SIDDHARTH GROUP OF INSTITUTIONS :: PUTTUR
Siddharth Nagar, Narayanavanam Road – 517583

QUESTION BANK (DESCRIPTIVE)

Subject with Code : CNS (13A05702) **Course & Branch**: B.Tech - CSE

Year & Sem: IV-B.Tech & I-Sem **Regulation:** R13

UNIT –I

1. A. Explain in detail different passive and active attacks. 5M
   B. What is software vulnerabalility? Explain various methods of vulnerability 5M
2. A. What is meant by security service? Explain various security services listed in X.800. 6M
   B. Differentiate the cipher properties of confusion and diffusion. 4M
3. A. Compare all the features of stream and block ciphers. 4M
   B. Explain about various non cryptographic vulnerabilities. 6M
4. A. Explain in detail the sub key generation and round function of DES algorithm in detail. 5M
   B. Explain the Fiestel cipher structure with a neat sketch. And also explain its importance. 5M
5. A. What is a security attack? Explain different security mechanism. 5M
   B. Explain the characteristics of block and stream ciphers. 5M
6. A. Define threat and attack. What is the difference between both? List some examples of attacks which have arisen in real world cases. 6M
   B. Describe the mechanisms for preventing and detecting hijacking problems. 4M
7. A. What is meant by Denial of Service (DOS), Spoofing & Phishing? Explain. 5M
   B. Explain Hill cipher with an example. 5M
8. Explain AES encryption and Decryption in detail. 10M
9. A. Compare the substitution method in DES and AES. Why do we need only one substitution table in AES, but several in DES? 6M
   B. What are the merits of Output-Feedback (OFB. as compared to Cipher Feedback (CFB. ? 4M
10. Write short notes on the following .
    A. OSI Security Architecture 2M
    B. Block cipher principles 2M
    C. Strength of DES 2M
    D. Linear and Differential cryptanalysis 2M
    E RC4 2M

UNIT 2

1. A. What is importance Chinese Remainder Theorem in cryptography? Explain. 5M
   B. Explain various logarithms used for modular arithmetic operations with example. 5M
2. A. State and prove Chinese remainder theorem. 6M
   B. Using CRT, solve for x for the following
   $x \equiv 2 \pmod 3$; $x \equiv 3 \pmod 5$; $x \equiv 2 \pmod 7$ 4M
3. A. Define some Elliptic curves on real numbers. Give the description of addition on those elliptic curves. 5M
   B. In what way Diffie Hellman key exchange algorithm prone to man in the middle attack? Explain. 5M
4. A. Given 2 as a primitive root of 29, construct a table of discrete logarithms, and use it to solve the congruence: 5M
   B. Use Euler's theorem to find a number between 0 and 28 with congruent to 6 modulo 35. 5M
5. A. What is a primitive root? Find all the primitive roots of 25. 6M
   B. What is the difference between an index and a discrete logarithm? 4M
6. Discuss the following related to Elliptic Curve Cryptography(ECC.
   A. ECC Encryption / Decryption and Security of ECC 5M
   B. ECC Diffie Hellman Key Exchange 5M
7. A. Explain Fermat's theorem and Euler totient function with an example each. 5M
   B. Discuss the following with respect to prime numbers 5M
   i) Relatively prime numbers ii) Test for primality.
8. A. What is an elliptic curve? Explain encryption in this context. 5M
   B. Explain about the strength of RSA. 5M
9. A. Explain the RSA algorithm. Compute cipher text for M=88, p=17 and q=11. 5M
   B. Differentiate Conventional encryption and public key encryption. 5M
10. Describe the following
    A. ELGamal cryptographic system 2M
    B. Factorization 2M
    C. Exponentiation and Logarithm 2M
    D. Principles of public-key cryptography 2M
    E. Elliptic Curve Arithmetic 2M

UNIT 3

1. A. Explain the process involved in message digest generation and processing of single block in SHA-512. 5M

   B. What is Message Authentication code? Explain its functions and basic uses. 5M

2. A. Explain in detail Digital Signature Standard approach and its algorithm 5M

   B. Explain requirements for Cryptographic Hash Functions. 5M

3. A. What is the purpose of digital signature? Explain its properties and requirements. 5M

   B. Explain two different MACs based on block ciphers. 5M

4. A. What is Hash function? Explain different applications of cryptographic hash functions. 5M

   B. Explain MACs based hash function with its design objectives and structure of the algorithm.5M

5. A. What is message authentication? List the authentication requirements. 6M

   B. Compare the principal characteristics of secure hash functions. 4M

6. A. What are the services provided by digital signatures? Explain if the following are provided 6M
   i) Source Authentication, ii) Data Integrity and iii) Source Non-Repudiation.

