R

Question Booklet Number

0628001

B.C.A. 6th Sem. (Main/Back/Ex) Examination, 2025

COMPUTER APPLICATION

(Computer Network Security)

Question Booklet Series

D

| Maximum Marks : 75
| अधिकतम अंक : 75

| Time : 2 Hours
| समय : 2 घण्टे

(To be filled in by the Candidate / निम्न पूर्तियाँ परीक्षार्थी स्वयं भरें)

Roll No. (in figures) _____
अनुक्रमांक (अंकों में)

Roll No. (in words) _____
अनुक्रमांक (शब्दों में)

Enrolment No. (in figures) _____

Name of Exam Centre _____
परीक्षा केन्द्र का नाम

Signature of Invigilator
कक्ष निरीक्षक के हस्ताक्षर

Instructions to the Examinee :

1. Do not open the booklet unless you are asked to do so.
2. The booklet contains 100 questions. Examinee is required to answer all 100 questions in the OMR Answer-Sheet provided and **not in the question booklet**. All questions carry equal marks.
3. Examine the Booklet and the OMR Answer-Sheet very carefully before you proceed. Faulty question booklet due to missing or duplicate pages/questions or having any other discrepancy should be got immediately replaced.

(Remaining Instructions on last page)

परीक्षार्थियों के लिए निर्देश :

1. प्रश्न-पुस्तिका को तब तक न खोलें जब तक आपसे कहा न जाए।
2. प्रश्न-पुस्तिका में 100 प्रश्न हैं। परीक्षार्थी को सभी 100 प्रश्नों को केवल दी गई OMR आन्सर-शीट पर ही हल करना है, **प्रश्न-पुस्तिका पर नहीं**। सभी प्रश्नों के अंक समान हैं।
3. प्रश्नों के उत्तर अंकित करने से पूर्व प्रश्न-पुस्तिका तथा OMR आन्सर-शीट को सावधानीपूर्वक देख लें। दोषपूर्ण प्रश्न-पुस्तिका जिसमें कुछ भाग छपने से छूट गये हों या प्रश्न एक से अधिक बार छप गए हों या उसमें किसी अन्य प्रकार की कमी हो, उसे तुरन्त बदल लें।

(शेष निर्देश अन्तिम पृष्ठ पर)

https://www.msustudy.com

1. Which protocol is commonly used for secure email communication?
   (A) POP
   (B) SMTP
   (C) S/MIME
   (D) FTP

2. What cryptographic algorithm is used in Pretty Good Privacy (PGP)?
   (A) AES
   (B) RSA
   (C) DES
   (D) SHA

3. Which of the following is NOT a component of the X.509 standard?
   (A) Certificate Authority (CA)
   (B) Certificate Revocation List (CRL)
   (C) Certificate Signing Request (CSR)
   (D) Simple Mail Transfer Protocol (SMTP)

4. What does S/MIME stand for in the context of network security?
   (A) Secure/Multipurpose Internet Mail Extensions
   (B) Secure/Media Internet Mail Encryption
   (C) Simple Mail Interception and Encryption
   (D) Secure/Multi-layered Internet Mail Encryption

1. सुरक्षित ईमेल संचार के लिए आमतौर पर किस प्रोटोकॉल का उपयोग किया जाता है?
   (A) पीओपी
   (B) एसएमटीपी
   (C) एस/माइम
   (D) एफ़टीपी

2. प्रीटी गुड प्राइवेसी (पीजीपी) में किस क्रिप्टोग्राफिक एल्गोरिथ्म का उपयोग किया जाता है?
   (A) एईएस
   (B) आरएसए
   (C) डीईएस
   (D) एसएचए

3. निम्नलिखित में से कौन X.509 मानक का एक घटक नहीं है?
   (A) प्रमाणपत्र प्राधिकरण (सीए)
   (B) प्रमाणपत्र निरस्तीकरण सूची (CRL)
   (C) प्रमाणपत्र हस्ताक्षर अनुरोध (CSR)
   (D) सिंपल मेल ट्रांसफर प्रोटोकॉल (SMTP)

4. नेटवर्क सुरक्षा के संदर्भ में S/MIME का क्या अर्थ है?
   (A) सुरक्षित/बहुउद्देशीय इंटरनेट मेल एक्सटेंशन
   (B) सुरक्षित/मीडिया इंटरनेट मेल एन्क्रिप्शन
   (C) सरल मेल अवरोधन और एन्क्रिप्शन
   (D) सुरक्षित/बहुस्तरीय इंटरनेट मेल एन्क्रिप्शन

https://www.msustudy.com

5. Which cryptographic technique is used to verify the integrity of message without revealing its contents.

(A) Encryption

(B) Decryption

(C) Digital signatures

(D) Hash functions

6. What is the purpose of authentication in network security?

(A) To ensure data confidentiality

(B) To verify the identity of users or systems

(C) To encrypt data during transmission

(D) To sign digital certificates

7. Which cryptographic mechanism uses a pair of keys for encryption and decryption.

(A) Symmetric cryptography

(B) Asymmetric cryptography

(C) Hash functions

(D) Digital signatures

8. What does the term 'cipher text refer to in cryptography?

(A) Original message

(B) Encrypted message

(C) Decrypted message

(D) Hashed message

5. किसी संदेश की सामग्री को प्रकट किए बिना उसकी अखंडता को सत्यापित करने के लिए किस क्रिप्टोग्राफिक तकनीक का उपयोग किया जाता है।

(A) एन्क्रिप्शन

(B) डिक्रिप्शन

(C) डिजिटल हस्ताक्षर

(D) हैश फंक्शन

6. नेटवर्क सुरक्षा में प्रमाणीकरण का उद्देश्य क्या है।

(A) डेटा गोपनीयता सुनिश्चित करने के लिए

(B) उपयोगकर्ताओं या सिस्टम की पहचान सत्यापित करने के लिए

(C) संचरण के दौरान डेटा एन्क्रिप्ट करने के लिए

(D) डिजिटल प्रमाणपत्रों पर हस्ताक्षर करने के लिए

7. कौन सा क्रिप्टोग्राफिक तंत्र एन्क्रिप्शन और डिक्रिप्शन के लिए कुंजी की एक जोड़ी का उपयोग करता है।

(A) सममित क्रिप्टोग्राफी

(B) असममित क्रिप्टोग्राफी

(C) हैश फंक्शन

(D) डिजिटल हस्ताक्षर

8. क्रिप्टोग्राफी में सिफर टेक्स्ट शब्द का क्या अर्थ है।

(A) मूल संदेश

(B) एन्क्रिप्टेड संदेश

(C) डिक्रिप्टेड संदेश

(D) हैश्ड संदेश

https://www.msustudy.com

9. What term describes an attempt to compromise the confidentiality, integrity or availability of computer system or networks.

