Total No. of Pages : 8

2169

CS308/IT308

Roll No. : .....

2016

INTRODUCTION TO NETWORK SECURITY AND CRYPTOGRAPHY

PART-I

निर्धारित समय : ½ घंटा] [अधिकतम अंक : 30

Time allowed : ½ Hour] [Maximum Marks : 30

नोट : *(i)* *सभी प्रश्न अनिवार्य हैं एवं प्रत्येक प्रश्न 1 अंक का है ।*

Note : *All Questions are compulsory and each question is of 1 mark.*

(ii) *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. कम्प्यूटर सुरक्षा में _____ । मतलब यह है कि कम्प्यूटर सिस्टम की संपत्ति केवल अधिकृत parties द्वारा ही संशोधित किया जा सकता है ।
   (a) गोपनीयता
   (b) अखण्डता
   (c) उपलब्धता
   (d) प्रामाणिकता

2. _____ का सिद्धांत सुनिश्चित करता है कि संदेश की सामग्री केवल प्रेषक और इच्छित प्राप्तकर्ता के उपयोग के लिए है ।
   (a) गोपनीयता
   (b) प्रमाणीकरण
   (c) अखण्डता
   (d) पहुँच नियंत्रण

1. In computer security, _____ means that computer system assets can be modified only by authorized parties.
   (a) Confidentiality
   (b) Integrity
   (c) Availability
   (d) Authenticity

2. The principle of _____ ensures that only the sender and the intended recipients have access to the contents of a message.
   (a) Confidentiality
   (b) Authentication
   (c) Integrity
   (d) Access control

P.T.O.

3. _____ हमले अखण्डता से सम्बन्धित है ।
   (a) अवरोधन
   (b) निर्माण
   (c) संशोधन
   (d) रुकावट

4. वाइरस एक कम्प्यूटर _____ है ।
   (a) फाइल
   (b) कार्यक्रम
   (c) डेटाबेस
   (d) अनुप्रयोग सॉफ्टवेयर

5. _____ हमलों में, संदेश सामग्री संशोधित की जाती हैं ।
   (a) निष्क्रिय
   (b) सक्रिय
   (c) ऊपर के दोनों
   (d) उपरोक्त में से कोई नहीं

6. एक _____ अपनी ही प्रतियाँ बनाने के द्वारा अपने आप को दोहरा सकता है ताकि एक नेटवर्क में ठहराव आ जाए ।
   (a) वायरस
   (b) कीड़ा
   (c) ट्रोजन हॉर्स
   (d) बम

7. डॉस हमले _____ के कारण से होते हैं ।
   (a) प्रमाणीकरण
   (b) संशोधन
   (c) निर्माण
   (d) रिप्ले हमले

8. _____ वायरस का एक रूप जिसको स्पष्ट रूप से एन्टीवायरस से पता लगाने से खुद को छिपाने के लिए बनाया गया है ।
   (a) चुपके वायरस
   (b) बहुरूपी वायरस
   (c) परजीवी वायरस
   (d) मेक्रो वायरस

3. The _____ attack is related to integrity.
   (a) Interception
   (b) Fabrication
   (c) Modification
   (d) Interruption

4. Virus is a computer _____.
   (a) File
   (b) Program
   (c) Database
   (d) Application software

5. In _____ attacks, the message contents are modified
   (a) Passive
   (b) Active
   (c) Both of the above
   (d) None of the above

6. A _____ replicates itself by creating its own copies, in order to bring the network to a halt.
   (a) Virus
   (b) Worm
   (c) Trojan horse
   (d) Bomb

7. DOS attacks are caused by _____.
   (a) Authentication
   (b) Modification
   (c) Fabrication
   (d) Replay attacks

8. _____ is a form of virus explicitly designed to hide itself from detection by antivirus software.
   (a) Stealth virus
   (b) Polymorphic virus
   (c) Parasitic virus
   (d) Macro virus

9. भाषा जो हम आमतौर पर प्रयोग करते है, उसे कहा जा सकता हैं
   (a) शुद्ध पाठ
   (b) साधारण पाठ
   (c) सादा पाठ
   (d) सामान्य पाठ