   B. What is Birthday Attack on Digital Signatures? Can it be performed by an 'Outsider'? 4M

7. A. List the generally accepted requirements for a cryptographic hash function. Explain each requirement. 5M

   B. Explain Digital signature scheme (DSS) and Digital Signature Algorithm (DSA. in detail. 5M

8. Describe the steps in message digest generation in Secure Hash Algorithm in detail. 10M

9. A. What is the difference between weak and strong collision resistance? 5M

   B. Describe the various modes of arbitrated digital signatures. 5M

10. Write short notes on the following

    A. Security of MACs 2M

    B. Applications of cryptographic hash functions 2M

    C. Message Authentication Codes 2M

    D. DSS 2M

    e) HMAC 2M

UNIT 4

1. A. Explain how authentication is performed in Kerberos. 5M
   B. Enumerate the differences between Kerberos Version 4 and 5. 5M
2. A. Write note on PGP session keys, public/private key rings and passphrase keys. 5M
   B. What are the similarities and differences between S? MIME and PGP? 5M
3. A. Give the format for X.509 certificate. How are users certificates obtained? 5M
   B. Explain the authentication services provided by X.509. 5M
4. A. Explain how email messages are protected using S/MIME signing and encryption? 5M
   B. What is Radix 64 format? What is its use in PGP? 5M
5. A. Explain key management and distribution in detail. 5M
   B. Describe Remote user Authentication Principles 5M
6. A. Write and explain typical approaches used to distribute the symmetric using asymmetric encryption. 5M
   B. Write and explain Client/ Server Authentication Exchange service in Kerberos version 4. 5M
7. A. What is Public Key certificate? Explain its usage with X.509 certificates. 5M
   B. Write the general format of PGP Message. Explain the PGP message generation from User A to User B with no compression. 5M
8. A. Draw and explain the architecture model and management functions of Public Key-Infrastructure. 5M
   B. Write and explain various PGP cryptographic functions and services in detail. 5M
9. A. Explain different approaches used for symmetric key distribution using symmetric-encryption. 5M
   B. With a neat sketch explain overview of Message Exchanges in Kerberos version 5. 5M
10. Write short notes on the following
    A. PGP
    2M
    B. S/MIME 2M
    C. Federal Identity Management 2M
    D. Public Key Infrastructure 2M
    e) Symmetric key distribution using Asymmetric encryption 2M

UNIT 5

1. A. What is the use of SSL protocol? Explain SSL record protocol operation with SSL record format. 5M

   B. What is the need for encapsulation of Security Payload? Write and explain different fields of top level format and substructure of ESP packet. 5M

2. A. Write and explain TLS functions and alert codes of Transport Layer Security. 5M

   B. Explain the scope of ESP encryption and authentication in tunnel mode. 5M

3. A. With a neat sketch explain the IPSec scenario and IPSec Services. 5M

   B. Why Internet Key Exchange is used? Write and explain header and payload formats of it. 5M

4. A. Draw and discuss the Architecture of IPSec 5M

   B. What is the need to combine Security Associations? Explain basic combinations of Security Associations. 5M

5. A. Explain ESP Header of IP Sec. 5M

   B. Explain different Web security requirement. 5M

6. A. Give the taxonomy of malicious programs. Define each one. 5M

   B. What are the different types of viruses? How do they get into the systems? 5M

7. A. What is a firewall? What is the need for firewalls? What is the role of firewalls in protecting networks? 5M

   B. What is a worm? Name some known worms. 5M

8. A. What is meant by stateful packet inspection? What are the advantages and disadvantages? 5M

   B. Compare the features of host based IDS and network based IDS. Why, when and where to use host based IDS? 5M

9. A. Explain Unix Password management. 5M

   B. Explain Intrusion detection in detail.

10. Write short notes on the following

    A. Firewall Configurations 2M

    B. Viruses 2M

    C. Trusted Systems 2M

    D. Worms 2M

    e) HTTPS 2M

SIDDHARTH GROUP OF INSTITUTIONS :: PUTTUR
Siddharth Nagar, Narayanavanam Road – 517583

QUESTION BANK (OBJECTIVE)

Subject with Code : CNS (13A05702) **Course & Branch**: B.Tech - CSE

Year & Sem: IV-B.Tech & I-Sem **Regulation:** R13

UNIT – I

1. The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and _____ of information system resources. [ ]

A. Confidentiality B. Conformity C. Infirmity D.All

2. The protection afforded to an automated information system in order to attain the applicable objectives of preserving the_____, availability, and confidentiality of information system resources. [ ]

A. Conformity B. Integrity C. Infirmity D.None

3. The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity,_____, and confidentiality of information system resources. [ ]