(A) Encryption

(B) Cryptanalysis

(C) Cyberattack

(D) Authentication

10. Which of the following is NOT a common service provided by network security mechanisms?

(A) Confidentiality

(B) Authentication

(C) Denial of service (DoS)

(D) Availability

11. Which model provides a framework for understanding and implementing network security policies and mechanisms?

(A) OSI model

(B) TCP/IP model

(C) CIA model

(D) ARPANET model

9. कौन सा शब्द कंप्यूटर सिस्टम या नेटवर्क की गोपनीयता, अखंडता या उपलब्धता से समझौता करने के प्रयास का वर्णन करता है।

(A) एन्क्रिप्शन

(B) क्रिप्टएनालिसिस

(C) साइबर हमला

(D) प्रमाणीकरण

10. निम्नलिखित में से कौन सी नेटवर्क सुरक्षा तंत्र द्वारा प्रदान की जाने वाली एक सामान्य सेवा नहीं है।

(A) गोपनीयता

(B) प्रमाणीकरण

(C) सेवा से इनकार (DoS)

(D) उपलब्धता

11. कौन सा मॉडल नेटवर्क सुरक्षा नीतियों और तंत्रों को समझने और कार्यान्वित करने के लिए एक रूपरेखा प्रदान करता है।

(A) OSI मॉडल

(B) TCP/IP मॉडल

(C) CIA मॉडल

(D) ARPANET मॉडल

https://www.msustudy.com

12. What does "CIA" stand for in the context of network security?

(A) Confidentiality, Integrity, Authentication

(B) Confidentiality, Integrity, Availability

(C) Cybersecurity, Information Assurance, Authorization

(D) Cryptography, Intrusion Detection, Access control

13. Which cryptographic concept refers to the process of converting plaintext into ciphertext?

(A) Decryption

(B) Authentication

(C) Encryption

(D) Digital Signature

14. What is plaintext in the context of cryptography?

(A) Secret message

(B) Encrypted message

(C) Original message

(D) Hashed message

12. नेटवर्क सुरक्षा के संदर्भ में सीआईए का क्या अर्थ है।

(A) गोपनीयता, अखंडता, प्रमाणीकरण

(B) गोपनीयता, अखंडता, उपलब्धता

(C) साइबर सुरक्षा, सूचना आश्वसन प्राधिकरण

(D) क्रिप्टोग्राफी घुसपैठ का पता लगाने अभिगम नियंत्रण

13. कौन सी क्रिप्टोग्राफिक अवधारणा प्लेनटेक्स्ट को सिफरटेक्स्ट में बदलने की प्रक्रिया को संदर्भित करती है।

(A) डिक्रिप्शन

(B) प्रमाणीकरण

(C) एन्क्रिप्शन

(D) डिजिटल हस्ताक्षर

14. क्रिप्टोग्राफी के संदर्भ में प्लेनटैक्स्ट क्या है।

(A) गुप्त संदेश

(B) एन्क्रिप्टेड संदेश

(C) मूल संदेश

(D) हैश्ड संदेश

https://www.msustudy.com

15. Which version of SNMP introduced the community-based security model?

(A) SNMPv1

(B) SNMPv2c

(C) SNMPv2u

(D) SNMPv3

16. What is the primary disadvantage of SNMPv1 in terms of security

(A) lack of authentication

(B) limited MIB support

(C) unreliable communication

(D) complex configuration

17. Which SNMP version introduced the concept of SNMP views to restrict access to certain portions of the MIB

(A) SNMPv1

(B) SNMPv2c

(C) SNMPv2u

(D) SNMPv3

18. What is the primary advantage of SNMPv2 over SNMPv1?

(A) improved security features

(B) enhance MIB support

(C) better error handling

(D) increased scalability

15. एसएनएमपी के किस संस्करण ने समुदाय आधारित सुरक्षा मॉडल पेश किया?

(A) एसएनएमपीवी 1

(B) एसएनएमपीवी 2 सी

(C) एसएनएमपीवी 2 यू

(D) एसएनएमपीवी 3

16. सुरक्षा के मामले में SNMPv1 का प्राथमिक नुकसान क्या है।

(A) प्रमाणीकरण का अभाव

(B) सीमित MIB समर्थन

(C) अविश्वसनीय संचार

(D) जटिल विन्यास

17. किस SNMP संस्करण ने MIB के कुछ हिस्सो तक पहुंच को प्रतिबंधित करने के लिए SNMP व्यूज की अवधारणा पेश की।

(A) एसएनएमपीवी 1

(B) एसएनएमपीवी 2 सी

(C) एसएनएमपीवी 2 यू

(D) एसएनएमपीवी 3

18. SNMPv1 की तुलना में SNMPv2 का प्राथमिक लाभ क्या है।

(A) बेहतर सुरक्षा सुविधाएँ

(B) उन्नत MIB समर्थन

(C) बेहतर त्रुटि हैंडलिंग

(D) बढ़ी हुई मापनीयता

https://www.msustudy.com

19. Which protocol is commonly used for communication between SNMP managers and agents?

(A) TCP

(B) UDP

(C) ICMP

(D) IPsec

20. Which SNMP version introduced the concept of SNMP inform messages for reliable delivery of traps?

(A) SNMPv1

(B) SNMPv2c

(C) SNMPv2u

(D) SNMPv3

21. What is the primary function of the management information base in SNMP?

(A) to manage network interfaces

(B) to store SNMP traps

(C) to define the structure of managed objects

(D) to encrypt SNMP messages

19. एसएनएमपी प्रबंधकों और एजेंटों के बीच संचार के लिए आमतौर पर कौन सा प्रोटोकॉल प्रयोग किया जाता है।

(A) टीसीपी

(B) यूडीपी

(C) आईसीएमपी

(D) आईपीएसईसी

20. किस SNMP संस्करण ने जाल के विश्वसनीय वितरण के लिए SNMP सूचना संदेशों की अवधारणा पेश की।

(A) एसएनएमपीवी 1

(B) एसएनएमपीवी 2 सी

(C) एसएनएमपीवी 2 यू

(D) एसएनएमपीवी 3

21. एसएनएमपी में प्रबंधन सूचना आधार (एमआईबी) का प्राथमिक कार्य क्या है।

(A) नेटवर्क इंटरफेस का प्रबंधन करने के लिए

(B) एसएनएमपी जाल को स्टोर करने के लिए

(C) प्रबंधित वस्तुओं की संरचना को परिभाषित करने के लिए

(D) SNMP संदेश एन्क्रिप्ट करने के लिए

https://www.msustudy.com

22. Which component is required for both encryption and decryption processes in symmetric cryptography?

(A) Public key

(B) Private key

(C) Hash function

(D) Digital Signature

23. In asymmetric cryptography, what is the purpose of the public key.

(A) To encrypt data

(B) To decrypt data

(C) To generate digital signatures

(D) To verify digital signatures

24. Which cryptographic mechanism is primarily used for ensuring data integrity and authenticity.

(A) Encryption

(B) Decryption

(C) Digital signatures

(D) Hash functions

22. सममित क्रिप्टोग्राफी में एन्क्रिप्शन और डिक्रिप्शन प्रक्रियाओं दोनों के लिए कौन सा घटक आवश्यक है।

(A) सार्वजनिक कुंजी

(B) निजी कुंजी

(C) हैश फंक्शन

(D) डिजिटल हस्ताक्षर

23. असममित क्रिप्टोग्राफी में सार्वजनिक कुंजी का उद्देश्य क्या है।

(A) डेटा एन्क्रिप्ट करने के लिए

(B) डेटा को डिक्रिप्ट करने के लिए

(C) डिजिटल हस्ताक्षर उत्पन्न करने के लिए

(D) डिजिटल हस्ताक्षर सत्यापित करने के लिए

24. डेटा अखंडता और प्रामाणिकता सुनिश्चित करने के लिए मुख्य रूप से किस क्रिप्टोग्राफिक तंत्र का उपयोग किया जाता है।