10. संहिताबद्ध भाषा के रूप में कहा जा सकता है ।
   (a) स्पष्ट पाठ
   (b) अस्पष्ट पाठ
   (c) कोड पाठ
   (d) सिफर पाठ

11. सीजर सिफर एक उदाहरण है _____ का ।
   (a) प्रतिस्थापन सिफर
   (b) स्थानांतरण सिफर
   (c) प्रतिस्थापन के रूप में अच्छी तरह से स्थानांतरण सिफर
   (d) उपरोक्त में से कोई नहीं

12. वर्नम साइफर को _____ भी कहा जाता है ।
   (a) रेल बाड तकनीक
   (b) वन-टाइम पैड
   (c) बुक साइफर
   (d) रनिंग कुंजी साइफर

13. सादा टेक्सट को साइफर टेक्सट में रूपांतरण को कहा जाता है _____
   (a) एनक्रिप्शन
   (b) डिक्रिप्शन
   (c) क्रिप्टोग्राफी
   (d) क्रिप्टएनालिस्ट

9. The language that we commonly use can be termed as _____.
   (a) Pure text
   (b) Simple text
   (c) Plain text
   (d) Normal text

10. The codified language can be termed as _____.
   (a) Clear text
   (b) Unclear text
   (c) Code text
   (d) Cipher text

11. Caesar cipher is an example of _____.
   (a) Substitution cipher
   (b) Transposition cipher
   (c) Substitution as well as transposition cipher
   (d) None of the above

12. Vernam cipher is also called as _____.
   (a) Rail fence technique
   (b) One-time pad
   (c) Book cipher
   (d) Running key cipher

13. Conversion of plain text into cipher text is called as _____.
   (a) Encryption
   (b) Decryption
   (c) Cryptography
   (d) Cryptanalyst

14. विकर्ण रूप में पाठ लिखने और पंक्तियों के दृश्य के रूप में पढ़ने की प्रक्रिया के रूप में कहा जाता है ।
(a) रेल बाड़ तकनीक
(b) सीजर साइफर
(c) मोनोवर्णमाला साइफर
(d) एक ही स्वर प्रतिस्थापन साइफर

15. _____ में सादे पाठ की एक बिट एक समय में एनक्रिप्ट की जाती है ।
(a) स्ट्रीम साइफर
(b) ब्लॉक साइफर
(c) दोनों
(d) कोई नहीं

16. _____ में सादा पाठ का एक ब्लॉक एक समय में एनक्रिप्ट किया जाता है ।
(a) स्ट्रीम साइफर
(b) ब्लॉक साइफर
(c) दोनों
(d) दोनों नहीं

17. एक _____ संदेश की अखंडता को सत्यापित करने के लिए प्रयोग किया जाता है ।
(a) संदेश डाइजेस्ट
(b) डिक्रिप्शन एल्गोरिथ्म
(c) डिजिटल लिफाफा
(d) उपरोक्त में से कोई नहीं

18. असममित कुंजी क्रिप्टोग्राफी में _____ चाबियाँ संवाद स्थापित करने के प्रति आवश्यक है ।
(a) 2
(b) 3
(c) 4
(d) 5

14. The process of writing the text as diagonals and reading it as sequence of rows is called as _____.
(a) Rail fence technique
(b) Caesar cipher
(c) Mono-alphabetic cipher
(d) Homophonic substitution cipher

15. In _____ one bit of plain text is encrypted at a time.
(a) Stream cipher
(b) Block cipher
(c) Both
(d) None

16. In _____ one block of plain text is encrypted at a time.
(a) Stream cipher
(b) Block cipher
(c) Both
(d) None

17. A _____ is used to verify the integrity of a message.
(a) Message digest
(b) Decryption algorithm
(c) Digital envelope
(d) None of the above

18. In asymmetric key cryptography, _____ keys are required per communicating.
(a) 2
(b) 3
(c) 4
(d) 5

19. एस.एस.एल. परत _____ एवं _____ के मध्य स्थित है ।
    (a) परिवहन परत, नेटवर्क परत
    (b) आवेदन परत, परिवहन परत
    (c) डाटालिंक परत, भौतिक परत
    (d) नेटवर्क परत, डाटालिंक परत