A. Availability B. Liability C. Maintainability D.All

4. In NIST definition on Computer security, the keywords are _____ [ ]

A. Confidentiality B. Integrity C. Availability D.All

5. _____ assures that systems work promptly and service is not denied to authorized users. [ ]

A. Confidentiality B. Integrity C.Availability D.None

6. Among which is additional concepts for CIA traid _____ [ ]

A. Authenticity B. Accountability C. Both A & B D.None

7. _____ is the property of being genuine and being able to be verified and trusted. [ ]

A. Authenticity B. Accountability C. Both A & B D.None

8. The more critical a component or service, the higher is the level of _____ required. [ ]

A. Confidentiality B. Integrity C. Availability D.None

9. The _____ security architecture is useful to managers as a way of organizing the task of providing security. [ ]

A. OSI B. ISO C. Both A & B D.None

10. The OSI security architecture focuses on _____ [ ]

A. Security Attacks B. Mechanisms C. Services D. All

11. Any action that compromises the security of information owned by an organization is defined as _____ [ ]

A. Security Mechanism B. Security Attacks C. Security service D. None

12. They are _____ types of security attacks [ ]

A. 3 B. 2 C. 4 D. 5

13. Which kind of security attacks are difficult to detect? [ ]

A. Passive attack B. Active attack C. Both A & B D. None

14. A _____ takes place when one entity pretends to be a different entity. [ ]

A. Denial of service B. Masquerade C. Replay D. None

15. _____ divides these services into five categories and fourteen specific services. [ ]

A. RFC 2828 B. X.800 C. RFC 2929 D. X.8000

16. How many authentication service are there? [ ]

A. 2 B. 4 C. 5 D. 1

17. _____ is the ability to limit and control the access to host systems and applications via communications links. [ ]

A. Access confidentiality B. Access Control C. Data Integrity D. None

18. _____ define availability to be the property of a system or a system resource being accessible and usable upon demand by an authorized system entity, according to performance specifications for the system. [ ]

A. X.800 B. RFC 2828 C. Both A & B D. None

19. _____ treats availability as a property to be associated with various security services. [ ]

A. X.800 B. RFC 2828 C. Both A & B D. None

20. A symmetric encryption scheme has _____ ingredients. [ ]

A. 6 B. 4 C. 5 D. 7

21. The _____ performs various substitutions and transformations on the plain text. [ ]

A. Secret text B. Cipher text C. Encryption algorithm D. None

22. In Symmetric encryption scheme cipher text depends on _____ [ ]

A. Plain text B. Secret key C. Both A & B D. Encryption algorithm

23. The _____ only attack is the easiest to defend against because the opponent has the least amount of information to work with. [ ]

A. Secret text B. Cipher text C. Encryption algorithm D. None

24. A _____ involves trying every possible key until an intelligible translation of the ciphertext into plaintext is obtained. [ ]

A. Cipher-text attack B. Brute-force attack C. Both A & B D.None

25. The basic building blocks of all encryption technique is/are [ ]

A. Substitution B. Transportation C. Both A & B D. Substitution&Transposition

26. In _____ technique the plaintext is written down as a sequence of diagonals and then read off as a sequence of rows. [ ]

A. Brute-Force technique B. Rail fence C. Rail force D. None

27. A _____ is one that encrypts a digital data stream one bit or one byte at a time. [ ]

A. Stream cipher B. Block cipher C. Both A & B D. Digital data stream cipher

28. A desirable property of any encryption algorithm is that a small change in either the plaintext or the key should produce a significant change in the ciphertext is called _____ effect. [ ]

A. Avalanche B. Avalanshe C. Avalanghe D. None

29. Timing attacks are related to _____ [ ]

A. DES algorithm B. Public-key algorithm C. Both A & B D. None

30. The most significant advances in crypt analysis in recent years is _____. [ ]

A. Integral crypt analysis B. Differential crypt analysis C. Both A & B D. None

31. A loss of _____ is the unauthorized disclosure of information. [ ]

A. Integrity B. Confidentiality C. Availability D. None

32. A loss of _____ is the unauthorized modification or destruction of information. [ ]

A. Integrity B. Confidentiality C. Availability D. None

33. A loss of _____ is the disruption of access to or use of information or an information system. [ ]

A. Integrity B. Confidentiality C. Availability D. None

34. _____ means verifying that users are who they say they are and that each input arriving at the system came from a trusted source. [ ]

A. Accountability B. Authenticity C. Both A & B D. None

35. _____supports non-repudiation, deterrence, fault isolation, intrusion detection and prevention.[ ]

A. Accountability B. Authenticity C. Both A & B D. None

36. The loss could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals is have _____ impact. [ ]

A. Low B. Moderate C. High D. None

37. _____ authentication in a connection less transfer, provides assurance that the source of received data is as claimed. [ ]