(A) एन्क्रिप्शन

(B) डिक्रिप्शन

(C) डिजिटल हस्ताक्षर

(D) हैश फंक्शन

https://www.msustudy.com

25. What does decryption refer to in the context of cryptography.

(A) Converting ciphertext into plaintext

(B) Converting plaintext into ciphertext

(C) Generating digital signatures

(D) Verifying digital signatures

26. What cryptographic technique is used to authenticate the sender of a message and ensure its integrity?

(A) Encryption

(B) Decryption

(C) Digital signatures

(D) Hash functions

27. In asymmetric cryptography, what is the purpose of the private key.

(A) To encrypt data

(B) To decrypt data

(C) To generate digital signatures

(D) To verify digital signatures

28. What does the term "Cryptanalysis" refer to?

(A) The process of encrypting plaintext

(B) The process of decrypting ciphertext

(C) The study of cryptographic algorithms and breaking them

(D) The study of digital signatures

25. क्रिप्टोग्राफी के संदर्भ में डिक्रिप्शन क्या संदर्भित करता है।

(A) सिफरटेक्स्ट को प्लेनटेक्स्ट में बदलना

(B) प्लेनटेक्स्ट को सिफरटेक्स्ट में बदलना

(C) डिजिटल हस्ताक्षर उत्पन्न करना

(D) डिजिटल हस्ताक्षर सत्यापित करना

26. किसी संदेश के प्रेषक को प्रमाणित करने और उसकी अखंडता सुनिश्चित करने के लिए किस क्रिप्टोग्राफिक तकनीक का उपयोग किया जाता है।

(A) एन्क्रिप्शन

(B) डिक्रिप्शन

(C) डिजिटल हस्ताक्षर

(D) हैश फंक्शन

27. असममित क्रिप्टोग्राफी में निजी कुंजी का उद्देश्य क्या है।

(A) डेटा एन्क्रिप्ट करने के लिए

(B) डेटा को डिक्रिप्ट करने के लिए

(C) डिजिटल हस्ताक्षर उत्पन्न करने के लिए

(D) डिजिटल हस्ताक्षर सत्यापित करने के लिए

28. क्रिप्टैनालिसिस शब्द का क्या अर्थ है।

(A) प्लेनटेक्स्ट को एन्क्रिप्ट करने की प्रक्रिया

(B) सिफरटेक्स्ट को डिक्रिप्ट करने की प्रक्रिया

(C) क्रिप्टोग्राफिक एल्गोरिदम का अध्ययन और उन्हें तोड़ना

(D) डिजिटल हस्ताक्षर का अध्ययन

https://www.msustudy.com

29. Which SNMP version uses community strings for authentication?

(A) SNMPv1

(B) SNMPv2c

(C) SNMPv2u

(D) SNMPv3

30. Which SNMP version is recommended for use in modern network management environments?

(A) SNMPv1

(B) SNMPv2c

(C) SNMPv2u

(D) SNMPv3

31. What term describes individuals who attempt to gain unauthorized access to computer systems?

(A) administrators

(B) intruders

(C) users

(D) developers

32. What is the primary function of kerberos in network security?

(A) encryption

(B) authentication

(C) authorization

(D) key exchange

29. कौन सा एसएनएमपी संस्करण प्रमाणीकरण के लिए सामुदायिक स्ट्रिंग का उपयोग करता है।

(A) एसएनएमपीवी 1

(B) एसएनएमपीवी 2 सी

(C) एसएनएमपीवी 2 यू

(D) एसएनएमपीवी 3

30. आधुनिक नेटवर्क प्रबंधन वातावरण में उपयोग के लिए किस SNMP संस्करण की सिफारिश की जाती है।

(A) एसएनएमपीवी 1

(B) एसएनएमपीवी 2 सी

(C) एसएनएमपीवी 2 यू

(D) एसएनएमपीवी 3

31. कौन सा शब्द उन व्यक्तियों का वर्णन करता है। जो कंप्यूटर सिस्टम तक अनधिकृत पहुंच प्राप्त करने का प्रयास करते है।

(A) प्रशासक

(B) घुसपैठिए

(C) उपयोगकर्ता

(D) डेवलपर्स

32. नेटवर्क सुरक्षा में केर्बेरोस का प्राथमिक कार्य क्या है?

(A एन्क्रिप्शन

(B) प्रमाणीकरण

(C) प्राधिकरण

(D) कुंजी विनिमय

https://www.msustudy.com

33. Which cryptographic concept involves the use of mathematical functions to create a fixed size output from variable size input?

(A) Encryption

(B) Decryption

(C) Hash functions

(D) Digital Signatures

34. What does the term "Key" represent in cryptography?

(A) The plaintext message

(B) The encrypted message

(C) A secret value used in encryption and decryption

(D) A digital signature

35. In the context of network security, what is the purpose of encryption.

(A) To verify the integrity of data

(B) To authenticate users

(C) To ensure confidentiality of data

(D) To prevent denial of service attacks

33. किस क्रिप्टोग्राफिक अवधारणा में चर-आकार इनपुट से एक निश्चित आकार का आउटपुट बनने के लिए गणितीय कार्यो का उपयोग शामिल है।

(A) एन्क्रिप्शन

(B) डिक्रिप्शन

(C) हैश फंक्शन

(D) डिजिटल हस्ताक्षर

34. क्रिप्टोग्राफी में कुंजी शब्द क्या दर्शाता है।

(A) सादा पाठ संदेश

(B) एन्क्रिप्टेड संदेश

(C) एन्क्रिप्शन और डिक्रिप्शन में उपयोग किया जाने वाला एक गुप्त मूल्य

(D) एक डिजिटल हस्ताक्षर

35. नेटवर्क सुरक्षा के संदर्भ में एन्क्रिप्शन का उद्देश्य क्या है।

(A) डेटा की अखंडता को सत्यापित करने के लिए

(B) उपयोगकर्ताओं को प्रमाणित करने के लिए

(C) डेटा की गोपनीयता सुनिश्चित करने के लिए

(D) सेवा हमलों से इनकार को रोकने के लिए

https://www.msustudy.com

36. What does SNMP stand for in computer networking?

(A) simple network monitoring protocol

(B) secure network management protocol

(C) systematic network management protocol

(D) secure network monitoring protocol

37. Which of the following is not a component of the SNMP architecture

(A) network management system(NMS)

(B) managed device

(C) management information base(MIB)

(D) transmission control protocol (TCP)

38. What is the primary function of the network management system (NMS) in SNMP?

(A) to store network data

(B) to monitor and manage network devices

(C) to transmit SNMP traps

(D) to compile MIB definitions

36. SNMP कम्प्यूटर नेटवर्किंगमा के लागछ?

(A) सरल नेटवर्क निगरानी प्रोटोकॉल

(B) सुरक्षित नेटवर्क प्रबंधन प्रोटोकॉल

(C) व्यवस्थित नेटवर्क प्रबंधन प्रोटोकॉल

(D) सुरक्षित नेटवर्क निगरानी प्रोटोकॉल

37. निम्नलिखित में से कौन सा एसएनएमपी आर्किटैक्चर का एक घटक नहीं है।

(A) नेटवर्क प्रबंधन प्रणाली (NMS)

