एम.आई.एम.ई.)
Secure multipurpose internet mail extensions. (SMIME) (5+5)