A. Data-Origin B. Peer-entity C. Data-based D. Peer-server

38. The prevention of unauthorized use of a resource is called as _____ [ ]

A. Access-service B. Access-Control C. Access-protection D. Access-Prevention

39. Which among is not one of the data confidentiality _____ [ ]

A. Connection confidentiality C. Connection less Confidentiality

B. Selection -field confidentiality D. Traffic-Flow confidentiality

40. Proof that the message was sent by the specified party is called _____ [ ]

A. Non-repudiation,origin B. Non-repudiation,Destination C. Both A & B D. None

Unit-II

1. The binary operations defined for integers are _____ [ ]
   A. Addition B. Division C. Both A & B D. None
2. The Euclidean algorithm gives an efficient and systematic way to calculation of _____ [ ]
   A. LCM B. GCD C. HCF D. LCF
3. A linear Diophantine equation of to variables is _____ [ ]
   A. ax+by=c B. ax*by=c C. ax/by=c D. ax%by=c
4. In a mod n = r, "r" is called _____ [ ]
   A. Remainder B. Residue C. Both A & B D. None
5. The congruent operator is denoted by _____ [ ]
   A. # B. ^ C. + D. None
6. The combination of the set and the operations applied to elements of the set is called an _____[ ]
   A. Integral structure B. Algebraic structure C. Operational structure D. All
7. Which among the following are algebraic structure? [ ]
   A. Groups B. Rings C. Fields D. All
8. which among the following is Closure property _____ [ ]
   A. c=a*b B. a+(b+C. =(a+B. +c C. a*b=b*a D. None
9. A group is called a _____ group if the set has a finite number of elements. [ ]
   A. Define B. Finite C. Infinite D. All
10. If a subgroup of a group can be generated using power of an element , the sub group is called _____ [ ]
    A. Symmetric sub-group B. Associative sub-group C. Cyclic subgroup D. None
11. _____ theorem relates the order of a group to the order of its subgroup. [ ]
    A. Lagrange B. Brute-force C. Closure D. Commutative
12. A _____ is an algebraic structure with 2 operations [ ]
    A. Ring B. Field C. Both A & B D. None
13. The positive integers can be divided into _____ groups. [ ]
    A. 4 B. 3 C. 2 D. 5
14. Exponentation and logarithm are _____ of each other [ ]
    A. Similar B. Inverse C. Converse D. Diverse
15. Fast exponentation is possible using the _____ method [ ]
    A. Square-and-multiply B. Division-and –multiply C. Addition-and-Subtraction D. None
16. The bit-operation complexity of the fast exponential algorithm is _____ [ ]
    A. Polynomial B. Binomial C. Trivial D. None
17. A public-key encryption scheme has _____ ingredients. [ ]
    A. 6 B. 4 C. 5 D. 3

18. This is the readable message or data that is fed into the algorithm as input. [ ]

A. Cipher text B. Plain text C. Both A & B D. None

19. The _____ performs various transformations on the plain text. [ ]

A. Encryption Algorithm B. Decryption Algorithm C. Both A & B D. None

20. The concept of public-key cryptography evolved from an attempt to attack of _____ [ ]

A. Key distribution B. Digital signatures C. Both A & B D. None

21. _____ is the scrambled message produced as output. [ ]

A. Plain text B. Cipher text C. Both A & B D. None

22. How many keys are used for asymmetric encryption? [ ]

A. 2 B. 4 C. 5 D. 3

23. We can classify the use of public-key cryptosystems into _____ categories. [ ]

A. 4 B. 5 C. 2 D. 3

24. which among is one of the category of classification of public-key cryptosystems. [ ]

A. Encryption/decryption B. Key change C. Digital writing D. All

25. A problem is _____ if the effort to solve it grows faster than polynomial time as a function of input size. [ ]

A. In fusible B. In feasible C. Induble D. Includble

26. In RSA Algorithm "R" is referred to _____ [ ]

A. Rivest B. Ron C. Ron Rivest D. None

27. RSA algorithm is proposed by _____ [ ]

A. Ron Rivest B. Len Adleman C. Adi Shamir D. All

28. RSA algorithm is developed to meet requirements of _____ systems [ ]

A. Public-key systems B. Private-Key Systems C. Both A & B D. None

29. The RSA scheme is a block cipher in which the plaintext and ciphertext are integers between ____ and _____ for some n. [ ]

A. 0 and n-1 B. 1 and n C. 0 and n D. None

30. Possible approaches to attacking the RSA algorithm are _____ [ ]

A. Brute-force B. Mathematical attacks C. Timing attacks D. All

31. T. Elgamal announced a public-key scheme based on _____ logarithms. [ ]

A. Define B. Discrete C. Different D. None

32. a(b+C. =ab+ac is called _____ [ ]