(B) प्रबंधित डिवाइस

(C) प्रबंधन सूचना आधार (MIB)

(D) ट्रांसमिशन कंट्रोल प्रोटोकॉल (TCP)

38. एसएनएमपी में नेटवर्क प्रबंधन प्रणाली (एनएमएस) का प्राथमिक कार्य क्या है।

(A) नेटवर्क डेटा स्टोर करने के लिए

(B) नेटवर्क उपकरणों की निगरानी और प्रबंधन करने के लिए

(C) SNMP जाल संचारित करने के लिए

(D) एमआईबी परिभाषाओं को संकलित करने के लिए

https://www.msustudy.com

39. Which version of SNMP introduced the user-based security model (USM)?

(A) SNMPv1

(B) SNMPv2c

(C) SNMPv2u

(D) SNMPv3

40. What is the purpose of the SNMP trap in network management?

(A) to request information from a managed device

(B) to initiate a configuration change on a managed device

(C) to notify the SNMP manager of significant events

(D) to authenticate users accessing the MIB

41. Which protocol is commonly used to transport SNMPv3 messages securely?

(A) TCP

(B) UDP

(C) SSH

(D) TLS

39. SNMP के किस संस्करण ने उपयोगकर्ता-आधारित सुरक्षा मॉडल (USM) पेश किया।

(A) एसएनएमपीवी 1

(B) एसएनएमपीवी 2 सी

(C) एसएनएमपीवी 2 यू

(D) एसएनएमपीवी 3

40. नेटवर्क प्रबंधन में एसएनएमपी ट्रैप का उद्देश्य क्या है।

(A) प्रबंधित डिवाइस से जानकारी का अनुरोध करने के लिए

(B) प्रबंधित डिवाइस पर कॉन्फिगरेशन परिवर्तन आरंभ करने के लिए

(C) महत्वपूर्ण घटनाओं के SNMP प्रबंधक को सूचित करने के लिए

(D) MIB तक पहुँचने वाले उपयोगकर्ताओं को प्रमाणित करने के लिए

41. SNMPv3 संदेशों को सुरक्षित रूप से परिवहन करने के लिए आमतौर पर किस प्रोटोकॉल का उपयोग किया जाता है।

(A) टीसीपी

(B) यूडीपी

(C) एसएसएच

(D) टीएलएस

https://www.msustudy.com

42. Which SNMP version provides support for cryptographic security features such as encryption and authentication

(A) SNMPv1

(B) SNMPv2c

(C) SNMPv2u

(D) SNMPv3

43. What is the primary functions of the SNMPv3 USM (user-based security model)?

(A) to provide community - based security

(B) to encrypt SNMP messages

(C) to authenticate SNMP messages

(D) to manage SNMP views

44. Which of the following is not a benefit of using SNMPv3 over SNMPv1 or SNMPv2?

(A) stronger security features

(B) improved error handling

(C) enhanced MIB support

(D) better performance

45. What is the purpose of the SNMP agent in network management?

(A) to manage network devices

(B) to authenticate SNMP managers

(C) to generate SNMP traps

(D) to compile MIB definitions

42. कौन सा एसएनएमपी संस्करण एन्क्रिप्शन और प्रमाणीकरण जैसी क्रिप्टोग्राफिक सुरक्षा सुविधाओं के लिए समर्थन प्रदान करता है।

(A) एसएनएमपीवी 1

(B) एसएनएमपीवी 2 सी

(C) एसएनएमपीवी 2 यू

(D) एसएनएमपीवी 3

43. SNMPv3 USM उपयोगकर्ता आधारित सुरक्षा मॉडल का प्राथमिक कार्य क्या है।

(A) समुदाय आधारित सुरक्षा प्रदान करना

(B) SNMP संदेश एन्क्रिप्ट करना

(C) SNMP संदेशों को प्रमाणित करने के लिए

(D) SNMP दृश्य का व्यवस्थापन करना

44. SNMPv1 या SNMPv2 की तुलना में SNMPv3 का उपयोग करने का निम्नलिखित में से क्या लाभ नहीं है।

(A) मजबूत सुरक्षा सुविधाएँ

(B) बेहतर त्रुटि हैंडलिंग

(C) उन्नत MIB समर्थन

(D) बेहतर प्रदर्शन

45. नेटवर्क प्रबंधन में एसएनएमपी एजेंट का उद्देश्य क्या है।

(A) नेटवर्क उपकरणों का प्रबंधन करने के लिए

(B) SNMP प्रबन्धकहरूलाई प्रमाणित करने के लिए

(C) SNMP जाल उत्पन्न करने के लिए

(D) एमआईबी परिभाषाओं को संकलित करने के लिए

https://www.msustudy.com

46. In Kerberos, what is the function of the Key Distribution Center (KDC)?

(A) Generates public-private key pairs

(B) Stores passwords in plaintext

(C) Issues ticket-granting tickets (TGTs)

(D) Encrypts session keys

47. What is the purpose of a Certificate Authority (CA) in X.509?

(A) To issue certificates

(B) To manage encryption keys

(C) To authenticate users

(D) To handle email encryption

48. Which authentication service provides a centralized database of user credentials?

(A) Kerberos

(B) X.509

(C) Directory Authentication Service

(D) S/MIME

49. What does PGP stand for in network security?

(A) Pretty Good Protocol

(B) Public Guardian Protocol

(C) Pretty Good Privacy

(D) Public Guardian Privacy

46. केर्बेरोस में, कुंजी वितरण केंद्र (केडीसी) का कार्य क्या है?

(A) सार्वजनिक-निजी कुंजी जोड़े उत्पन्न करता है

(B) सादे पाठ में पासवर्ड स्टोर करता है

(C) टिकट ग्रांटिंग टिकट (TGT) जारी करता है

(D) सत्र कुंजियों को एन्क्रिप्ट करता है

47. X.509 में सर्टिफिकेट अथॉरिटी (CA) का उद्देश्य क्या है?

(A) प्रमाण पत्र जारी करने के लिए

(B) एन्क्रिप्शन कुंजियों को प्रबंधित करने के लिए

(C) उपयोगकर्ताओं को प्रमाणित करने के लिए

(D) ईमेल एन्क्रिप्शन को संभालने के लिए

48. कौन सी प्रमाणीकरण सेवा उपयोगकर्ता क्रेडेंशियल्स का एक केंद्रीकृत डेटाबेस प्रदान करती है?

(A) केर्बेरोस

(B) X.509

(C) निर्देशिका प्रमाणीकरण सेवा

(D) एस/माइम

49. नेटवर्क सुरक्षा में PGP का क्या अर्थ है?

