**Chapter 8 – Cryptography Answers**

1. What is called a mathematical encryption operations that cannot be reversed?
   1. One-way hash
   2. DES
   3. Transposition
   4. Substitution
2. FIPS-140 is a standard for the security of which of the following?
   1. Cryptographic service providers
   2. Smartcards
   3. Hardware and software cryptographic modules
   4. Hardware security modules
3. Which of the following is NOT a property of a one-way hash function?
   1. It converts a message of a fixed length into a message digest of arbitrary length.
   2. It is computationally infeasible to construct two different messages with the same digest.
   3. It converts a message of arbitrary length into a message digest of a fixed length.
   4. Given a digest value, it is computationally infeasible to find the corresponding message.
4. Microsoft and Netscape offer two version of Web browser, export and domestic. Which of the following differentiates the versions?
   1. The browser for domestic market uses 40-bit encryption and the browser for international market uses 128-bit encryption.
   2. The browser for domestic market uses 128-bit encryption and the browser for international market uses 64-bit encryption.
   3. The browser for domestic market uses 128-bit encryption and the browser for international market uses 40-bit encryption.
   4. The browser for domestic market uses 64-bit encryption and the browser for international market uses 96-bit encryption.
5. Which of the following was developed in 1997 as a means of preventing fraud from occurring during electronic payments?
   1. Secure Electronic Transaction (SET)
   2. MONDEX
   3. Secure Shell (SSH-2)
   4. Secure Hypertext Transfer Protocol (S-HTTP)
6. "Strong" encryption means which of the following?
   1. using 16 or more rounds.
   2. using 64 or more rounds.
   3. a 64-bit or longer key.
   4. a 128-bit or longer key.
7. Which of the following is not an example of a block cipher?
   1. Skipjack
   2. IDEA
   3. Blowfish
   4. RC4
8. Which of the following statements is true about data encryption as a method of protecting data?
   1. It should sometimes be used for password files.
   2. It is usually easily administered.
   3. It makes few demands on system resources.
   4. It requires careful key management.
9. Cryptography does not concern itself with:
   1. Availability
   2. Integrity
   3. Confidentiality
   4. Authenticity
10. What is the maximum number of different keys that can be used when encrypting with Triple DES?
    1. 1
    2. 2
    3. 3
    4. 4
11. What is NOT true about a one-way hashing function?
    1. It provides authentication of the message
    2. It is never performed in reverse
    3. The results of a one-way hash is a message digest
    4. It provides integrity of the message
12. Which of the following services is not provided by the digital signature standard (DSS)?
    1. Encryption
    2. Integrity
    3. Digital signature
    4. Authentication
13. Which of the following is the most secure form of triple-DES encryption?
    1. DES-EDE3
    2. DES-EDE1
    3. DES-EEE4
    4. DES-EDE2
14. What algorithm was DES derived from?
    1. Twofish
    2. Skipjack
    3. Brooks-Aldeman
    4. Lucifer
15. In what way does the Rivest-Shamir-Adleman algorithm differ from the Data Encryption Standard?
    1. It is based on a symmetric algorithm.
    2. It uses a public key for encryption.
    3. It eliminates the need for a key-distribution center.
    4. It cannot produce a digital signature.
16. Which of the following is NOT a mode of the Data Encryption Standard (DES)?
    1. Electronic Code Book (ECB)
    2. Cipher Block Chaining (CBC)
    3. Substitution
    4. Output Feedback (OFB)
17. Kerberos depends upon what encryption method?
    1. Public Key cryptography
    2. Secret Key cryptography
    3. El Gamal cryptography
    4. Blowfish cryptography
18. The RSA Algorithm uses which mathematical concept as the basis of its encryption?
    1. Geometry
    2. Irrational numbers
    3. PI (3.14159...)
    4. Large prime numbers
19. What is the result of a hash algorithm being applied to a message ?
    1. A digital signature
    2. A ciphertext
    3. A message digest
    4. A plaintext
20. PGP uses which of the following to encrypt data?
    1. An asymmetric scheme
    2. A symmetric scheme
    3. A symmetric key distribution system
    4. An asymmetric key distribution
21. PKI is:
    1. An infrastructure for handling escrowed keys.
    2. More cheap to be built in-house that use 3rd-party certificates.
    3. responsible for: issuing, locating, trusting, renewing, revocating certificates.
    4. Private Key Infrastructure.
22. Which of the following is not related to a Public key infrastructure (PKI)?
    1. A Certificate authority
    2. A Ticket Granting Service
    3. A Registration authority
    4. A X.509 certificate
23. Which of the following can best be defined as a cryptanalysis technique in which the analyst tries to determine the key from knowledge of some plaintext-ciphertext pairs?
    1. A known-plaintext attack
    2. A known-algorithm attack
    3. A chosen-ciphertext attack
    4. A chosen-plaintext attack
24. Which of the following statements pertaining to link encryption is false?
    1. It encrypts all the data along a specific communication path.
    2. It provides protection against packet sniffers and eavesdroppers.
    3. Information stays encrypted from one end of its journey to the other.
    4. User information, header, trailers, addresses and routing data that are part of the packets are encrypted.
25. Which of the following is defined as a key establishment protocol based on the Diffie-Hellman algorithm proposed for IPsec but superseded by IKE?