A. Associative B. Distributive C. Closure D. Commutative

33. Elliptic curve cryptography makes use of elliptic curves in which the variables and coefficients are all restricted to elements of a _____ field. [ ]

A. Finite B. Infinite C. Define D. In define

34. Full form of ECC _____ [ ]

A. Elliptic curve crypto systems B. Elliptic curve cryptography

C. Elliptic curve cryptograph D. None

35. Security mechanisms typically involve _____ [ ]

A. Algorithm B. Protocol C. Both A & B D. None

36. One of the most useful results of number theory is the _____ theorem. [ ]

A. Chinese remainder B. Chinese quotient C. Chinese divisor D. None

37. Full form of DSA is _____ [ ]

A. Digital signal algorithm B. Digital system algorithm

C. Digital similar algorithm D. None

38. Asymmetric encryption can be used for _____ [ ]

A. Confidentiality B. Authentication C. Both A & B D. None

39. Asymmetric encryption transforms _____text into _____text using a one of two keys and an encryption algorithm. [ ]

A. Plain,cipher B. Cipher,Plain C. Both A & B D. None

40. The difficulty of attacking RSA is based on the difficulty of finding _____of a composite number. [ ]

A. Prime factors B. Divisors C. Factors D. None

UNIT III

1. The kind of hash functions needed for security applications is referred to as a __hash function. [ ]

A. Cryptographic B. Cryptosysytem C. Crypto D. Cryptography

2. Message _____ is a mechanism or service used to verify the integrity of a message. [ ]

A. Verification B. Authentication C. Protection D. Server

3. MAC refers to _____ [ ]

A. Method automatic function B. Method automate function

C. Method authentication function D. Message authentication function

4. MAC is also known as [ ]

A. Key hash function B. Keyed hash function

C. Message automatic function D. Method authentication function

5. In the case of the digital signature, the hash value of message is encrypted with a user's__key [ ]

A. Public B. Private C. Secret D. Common

6. Hash functions are commonly used to create a _____ [ ]

A. One time password B. One way password C. One time code D. One way code

7. For a hash value h=H(x) , we say that x is the _____ of h. [ ]

A. Preimage B. Postimage C. Collison D. Function

8. which among following are security requirements for Cryptographic Hash function [ ]

A. Variable output size B. Efficiency C. Post image resistant D. Fixed input size

9. A function that is collision resistant is also _____ resistant [ ]

A. Preimage resistant B. Second preimage resistant C. Both A & B D. None

10. SHA is referred as _____ [ ]

A. Security hash algorithm B. Secure hash algorithm

C. Secure has algorithm D. None

11. Any message authentication or digital signature mechanism has ___ levels of functionality. [ ]

A. 2 B. 3 C. 4 D. 5

12. Among the following which kind of attacks can be identified in the context of communication across a network. [ ]

A. Masquarade B. Disclosure C. Content repudiation D. Source modification

13. Denial of transmission of message by source is called _____ [ ]

A. Source repudiation B. Destination repudiation C. Sequence modification D. None

14. _____ is function in which ciphertext of the entire message serves as its authenticator. [ ]

A. Message encryption B. Message decryption C. Hash function D. None

15. The straightforward use of public-key encryption provides _____ [ ]

A. Authentication B. Protection C. Security D. Confidentiality

16. An authentication technique involves the use of a secret key to generate a small-fixed block of data known as _____ [ ]

A. Cryptographic checksum B. MAC C. Both A & B D. None

17. In the equation MAC = C(K,M) "K" is referred as _____ [ ]

A. Shared secret key B. Input message C. MAC function D. None

18. In general MAC function is _____ function. [ ]

A. One-to-one B. Many-to-one C. One-to-many D. None

19. We can group attacks on MACs into _____ categories. [ ]

A. 3 B. 2 C. 4 D. None

20. Which among is group of attacks on MAC [ ]

A. Cryptograph B. Cryptanalysis C. Brute-Force attacks D. Both C & D

21. An ideal MAC algorithm will require a cryptanalytic effort _____ the brute force attack [ ]

A. Greater than or equal to B. Less than or equal to C. Greater than D. Less than

22. DAA is referred as _____ [ ]

A. Data analysis algorithm B. Data authentication algorithm

C. Data authentic algorithm D. Data automate algorithm

23. DAA is widely adopted in _____ sectors [ ]

A. Government B. Industry C. Both A & B D. None

24. The CCM mode of operation was standardized to support the security requirements of [ ]

A. Computer networks B. WiFi wireless local area network

C. Local area networks D. None

25. The key algorithmic ingredients of CCM are the _____ [ ]

A. AES encryption algorithm B. The CPR mode of operation

C. The CNAC authentication D. None

26. Message authentication protects two parties who exchange message from _____ [ ]

A. Each other B. Any third party C. Both A & B D. None

27. _____ must verify author and the date and time of the signature. [ ]