(A) प्रीटी गुड प्रोटोकॉल

(B) पब्लिक गार्जियन प्रोटोकॉल

(C) प्रीटी गुड प्राइवेसी

(D) पब्लिक गार्जियन प्राइवेसी

https://www.msustudy.com

50. Which of the following is NOT true about X.509 certificates?

(A) They contain a public key

(B) They are signed by a Certificate Authority (CA)

(C) They can be decrypted by anyone

(D) They have an expiration date

51. What is the primary role of a digital certificate in the X.509 infrastructure?

(A) Encrypt data

(B) Authenticate users

(C) Store private keys

(D) Manage network traffic

52. Which encryption algorithm is commonly used in S/MIME for securing email messages?

(A) AES

(B) RSA

(C) Triple DES

(D) Blowfish

53. What is the primary purpose of the Key Distribution Center (KDC) in Kerberos?

(A) To store passwords

(B) To issue tickets

(C) To manage encryption keys

(D) To authenticate users

50. X.509 प्रमाणपत्रों के बारे में निम्नलिखित में से कौन सा सत्य नहीं है?

(A) उनमें एक सार्वजनिक कुंजी होती है

(B) वे एक प्रमाणपत्र प्राधिकरण (सीए) द्वारा हस्ताक्षरित हैं

(C) उन्हें किसी के द्वारा डिक्रिप्ट किया जा सकता है

(D) उनकी समाप्ति तिथि है

51. X.509 बुनियादी ढांचे में डिजिटल प्रमाणपत्र की प्राथमिक भूमिका क्या है?

(A) डेटा एन्क्रिप्ट करें

(B) उपयोगकर्ताओं को प्रमाणित करें

(C) निजी चाबियाँ स्टोर करें

(D) नेटवर्क ट्रैफ़िक प्रबंधित करें

52. ईमेल संदेशों को सुरक्षित करने के लिए S/MIME में आमतौर पर किस एन्क्रिप्शन एल्गोरिथ्म का उपयोग किया जाता है?

(A) एईएस

(B) आरएसए

(C) ट्रिपल डेस

(D) ब्लोफिश

53. केर्बेरोस में प्रमुख वितरण केंद्र (केडीसी) का प्राथमिक उद्देश्य क्या है?

(A) पासवर्ड स्टोर करने के लिए

(B) टिकट जारी करने के लिए

(C) एन्क्रिप्शन कुंजियों का प्रबंधन करने के लिए

(D) उपयोगकर्ताओं को प्रमाणित करने के लिए

https://www.msustudy.com

54. In X.509, what is the function of the Certificate Revocation List (CRL)?
(A) It lists all the valid certificates
(B) It verifies the authenticity of certificates
(C) It lists revoked certificates
(D) It encrypts communication

55. Which protocol is commonly used for secure remote authentication within a network using tickets?
(A) HTTPS
(B) SSH
(C) Kerberos
(D) SNMP

56. What type of cryptography is primarily used in Pretty Good Privacy (PGP)?
(A) Symmetric-key
(B) Asymmetric-key
(C) Hybrid
(D) Quantum

57. What component of Kerberos is responsible for authenticating users and services?
(A) Authentication Server (AS)
(B) Ticket Granting Server (TGS)
(C) Ticket-Granting Ticket (TGT)
(D) Key Distribution Center (KDC)

54. X.509 में, प्रमाणपत्र निरस्तीकरण सूची (CRL) का कार्य क्या है?
(A) यह सभी वैध प्रमाणपत्रों को सूचीबद्ध करता है
(B) यह प्रमाण पत्र की प्रामाणिकता की पुष्टि करता है
(C) यह निरस्त प्रमाणपत्रों को सूचीबद्ध करता है
(D) यह संचार को एन्क्रिप्ट करता है

55. टिकटों का उपयोग करके नेटवर्क के भीतर सुरक्षित दूरस्थ प्रमाणीकरण के लिए आमतौर पर किस प्रोटोकॉल का उपयोग किया जाता है?
(A) एचटीटीपीएस
(B) एसएसएच
(C) केर्बेरोस
(D) एसएनएमपी

56. प्रीटी गुड प्राइवेसी (PGP) में मुख्य रूप से किस प्रकार की क्रिप्टोग्राफी का उपयोग किया जाता है?
(A) सममित-कुंजी
(B) असममित-कुंजी
(C) हाइब्रिड
(D) क्वांटम

57. उपयोगकर्ताओं और सेवाओं को प्रमाणित करने के लिए Kerberos का कौन सा घटक जिम्मेदार है?
(A) प्रमाणीकरण सर्वर (AS)
(B) टिकट ग्रांटिंग सर्वर (TGS)
(C) टिकट-ग्रांटिंग टिकट (TGT)
(D) प्रमुख वितरण केंद्र (KDC)

https://www.msustudy.com

58. What does the acronym TGT stand for in the Kerberos authentication protocol?

(A) Ticket-Granting Ticket

(B) Token Generation Token

(C) Ticket Generation Token

(D) Token-Granting Ticket

59. Which of the following is a disadvantage of using a directory service for authentication?

(A) Centralized management

(B) Single point of failure

(C) Enhanced security

(D) Rapid scalability

60. What does S/MIME provide in email communication?

(A) Authentication and integrity

(B) Compression and encryption

(C) Digital signatures and encryption

(D) File transfer security

61. What is the primary purpose of the Authentication Header (AH) in IPsec.

(A) Providing confidentiality

(B) Ensuring data integrity and authentication

(C) Encrypting data traffic

(D) Managing encryption keys

58. केर्बेरोस प्रमाणीकरण प्रोटोकॉल में टीजीटी का संक्षिप्त नाम क्या है?

(A) टिकट ग्रांटिंग टिकट

(B) टोकन जनरेशन टोकन

(C) टिकट जनरेशन टोकन

(D) टोकन-ग्रांटिंग टिकट

59. प्रमाणीकरण के लिए निर्देशिका सेवा का उपयोग करने का निम्नलिखित में से क्या नुकसान है?

(A) केंद्रीकृत प्रबंधन

(B) विफलता का एकल बिंदु

(C) बढ़ी हुई सुरक्षा

(D) तीव्र मापनीयता

60. ईमेल संचार में S/MIME क्या प्रदान करता है?

(A) प्रमाणीकरण और अखंडता

(B) संपीडन और एन्क्रिप्शन

(C) डिजिटल हस्ताक्षर और एन्क्रिप्शन

(D) फ़ाइल स्थानांतरण सुरक्षा

61. IPsec में प्रमाणीकरण हैडर (AH) का प्राथमिक उद्देश्य क्या है?

(A) गोपनीयता प्रदान करना

(B) डेटा अखंडता और प्रमाणीकरण सुनिश्चित करना

(C) डेटा ट्रैफ़िक को एन्क्रिप्ट करना

(D) एन्क्रिप्शन कुंजियों का प्रबंधन

https://www.msustudy.com

62. Which of the following is NOT a function of the Authentication Header (AH)?

(A) Integrity protection

(B) Confidentiality

(C) Authentication

(D) Replay protection

63. In IPsec, which protocol provides encryption and authentication services?

(A) Authentication Header (AH)

(B) Encapsulating Security Payload (ESP)

(C) Internet Key Exchange (IKE)

(D) Secure Socket Layer (SSL)

64. What does ESP stand for in the context of IPsec?

(A) Encrypted Security Payload

(B) Encapsulated Security Protocol

(C) Encapsulating Security Payload

(D) Enhanced Security Protocol

65. Which IPsec component provides confidentiality, integrity, and optional authentication?

(A) Authentication Header (AH)

(B) Encapsulating Security Payload (ESP)

(C) Security Association (SA)

(D) Key Management Protocol (KMP)

62. निम्नलिखित में से कौन सा प्रमाणीकरण हैडर (AH) का कार्य नहीं है?