20. SHTTP एनक्रिप्शन _____ पर काम करता है ।
    (a) आवेदन परत
    (b) डाटालिंक परत
    (c) परिवहन परत
    (d) भौतिक परत

21. SET का मुख्य उद्देश्य _____ के लिए सम्बन्धित है ।
    (a) ब्राउजर के बीच सुरक्षित संचार
    (b) डिजिटल हस्ताक्षर और सर्वर
    (c) मेसेज डाइजेस्ट
    (d) इंटरनेट पर सुरक्षित क्रेडिट कार्ड से भुगतान

22. टी.एस.पी. का मतलब है
    (a) टाइम सर्विस प्रोटोकोल
    (b) ट्रांसपोर्ट सर्विस प्रोटोकोल
    (c) टाइम सिग्नेचर प्रोटोकोल
    (d) टाइम स्टेम्पिंग प्रोटोकोल

23. ई-मेल सुरक्षा _____ प्रोटोकोल द्वारा प्राप्त की जा सकती है ।
    (a) पी.ई.एम.
    (b) पी.जी.पी.
    (c) एस/एम.आई.एम.ई.
    (d) उपरोक्त सभी

24. पी.ई.एम. निम्नलिखित सेवाएँ प्रदान करता है :
    (a) एनक्रिप्शन
    (b) मेसेज डाइजेस्ट
    (c) डीजिटल हस्ताक्षर
    (d) उपरोक्त सभी

19. SSL layer is located between _____ and _____.
    (a) Transport layer, Network layer
    (b) Application layer, Transport layer
    (c) Data link layer, physical layer
    (d) Network layer, Data link layer

20. SHTTP encrypts at the _____.
    (a) Application layer
    (b) Datalink layer
    (c) Transport layer
    (d) Physical layer

21. The main purpose of SET is related to _____.
    (a) Secure communication between browser
    (b) Digital signature and server
    (c) Message digest
    (d) Secure credit card payment on the internet

22. TSP means _____
    (a) Time Service Protocol
    (b) Transport Service Protocol
    (c) Time Signature Protocol
    (d) Time Stamping Protocol

23. E-mail security can be achieved by the _____ protocols
    (a) PEM protocol
    (b) PGP protocol
    (c) S/MIME protocol
    (d) All of the above

24. PEM provides the following services :
    (a) Encryption
    (b) Message digest
    (c) Digital signature
    (d) All of the above

25. एस.एम.टी.पी. का मतलब है
(a) सिम्पल मेल ट्रांसफर प्रोटोकोल
(b) सर्विस मेल ट्रांसफर प्रोटोकोल
(c) सिम्पल मेसेज ट्रांसफर प्रोटोकोल
(d) उपरोक्त में से कोई नहीं

26. फायरवॉल _____ स्थित होना चाहिए ।
(a) एक कंपनी के नेटवर्क के अन्दर
(b) एक कंपनी के नेटवर्क के बाहर
(c) एक कंपनी के नेटवर्क और बाहरी दुनिया के बीच
(d) इनमें से कोई नहीं

27. फायरवाल _____ का एक विशेष रूप है
(a) पुल
(b) डिस्क
(c) प्रिंटर
(d) राउटर

28. संभावित हमलावरों को आकर्षित करने के लिए स्थापित किया जाने वाला जाल _____ कहलाता है ।
(a) वी.पी.एन.
(b) ट्रेपडोर
(c) प्रोक्सी
(d) हनीपॉट

29. एक पैकेट फिलर _____ पैकेट का परीक्षण करता है ।
(a) सभी
(b) किसी को नहीं
(c) कुछ
(d) वैकल्पिक

30. डी.एम.जेड़ का मतलब है
(a) डायरेक्ट मेल जोन
(b) डिजाइन मेल जोन
(c) डवलप मेल जोन
(d) डिमिलिट्राइज जोन

25. SMTP means _____.
(a) Simple Mail Transfer Protocol
(b) Service Mail Transfer Protocol
(c) Simple Message Transfer Protocol
(d) None of the above