A. Digital signature B. Data signature C. Data signal D. Digital signal

28. _____ must authenticate the contents at the time of the signature. [ ]

A. Digital signature B. Data signature C. Data signal D. Digital signal

29. The digital signature function includes the _____ function [ ]

A. Verification B. Authentication C. Security D. Checking

30. Which among the following are types attacks _____ [ ]

A. Known message attack B. Key-only attack

C. Directed chosen message attack D. All

31. Which among the following are types of forgeries _____ [ ]

A. Half break B. Universal forgery C. Essential forgery D. All

32. Digital signature must be relatively _____ to produce. [ ]

A. Difficult B. Complicated C. Easy D. Huge

33. The signature must be a _____ pattern that depends on the message being signed. [ ]

A. Byte B. Bit C. Bite D. Beat

33. Digital signature must be relatively _____ to recognize and verify the digital signature. [ ]

A. Easy B. Difficult C. Complicated D. Huge

34. The _____ encryption scheme involves the use of the private key for encryption and the public key for decryption. [ ]

A. Egammal B. Elgamal C. Elgammal D. Egammal

35. The schnorr signature scheme is based on _____ . [ ]

A. Discrete logarithms B. Discrete algorithms C.Discreate algorithms D.Discreate logarithms

36. The DSA makes use of the _____ algorithm [ ]

A. Secure Hash B. Discrete C. Brute-force D. None

37. NIST stands for _____ [ ]

A. National institute of science and technology B. National institute of standards and technology

C. National informal social terminal D. None

38. The DSA can be provide _____ [ ]

A. Digital signature B. Encryption C. Key exchange D. All

39. which among algorithms had high acceptance due to the efficiency advantage of elliptic curve cryptography. [ ]

A. ECDSA B. NIST DSA C. Both A & B D. RSA-PSS DSA

40. _____ must be verifiable by third parties to resolve disputes. [ ]

A. Data signals B. Data signature C. Data signs D. None

Unit-IV

1. The strength of any cryptographic system rests with the _____ [ ]

A. Key distribution technique B. Key distributed technique

C. Key developed technique D. None

2. _____ the term that refers to the means of delivering a key to two parties who wish to exchange data without allowing others to see the key. [ ]

A. Key distribution technique B. Key distributed technique

C. Key developed technique D. None

3. Communication between end systems is encrypted using a temporary key, often referred to as a _ key [ ]

A. Section B. Session C. Master D. None

4. Session keys are transmitted in encrypted form, using a _____ key [ ]

A. Other session key B. Travel key C. Master key D. None

5. A nonce minimum requirement is it _____ with each request [ ]

A. Differs B. Equals C. Compares D. None

6. _____ is a good choice for a nonce. [ ]

A. A random number B. A counter C. A time stamp D. All

7. The more frequently session keys are exchanged, the more _____ they are. [ ]

A. Risky B. Secure C. Complicate D. None

8. For connection oriented protocols, use _____ session key for each new session. [ ]

A. Same B. New C. Either A or B\ D. None

9. _____ key is used for general communication across a network [ ]

A. Data-encryption B. PIN-encryption C. File-encryption D. None

10. Which among the following is group scheme name of public keys? [ ]

A. Public announcement B. Publicly available directory

C. Public-key authority D. All

11. _____ scheme can be forged by any one [ ]

A. Public announcement B. Publicly available directory

C. Public-key authority D. All

12. A greater degree of security can be achieved by maintaining a _____ of public keys. [ ]

A) Public announcement B. Publicly available directory

C. Public-key authority D. All

13. Only the certificate authority can create and update certificates under _____ scheme. [ ]

A. Public key certificate B. Public key authority

C. Both A & B D. None

14. X.509 is part of the _____ series of recommendation that define a directory service. [ ]

A. X.500 B. X.600 C. X.700 D. X.800

15. X.509 defines alternative authentication protocols based on the use of ___key certificates. [ ]

A. Public B. Private C. Master D. None

16. X.509 is based on the use of public-key _____ . [ ]

A. Public key cryptography B. Digital signatures C. Both A & B D. Private key cryptography

17. Which among the following are elements of certificate format? [ ]

A. Version B. Serial Number C. Issuer Number D. Both A & B

18. The name of the user to whom this certificate refers is called as _____ name. [ ]

A. Title B. Subject C. Version D. User

19. In Public - key - infrastructure CA refers to _____ [ ]

A. Certificate authority B. Certificate author C. Chared accountant D. None of the above

20. _____ is a generic term used to denote any method for storing certificates and CRLs. [ ]