(A) अखंडता संरक्षण

(B) गोपनीयता

(C) प्रमाणीकरण

(D) रिप्ले सुरक्षा

63. IPsec में, कौन सा प्रोटोकॉल एन्क्रिप्शन और प्रमाणीकरण सेवाएं प्रदान करता है?

(A) प्रमाणीकरण हैडर (AH)

(B) सुरक्षा पेलोड (ESP) को एनकैप्सुलेट करना

(C) इंटरनेट कुंजी एक्सचेंज (IKE)

(D) सिक्योर सॉकेट लेयर (SSL)

64. IPsec के संदर्भ में ESP का क्या अर्थ है?

(A) एन्क्रिप्टेड सुरक्षा पेलोड

(B) एनकैप्सुलेटेड सिक्योरिटी प्रोटोकॉल

(C) सुरक्षा पेलोड को एनकैप्सुलेट करना

(D) उन्नत सुरक्षा प्रोटोकॉल

65. कौन सा IPsec घटक गोपनीयता, अखंडता और वैकल्पिक प्रमाणीकरण प्रदान करता है?

(A) प्रमाणीकरण हैडर (AH)

(B) सुरक्षा पेलोड को एनकैप्सुलेट करना (ESP)

(C) सुरक्षा संघ (SA)

(D) कुंजी प्रबंधन प्रोटोकॉल (KMP)

https://www.msustudy.com

66. What is the purpose of a Security Association (SA) in IPsec?

(A) To manage encryption keys

(B) To encrypt data traffic

(C) To establish a secure tunnel

(D) To authenticate users

67. Which protocol is used for negotiating Security Associations in IPsec?

(A) IPSec Security Protocol (ISSP)

(B) Internet Key Exchange (IKE)

(C) Authentication Header (AH)

(D) Encapsulating Security Payload (ESP)

68. What does IKE stand for in the context of IPsec?

(A) Internet Key Exchange

(B) Intrusion Key Encryption

(C) Integrated Key Encryption

(D) Interlink Key Exchange

69. Which phase of Internet Key Exchange (IKE) involves the negotiation of security parameters?

(A) Phase 1

(B) Phase 2

(C) Phase 3

(D) Phase 4

66. IPsec में एक सुरक्षा संघ (SA) का उद्देश्य क्या है?

(A) एन्क्रिप्शन कुंजियों का प्रबंधन करने के लिए

(B) डेटा ट्रैफ़िक को एन्क्रिप्ट करने के लिए

(C) एक सुरक्षित सुरंग स्थापित करना

(D) उपयोगकर्ताओं को प्रमाणित करने के लिए

67. IPsec में सुरक्षा संघों पर बातचीत करने के लिए किस प्रोटोकॉल का उपयोग किया जाता है?

(A) IPsec सुरक्षा प्रोटोकॉल (ISSP)

(B) इंटरनेट कुंजी एक्सचेंज (IKE)

(C) प्रमाणीकरण हैडर (AH)

(D) सुरक्षा पेलोड को एनकैप्सुलेट करना (ESP)

68. IPsec के संदर्भ में IKE का क्या अर्थ है?

(A) इंटरनेट कुंजी विनिमय

(B) घुसपैठ कुंजी एन्क्रिप्शन

(C) एकीकृत कुंजी एन्क्रिप्शन

(D) इंटरलिंक कुंजी विनिमय

69. इंटरनेट कुंजी एक्सचेंज (IKE) के किस चरण में सुरक्षा मापदंडों की बातचीत शामिल है?

(A) चरण 1

(B) चरण 2

(C) चरण 3

(D) चरण 4

https://www.msustudy.com

70. Which key management protocol is commonly used in IPsec VPN deployments?

(A) SSL/TLS

(B) SNMP

(C) IKE

(D) SSH

71. In IPsec, what is the purpose of the Security Parameter Index (SPI)?

(A) To uniquely identify a Security Association

(B) To encrypt data packets

(C) To authenticate users

(D) To manage encryption keys

72. What is the function of the Security Association Database (SAD) in IPsec?

(A) To store security policies

(B) To manage encryption keys

(C) To authenticate users

(D) To encrypt data traffic

73. Which key management protocol is used for manual keying in IPsec?

(A) Internet Key Exchange (IKE)

(B) Simple Key Exchange Protocol (SKEP)

(C) Kerberos

(D) Secure Shell (SSH)

70. IPsec VPN परिनियोजन में आमतौर पर किस कुंजी प्रबंधन प्रोटोकॉल का उपयोग किया जाता है?

(A) एसएसएल/टीएलएस

(B) एसएनएमपी

(C) आईकेई

(D) एसएसएच

71. IPsec में, सुरक्षा पैरामीटर इंडेक्स (SPI) का उद्देश्य क्या है?

(A) विशिष्ट रूप से एक सुरक्षा संघ की पहचान करने के लिए

(B) डेटा पैकेट एन्क्रिप्ट करने के लिए

(C) उपयोगकर्ताओं को प्रमाणित करने के लिए

(D) एन्क्रिप्शन कुंजियों का प्रबंधन करने के लिए

72. IPsec में सुरक्षा एसोसिएशन डेटाबेस (SAD) का कार्य क्या है?

(A) सुरक्षा नीतियों को संग्रहित करने के लिए

(B) एन्क्रिप्शन कुंजियों का प्रबंधन करने के लिए

(C) उपयोगकर्ताओं को प्रमाणित करने के लिए

(D) डेटा ट्रैफ़िक को एन्क्रिप्ट करने के लिए

73. IPsec में मैनुअल कुंजीयन के लिए किस कुंजी प्रबंधन प्रोटोकॉल का उपयोग किया जाता है?

(A) इंटरनेट कुंजी एक्सचेंज (IKE)

(B) सिंपल की एक्सचेंज प्रोटोकॉल (SKEP)

(C) केर्बेरोस

(D) सिक्योर शेल (SSH)

https://www.msustudy.com

74. What does KMP stand for in the context of IPsec?

(A) Key Management Protocol

(B) Key Mapping Protocol

(C) Key Migration Protocol

(D) Key Monitoring Protocol

75. Which phase of Internet Key Exchange (IKE) establishes a secure channel for exchanging keying material?

(A) Phase 1

(B) Phase 2

(C) Phase 3

(D) Phase 4

76. Which IPsec component provides anti-replay protection?

(A) Security Association (SA)

(B) Authentication Header (AH)

(C) Encapsulating Security Payload (ESP)

(D) Internet Key Exchange (IKE)

77. In IPsec, what is the purpose of a Diffie-Hellman exchange?

(A) To authenticate users

(B) To negotiate encryption keys

(C) To encrypt data packets

(D) To establish a secure tunnel

74. IPsec के संदर्भ में KMP का क्या अर्थ है?

(A) कुंजी प्रबंधन प्रोटोकॉल

(B) कुंजी मानचित्रण प्रोटोकॉल

(C) प्रमुख प्रवासन प्रोटोकॉल

(D) प्रमुख निगरानी प्रोटोकॉल

75. इंटरनेट कुंजी एक्सचेंज (IKE) का कौन सा चरण कुंजीयन सामग्री के आदान-प्रदान के लिए एक सुरक्षित चैनल स्थापित करता है?