26. Firewall should be situated _____.
(a) Inside a corporate network
(b) Outside a corporate network
(c) Between a corporate network and the outside word
(d) None of these

27. Firewall is a specialized form of a _____.
(a) Bridge
(b) Disk
(c) Printer
(d) Router

28. The trap set to attract potential attacker is called as _____
(a) VPN
(b) Trapdoor
(c) Proxy
(d) Honeypot

29. A packet filter examines _____ packets
(a) All
(b) No
(c) Some
(d) Alternate

30. DMZ means _____
(a) Direct Mail Zone
(b) Design Mail Zone
(c) Develop Mail Zone
(d) Demilitarized Zone

2169

CS308/IT308 **Roll No. : .....**

2016

INTRODUCTION TO NETWORK SECURITY AND CRYPTOGRAPHY

PART-II

निर्धारित समय : तीन घंटे] **[अधिकतम अंक : 70**
Time allowed : Three Hours] **[Maximum Marks : 70**

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

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

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

(iii) *प्रत्येक प्रश्न को नये पृष्ठ से प्रारम्भ कीजिए ।*
Start each question on a 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. (i) एस.एच.टी.टी.पी. (SHTTP) एवं एस.एम.टी.पी. (SMTP) के पूरे रूप लिखिए ।
Write the full forms of SHTTP and SMTP.

(ii) 'पेसिव अटैक' से आप क्या समझते हैं ?
What do you mean by passive Attack ?

(iii) 'इण्ट्रुजन' से आप क्या समझते हैं ?
What do you understand by intrusion ?

(iv) 'प्लेन टेक्सट' एवं 'साइफर टेक्सट' क्या होता है ?
What is plain text and cipher text ?

(v) 'ट्रोजन होर्स' क्या है ?
What is Trojan Horse ? **(2×5)**

2. (i) डिजिटल हस्ताक्षर का वर्णन कीजिए तथा दिखाइये कि डिजिटल हस्ताक्षर में हस्ताक्षरण तथा पुष्टिकरण किस प्रकार होती है ?
Describe Ditigal singnature and show how signing and verification of digital signature is done.

(ii) सुरक्षा के 'इंटेग्रिटी' तथा 'नॉन रिप्यूडिएशन' सिद्धांतो को समझाइये ।
Explain integrity and Non-Repudiation principles of security. (6+6)

3. (i) कुकीज के बनाने तथा प्रयोग को समझाइये ।
Explain the creation and usage of cookies.
(ii) 'सिमेट्रिक की क्रिप्टोग्राफी' को संक्षेप में समझाइये ।
Explain the symmetric key crysptography in short. (6+6)

4. (i) सीजर साइफर सबस्टीट्यूशन तकनीक को उदाहरण देकर समझाइये ।
Explain ceasar cipher substitution technique by giving example.
(ii) डी.एम.जेड. की अवधारणा की विवेचना कीजिए ।
Discuss the concept of DMZ. (6+6)

5. (i) सुरक्षा एप्रोचेस (Security Approaches) को समझाइये ।
Explain Security Approaches.
(ii) प्राइवेसी एन्हान्सड मेल से सुरक्षा कैसे प्राप्त की जाती हैं ?
How is security achieved through privacy Enhanced Mail ? (6+6)

6. (i) सममित एवं असममित कुंजी क्रिप्टोग्राफी के लाभों व हानियों का वर्णन कीजिए ।
Describe the advantages and disadventages of symmetric and asymmetric key cryptography.
(ii) सीक्योर सॉकेट लेयर (SSL) की कार्यप्रणाली को समझाइये ।
Explain the working of Secure Socket Layer (SSL). (6+6)

7. (i) मेसेज डाइजेस्ट के सिद्धांत की विवेचना कीजिए ।
Discuss the concept of message digest.
(ii) फायर वॉल के फायदे तथा सीमाओं का वर्णन कीजिए ।
Describe the advantages and limitations of firewall. (6+6)

8. निम्न पर संक्षिप्त टिप्पणियाँ लिखिए :
Write short notes on the following :
(i) वाइरस तथा वोर्म
Virus and Worm
(ii) प्रेटी गुड प्राइवेसी
Pretty Good Privacy (6+6)