A. CRL issuer B. Repository C. CA D. RA

21. there are _____ general methods of authenticating a user's identity [ ]

A. 3 B. 5 C. 4 D. 1

22. General means of authenticating can be used _____ [ ]

A. Alone B. In combination C. Both A & B D. None

23. The simplest _____ attack is one in which the opponent simply copies a message and reply later. [ ]

A. React B. Counter C. Reply D. None

24. one application for which encryption is growing in popularity is _____ [ ]

A. e-mail B. Electric mail C. Both A & B D. None

25. Kerberos is an/a _____ service [ ]

A. Protection B. Security C. Authentication D. None

26. Among the following which are the requirements of kerberos _____ [ ]

A. Reliable B. Secure C. Scalable D. All

27. A full service kerberos environment consisting of a _____ [ ]

A. Server B. A number of clients C. A number of application servers D. All

28. Kerberos principal's name consists of _____ parts [ ]

A. 4 B. 3 C. 5 D. 2

29. Kerberos provides a mechanism for supporting _____ authentication. [ ]

A. Outer realm B. Inner Realm C. Both A & B D. None

30. Kerberos version 5 was developed to overcome issues of version 4 in _____ area(s). [ ]

A. Environmental short comings B. Environmental deficiencies

C. Technical deficiencies D. Both A & C

31. Services provided by a federated identity management system include _____ [ ]

A. Point of contract B. SSO Protocol server C. Authorization D. All

32. A principal is _____ holder [ ]

A. Information B. Command C. Program D. Identity

33. PGP provides a ____service that can be used for electronic mail and file storage applications. [ ]

A. Confidentiality B. Authentication C. Both A & B D. None

34. EP is notation for _____ [ ]

A. Public key encryption B. Private key encryption C. Both A & B D. None

35. || is notation for _____ in PGP [ ]

A. Concatenation B. Addition C. Or D. And

36. _____ cannot transmit executable file or other binary objects. [ ]

A. SMTP B. MIME C. S/MIME D. None

37. _____ is used to identity MIME entities uniquely in multiple contents [ ]

A. Content-ID B. Content-Name C. Entity-ID D. MIME-ID

38. S/MIME provides follwing funcions_____ [ ]

A. Envelope data B. Signed data C. Both A & B D. Unsigned data

39. S/MIME secures a MIME entity with a _____ [ ]

A. Signature B. Encryption C. Both A & B D. None

40. In S/MIME certificate processing A user's public key must be registered with a certificate authority in order to receive an _____ key certificate [ ]

A. X.507 public B. X.507 private C. X.509 public D. X.509 private

Unit-V

1. _____security provides end-to-end security services for applications [ ]

A. transport layer B. application layer C. network layer D. physical layer

2. SSL stands for_____ [ ]

A. server socket layer B. socket server layer C. socket server D. Secure Sockets layer

3. TLS stands for_____ [ ]

A. transport layer B. Transport Layer Security C. transport level security D. transport layer services

4. HTTP stands for _____ [ ]

A. hypo transfer text protocol B. hyper text transfer C. Hyper text transfer protocol D. Hyper text translates protocol

5. _____is designed by provide security and compression services to data generated from the application layer [ ]

A. SSL B. TCP C. ISP D. URL

6. SSL divides the data into blocks of 224 bytes [ ]

A. Framing B. Message integrity C. Fragmentation D. Compression

7. A leader is added to the encrypted payload [ ]

A. compression B. message integrity C. framing D. Framing

8. How many SSL protocols [ ]

A. 4 B. 1 C. 5 D. 6

9. SSC protocols are_____ [ ]

A. Handshake B. Alert C. Both A&B D. none

10._____ for reporting errors and abnormal conditions [ ]

A. Handshake protocol B. Record protocol C. Alert protocol D. none

11. A collections of protocols [ ]

A. transport layer B. IP Security C. session layer D. network security

12.IPSec has modes [ ]

A. transport mode B. tunnel mode C. Both A&B D. none

13. Transport mode protects the network layer payload [ ]

A. Tunnel mode B. transport mode C. all the above D. none

14. _____ is a very important aspect of IPSec [ ]

A. Security Association B. standard archive C. protocol D. danger

15. A set of SAs that can be collected into a database [ ]

A. security association B. Security Association Database C. security D. database

16.Host that is using the IPSec protocol needs to keep_____ [ ]

A. SP B. SA C. SAD D. SPD

17. _____is a protocol designed to create both inbound and outbound Security Associations [ ]

A. SP B. IKE C. SAD D. SPD

18)The _____protocol is designed to carry messages for the IKE exchange [ ]

A. SP B. SAD C. ISAKMP D. SPD

19. _____are actually designed to carry messages [ ]