(A) चरण 1

(B) चरण 2

(C) चरण 3

(D) चरण 4

76. कौन सा IPsec घटक एंटी-रिप्ले सुरक्षा प्रदान करता है?

(A) सुरक्षा संघ (SA)

(B) प्रमाणीकरण हैडर (AH)

(C) सुरक्षा पेलोड को एनकैप्सुलेट करना (ESP)

(D) इंटरनेट कुंजी एक्सचेंज (IKE)

77. IPsec में, डिफी-हेलमैन एक्सचेंज का उद्देश्य क्या है?

(A) उपयोगकर्ताओं को प्रमाणित करने के लिए

(B) एन्क्रिप्शन कुंजियों पर बातचीत करने के लिए

(C) डेटा पैकेट एन्क्रिप्ट करने के लिए

(D) एक सुरक्षित सुरंग स्थापित करना

https://www.msustudy.com

78. What is the primary function of a Security Policy Database (SPD) in IPsec?

(A) To manage encryption keys

(B) To store security policies

(C) To authenticate users

(D) To encrypt data traffic

79. Which phase of Internet Key Exchange (IKE) establishes the IPsec Security Associations?

(A) Phase 1

(B) Phase 2

(C) Phase 3

(D) Phase 4

80. What is the main advantage of using IPsec for securing network communications?

(A) Enhanced network performance

(B) Simplified key management

(C) Protection against eavesdropping and tampering

(D) Reduced network latency

78. IPsec में सुरक्षा नीति डेटाबेस (SPD) का प्राथमिक कार्य क्या है?

(A) एन्क्रिप्शन कुंजियों का प्रबंधन करने के लिए

(B) सुरक्षा नीतियों को संग्रहित करने के लिए

(C) उपयोगकर्ताओं को प्रमाणित करने के लिए

(D) डेटा ट्रैफिक को एन्क्रिप्ट करने के लिए

79. इंटरनेट कुंजी एक्सचेंज (IKE) का कौन सा चरण IPsec सुरक्षा संघों की स्थापना करता है?

(A) चरण 1

(B) चरण 2

(C) चरण 3

(D) चरण 4

80. नेटवर्क संचार को सुरक्षित करने के लिए IPsec का उपयोग करने का मुख्य लाभ क्या है?

(A) उन्नत नेटवर्क प्रदर्शन

(B) सरलीकृत कुंजी प्रबंधन

(C) ईव्सड्रॉपिंग (चोरी हुये सुनना) और छेड़छाड़ से सुरक्षा

(D) कम नेटवर्क विलंबता

https://www.msustudy.com

81. What is the primary purpose of Secure Socket Layer (SSL) and Transport Layer Security (TLS) protocols?

(A) To provide secure email communication

(B) To encrypt data at the network layer

(C) To secure web communication over the Internet

(D) To authenticate users in a local network

82. Which of the following is NOT a requirement for secure communication over the internet?

(A) Authentication

(B) Confidentiality

(C) Scalability

(D) Integrity

83. Which cryptographic protocol is the predecessor of Transport Layer Security (TLS)?

(A) Secure Socket Layer (SSL)

(B) Simple Mail Transfer Protocol (SMTP)

(C) Internet Protocol Security (IPsec)

(D) Point-to Point Protocol (PPP)

81. सिक्योर सॉकेट लेयर (एसएसएल) और ट्रांसपोर्ट लेयर सिक्योरिटी (टीएलएस) प्रोटोकॉल का प्राथमिक उद्देश्य क्या है?

(A) सुरक्षित ईमेल संचार प्रदान करने के लिए

(B) नेटवर्क परत लेयर पर डेटा एन्क्रिप्ट करने के लिए

(C) इंटरनेट पर वेब संचार को सुरक्षित करने के लिए

(D) स्थानीय नेटवर्क में उपयोगकर्ताओं को प्रमाणित करने के लिए

82. इंटरनेट पर सुरक्षित संचार के लिए निम्नलिखित में से कौन सा आवश्यक नहीं है?

(A) प्रमाणीकरण

(B) गोपनीयता

(C) मापनीयता

(D) अखंडता

83. कौन सा क्रिप्टोग्राफिक प्रोटोकॉल ट्रांसपोर्ट लेयर सिक्योरिटी (TLS) का पूर्ववर्ती है?

(A) सिक्योर सॉकेट लेयर (SSL)

(B) सिंपल मेल ट्रांसफर प्रोटोकॉल (SMTP)

(C) इंटरनेट प्रोटोकॉल सुरक्षा (IPsec)

(D) पॉइंट-टू-पॉइंट प्रोटोकॉल (PPP)

https://www.msustudy.com

84. Which layer of the OSI model do SSL and TLS operate on?

(A) Network Layer

(B) Transport Layer

(C) Session Layer

(D) Application Layer

85. What is the primary function of SSL and TLS?

(A) Encrypting data at rest

(B) Authenticating users

(C) Providing secure communication channels

(D) Managing network traffic

86. Which protocol is commonly used for securing email communication?

(A) SSL

(B) TLS

(C) HTTPS

(D) FTPS

87. What cryptographic algorithm is commonly used in SSL and TLS for key exchange and encryption?

(A) AES

(B) RSA

(C) DES

(D) SHA

84. एसएसएल और टीएलएस ओएसआई मॉडल की किस परत लेयर पर काम करते हैं?

(A) नेटवर्क लेयर

(B) ट्रांसपोर्ट लेयर

(C) सेशन लेयर

(D) एप्लीकेशन लेयर

85. एसएसएल और टीएलएस का प्राथमिक कार्य क्या है?

(A) आराम से डेटा एन्क्रिप्ट करना

(B) उपयोगकर्ताओं को प्रमाणित करना

(C) सुरक्षित संचार चैनल प्रदान करना

(D) नेटवर्क ट्रैफ़िक का प्रबंधन

86. ईमेल संचार को सुरक्षित करने के लिए आमतौर पर किस प्रोटोकॉल का उपयोग किया जाता है?

(A) एसएसएल

(B) टीएलएस

(C) एचटीटीपीएस

(D) एफटीपीएस

87. कुंजी विनिमय और एन्क्रिप्शन के लिए एसएसएल और टीएलएस में आमतौर पर किस क्रिप्टोग्राफिक एल्गोरिथ्म का उपयोग किया जाता है?

(A) एईएस

(B) आरएसए

(C) डीईएस

(D) एसएचए

https://www.msustudy.com

88. Which of the following is NOT a security feature provided by SSL and TLS?

(A) Authentication

(B) Data compression

(C) Integrity protection

(D) Confidentiality

89. What is the primary role of the SSL Handshake Protocol?

(A) Establishing a secure connection

(B) Encrypting data transmission

(C) Authenticating the server

(D) Managing encryption keys

90. Which version of SSL introduced significant security vulnerabilities leading to its deprecation?

(A) SSL 1.0

(B) SSL 2.0

(C) SSL 3.0

(D) SSL 4.0

91. What is the primary purpose of Secure Electronic Transactions (SET)?

(A) Secure online shopping

(B) Secure file transfer

(C) Secure email communication

(D) Secure social media interaction

88. निम्नलिखित में से कौन सा एसएसएल और टीएलएस द्वारा प्रदान की गई सुरक्षा सुविधा नहीं है?