A. proposal B. transform C. hash D. payloads

20. which one used for starting the negotiation [ ]

A. SA B. none C. Hash D. Delete

21._____ carriers one more SA that sender has deleted [ ]

A. SA B. none C. Delete D. hash

22.which is the one used to show the end of the layout [ ]

A. SA B. delete C. hash D. NONE

23._____carriers data generated by a hash function [ ]

A. SA B. Hash C. delete D. none

24.It defines vendor-specification extensions [ ]

A. SA B. hassh C. delete D. Vendor

25._____ initiates the mechanism of negotiation [ ]

A. SA payload B. proposal C. Proposal Payload D. payload

26.Payload is used to negotiate security parameters [ ]

A. SA payload B. proposal C. payload D. transform payload

27._____ actually carries attributes of the SA negotiation [ ]

A. SA Payload B. Transform payload C. proposal D. payload

28. It is used in those exchanges that need to send preliminary keys that are used for creating section keys [ ]

A. Key-Exchange payload B. SA payload C. transform payload D. payload

29._____ contains data generated by the hash function as described in the IKE changes [ ]

A. SA payload B. payload C. transform payload D. Hash payload

30._____ payload contains data generrated by applying the digital signature procedure over some part of the messages state [ ]

A. SA B. Signature C. transform D. hash

31.These programs on the other hand,cannot run independently [ ]

A. Logic bombs B. Spyware C. Viruses D. Trojans

32._____is a malicious program [ ]

A. Spyware B. viruses C. Trojans D. Logic Bombs

33.Logic bombs has typically two parts [ ]

A. payload B. trigger C. all the above D. none

34._____are malicious program that performs some harmless activities in addition to some malicious [ ]

A. payload B. Trojans C. trigger D. none

35._____ is a software to collect information from a computer and transmit it to another computer [ ]

A. Spyware B. payload C. trigger D. trojans

36._____have much similarity with spywares [ ]

A. payload B. Adwares C. trigger D. none

37.A _____ is a single point of defense between two networks [ ]

A. payload B. adwares C. trigger D. Firewall

38._____ is one of the foremost firewall technologies that analyze network traffic at the transport protocol layer [ ]

A. application layers B. Packet Filters C. firewalls D. circuit level firewalls

39.Services do not allow direct connection between the real service and the user [ ]

A. application layers B. packet filters C. Proxy D. trigger

40.An _____ may only detect and warm about security violations [ ]

A. IDS B. SP C. SPD D. SAD

OBJECTIVE - ANSWERS

Unit 1		Unit 2		Unit 3		Unit 4		Unit 5	
1	A	1	B	1	A	1	A	1	A
2	B	2	B	2	B	2	A	2	D
3	A	3	A	3	D	3	B	3	B
4	D	4	B	4	D	4	C	4	C
5	C	5	D	5	B	5	A	5	A
6	C	6	B	6	B	6	A	6	C
7	D	7	D	7	A	7	B	7	D
8	C	8	A	8	B	8	A	8	A
9	A	9	B	9	B	9	A	9	C
10	D	10	C	10	B	10	D	10	C
11	A	11	A	11	A	11	A	11	B
12	B	12	A	12	B	12	B	12	C
13	A	13	B	13	A	13	A	13	B
14	B	14	B	14	A	14	A	14	A
15	B	15	A	15	D	15	a	15	C
16	A	16	A	16	C	16	C	16	D
17	B	17	A	17	A	17	D	17	B
18	C	18	B	18	B	18	B	18	C
19	C	19	C	19	B	19	A	19	D
20	C	20	C	20	D	20	B	20	A
21	C	21	B	21	A	21	C	21	C
22	B	22	A	22	B	22	C	22	D
23	B	23	D	23	C	23	C	23	B
24	B	24	A	24	B	24	A	24	D
25	D	25	B	25	A	25	C	25	C
26	B	26	C	26	B	26	D	26	A
27	A	27	D	27	A	27	D	27	B
28	A	28	A	28	A	28	B	28	A
29	B	29	A	29	B	29	B	29	D
30	B	30	D	30	D	30	D	30	B
31	B	31	B	31	B	31	C	31	C
32	A	32	A	32	C	32	D	32	D
33	C	33	B	33	B	33	C	33	C
34	B	34	B	34	A	34	A	34	B
35	B	35	C	35	B	35	C	35	A
36	A	36	A	36	A	36	A	36	B
37	A	37	A	37	B	37	A	37	D
38	B	38	C	38	A	38	C	38	B
39	C	39	B	39	D	39	C	39	C
40	A	40	A	40	D	40	C	40	A

Prepared by: Mr. A.Dhasaradhi, Mr.P.Balaji,