(A) प्रमाणीकरण

(B) डेटा संपीडन

(C) अखंडता संरक्षण

(D) गोपनीयता

89. एसएसएल हैंडशेक प्रोटोकॉल की प्राथमिक भूमिका क्या है?

(A) एक सुरक्षित कनेक्शन स्थापित करना

(B) डेटा ट्रांसमिशन को एन्क्रिप्ट करना

(C) सर्वर को प्रमाणित करना

(D) एन्क्रिप्शन कुंजियों का प्रबंधन

90. एसएसएल के किस संस्करण ने महत्वपूर्ण सुरक्षा कमजोरियों को पेश किया जिससे इसका बहिष्करण हुआ?

(A) एसएसएल 1.0

(B) एसएसएल 2.0

(C) एसएसएल 3.0

(D) एसएसएल 4.0

91. सुरक्षित इलेक्ट्रॉनिक लेनदेन (एसईटी) का प्राथमिक उद्देश्य क्या है?

(A) सुरक्षित ऑनलाइन शॉपिंग

(B) सुरक्षित फ़ाइल स्थानांतरण

(C) सुरक्षित ईमेल संचार

(D) सुरक्षित सोशल मीडिया इंटरैक्शन

https://www.msustudy.com

92. Which organization developed the Secure Electronic Transactions (SET) protocol?

(A) Internet Engineering Task Force (IETF)

(B) World Wide Web Consortium (W3C)

(C) Visa and Mastercard

(D) International Organization for Standardization (ISO)

93. In the context of SSL/TLS, what is a Certificate Authority (CA) responsible for?

(A) Encrypting data transmission

(B) Authentication users

(C) Issuing digital certificates

(D) Managing encryption keys

94. Which cryptographic protocol is commonly used for securing web browsing sessions?

(A) HTTP

(B) SMTP

(C) FTP

(D) HTTPS

92. किस संगठन ने सिक्योर इलेक्ट्रॉनिक लेनदेन (SET) प्रोटोकॉल विकसित किया?

(A) इंटरनेट इंजीनियरिंग टास्क फोर्स (IETF)

(B) वर्ल्ड वाइड वेब कंसोर्टियम (W3C)

(C) वीज़ा और मास्टरकार्ड

(D) अन्तर्राष्ट्रीय मानकीकरण संगठन (आईएसओ)

93. एसएसएल/टीएलएस के संदर्भ में, सर्टिफिकेट अथॉरिटी (सीए) किसके लिए जिम्मेदार है?

(A) डेटा ट्रांसमिशन को एन्क्रिप्ट करना

(B) उपयोगकर्ताओं को प्रमाणित करना

(C) डिजिटल प्रमाणपत्र जारी करना

(D) एन्क्रिप्शन कुंजियों का प्रबंधन

94. वेब ब्राउज़िंग सत्रों को सुरक्षित करने के लिए आमतौर पर किस क्रिप्टोग्राफिक प्रोटोकॉल का उपयोग किया जाता है?

(A) एचटीटीपी

(B) एसएमटीपी

(C) एफ़टीपी

(D) एचटीटीपीएस

https://www.msustudy.com

95. What does HTTPS stand for?

(A) Hypertext Transfer Protocol Secure

(B) Hypertext Transmission Protocol Secure

(C) Hypertext Transfer Protocol Standard

(D) Hypertext Transmission Protocol Standard

96. Which component of SSL/TLS is responsible for negotiating encryption algorithms and exchanging cryptographic keys?

(A) Handshake Protocol

(B) Record Protocol

(C) Change Cipher Spec Protocol

(D) Alert Protocol

97. Which version of TLS addressed vulnerabilities found in SSL 3.0 and its predecessors?

(A) TLS 1.0

(B) TLS 1.1

(C) TLS 1.2

(D) TLS 1.3

95. HTTPS का क्या अर्थ है?

(A) हाइपरटेक्स्ट ट्रांसफर प्रोटोकॉल सिक्योर

(B) हाइपरटेक्स्ट ट्रांसमिशन प्रोटोकॉल सिक्योर

(C) हाइपरटेक्स्ट ट्रांसफर प्रोटोकॉल स्टैंडर्ड

(D) हाइपरटेक्स्ट ट्रांसमिशन प्रोटोकॉल मानक

96. एसएसएल/टीएलएस का कौन सा घटक एन्क्रिप्शन एल्गोरिदम पर बातचीत करने और क्रिप्टोग्राफिक कुंजी का आदान-प्रदान करने के लिए जिम्मेदार है?

(A) हैंडशेक प्रोटोकॉल

(B) रिकॉर्ड प्रोटोकॉल

(C) सिफर स्पेक प्रोटोकॉल बदलें

(D) अलर्ट प्रोटोकॉल

97. टीएलएस के किस संस्करण ने एसएसएल 3.0 और उसके पूर्ववर्तियों में पाई गई कमजोरियों को संबोधित किया?

(A) टीएलएस 1.0

(B) टीएलएस 1.1

(C) टीएलएस 1.2

(D) टीएलएस 1.3

https://www.msustudy.com

98. What security measure doe SSL/TLS provide against eavesdropping?

(A) Data encryption

(B) User authentication

(C) Access control

(D) Intrusion detection

99. What is the purpose of the Record Protocol in SSL/TLS?

(A) To establish a secure connection

(B) To exchange cryptographic keys

(C) To encrypt and authenticate data

(D) To handle alerts and error message

100. In the context of SSL/TLS, what is a cipher suite?

(A) A set of cryptographic algorithms and key sizes used for encryption

(B) A protocol for secure key exchange

(C) An encryption key used for data transmission

(D) A digital certificate issued by a Certificate Authority

98. एसएसएल/टीएलएस ईवसड्रॉपिंग के खिलाफ क्या सुरक्षा उपाय प्रदान करता है?

(A) डेटा एन्क्रिप्शन

(B) उपयोगकर्ता प्रमाणीकरण

(C) अभिगम नियंत्रण

(D) घुसपैठ का पता लगाना

99. एसएसएल/टीएलएस में रिकॉर्ड प्रोटोकॉल का उद्देश्य क्या है?

(A) एक सुरक्षित कनेक्शन स्थापित करने के लिए

(B) क्रिप्टोग्राफिक कुंजियों का आदान-प्रदान करने के लिए

(C) डेटा को एन्क्रिप्ट और प्रमाणित करने के लिए

(D) अलर्ट और त्रुटि संदेशों को संभालने के लिए

100. एसएसएल/टीएलएस के संदर्भ में, सिफर सूट क्या है?

(A) एन्क्रिप्शन के लिए उपयोग किए जाने वाले क्रिप्टोग्राफिक एल्गोरिदम और कुंजी आकारों का एक सेट

(B) सुरक्षित कुंजी विनिमय के लिए एक प्रोटोकॉल

(C) डेटा ट्रांसमिशन के लिए उपयोग की जाने वाली एन्क्रिप्शन कुंजी

(D) प्रमाणपत्र प्राधिकारी द्वारा जारी एक डिजिटल प्रमाणपत्र

https://www.msustudy.com