    1. Diffie-Hellman Key Exchange Protocol
    2. Internet Security Association and Key Management Protocol (ISAKMP)
    3. Simple Key-management for Internet Protocols (SKIP)
    4. OAKLEY
26. What does the directive of the European Union on Electronic Signatures deal with?
    1. Encryption of classified data
    2. Encryption of secret data
    3. Non repudiation
    4. Authentication of web servers
27. What algorithm has been selected as the AES algorithm, replacing the DES algorithm?
    1. RC6
    2. Twofish
    3. Rijndael
    4. Blowfish
28. In a SSL session between a client and a server, who is responsible for generating the master secret that will be used as a seed to generate the symmetric keys that will be used during the session?
    1. Both client and server
    2. The client's browser
    3. The web server
    4. The merchant's Certificate Server
29. Which of the following ciphers is a subset of the Vignere polyalphabetic cipher?
    1. Caesar
    2. Jefferson
    3. Alberti
    4. SIGABA
30. What are the three most important functions that Digital Signatures perform?
    1. Integrity, Confidentiality and Authorization
    2. Integrity, Authentication and Nonrepudiation
    3. Authorization, Authentication and Nonrepudiation
    4. Authorization, Detection and Accountability
31. Secure Sockets Layer (SSL) provides security services at which layer of the OSI model?
    1. Network Layer
    2. Transport Layer
    3. Session Layer
    4. Application Layer
32. Which of the following encryption methods is unbreakable?
    1. Symmetric ciphers
    2. DES codebooks
    3. One-time pads
    4. Elliptic-curve cryptography
33. Which type of attack is most commonly associated with public key cryptosystems?
    1. Chosen-Ciphertext
    2. Ciphertext-only
    3. Chosen-Plaintext
    4. Adaptive-Chosen-Chipertext
34. Which of the following statements related to a private key cryptosystem is FALSE?
    1. The encryption key should be secure.
    2. Data Encryption Standard (DES) is a typical private key cryptosystem.
    3. The key used for decryption is known to the sender
    4. Two different keys are used for the encryption and decryption.
35. To comply with the Internet Engineering Task Force (IETF) standard for the IP Security (IPSEC) Protocol, which key-exchange method must be used?
    1. Internet Key Exchange (IKE)
    2. Internet Security Association and Key Management Protocol (ISAKMP)
    3. Diffie-Hellman
    4. none of the above
36. Which of the following are suitable protocols for securing VPN connections?
    1. S/MIME and SSH
    2. TLS and SSL
    3. IPsec and L2TP
    4. PKCS#10 and X.509
37. Why is public key cryptography recommended for use in the process of securing facsimiles during transmission?
    1. Keys are never transmitted over the network.
    2. Data compression decreases key change frequency.
    3. Key data is not recognizable from facsimile data.
    4. The key is securely passed to the receiving machine.
38. Which of the following would best define a digital envelope?
    1. A message that is encrypted and signed with a digital certificate.
    2. A message that is signed with a secret key and encrypted with the sender's private key.
    3. A message that is encrypted with a secret key and accompanied with that key, encrypted with a public key.
    4. A message that is encrypted with the recipient's public key and signed with the sender's private key.
39. Secure Sockets Layer (SSL) also uses a Message Authentication Code for:
    1. message non-repudiation.
    2. message confidentiality.
    3. message interleave checking.
    4. message integrity.
40. Which of the following is more suitable for a hardware implementation?
    1. Stream ciphers
    2. Block ciphers
    3. Cipher block chaining
    4. Electronic code book
41. Electronic signatures can prevent messages from being:
    1. Erased
    2. Disclosed
    3. Repudiated
    4. Forwarded
42. The Diffie-Hellman algorithm is primarily used to provide which of the following?
    1. Confidentiality
    2. Key exchange
    3. Integrity
    4. Non-repudiation
43. Which of the following encryption algorithms does not deal with discrete logarithms?
    1. El Gamal
    2. Diffie-Hellman
    3. RSA
    4. Elliptic Curve
44. Which type of attack is based on the probability of two different messages using the same hash function producing a common message digest?
    1. Differential cryptanalysis
    2. Differential linear cryptanalysis
    3. Birthday attack
    4. Statistical attack
45. Where parties do not have a shared secret and large quantities of sensitive information must be passed, the most efficient means of transferring information is to use a hybrid encryption technique. What does this mean?
    1. Use of public key encryption to secure a secret key, and message encryption using the secret key.
    2. Use of the recipient's public key for encryption and decryption based on the recipient's private key.
    3. Use of software encryption assisted by a hardware encryption accelerator.
    4. Use of elliptic curve encryption.
46. The Secure Hash Algorithm (SHA-1) creates:
    1. a fixed length message digest from a fixed length input message
    2. a variable length message digest from a variable length input message
    3. a fixed length message digest from a variable length input message
    4. a variable length message digest from a fixed length input message
47. Which of the following is not a DES mode of operation?
    1. Cipher block chaining
    2. Electronic code book
    3. Input feedback
    4. Cipher feedback
48. Which DES mode of operation is best suited for database encryption?
    1. Cipher Block Chaining (CBC) mode
    2. Cycling Redundancy Checking (CRC) mode
    3. Electronic Code Book (ECB) mode
    4. Cipher Feedback (CFB) mode
49. Which of the following keys has the shortest lifespan?
    1. Secret key
    2. Public key
    3. Session key
    4. Private key
50. Which of the following statements pertaining to message digests is incorrect?
    1. The original file cannot be created from the message digest.
    2. Two files should not have the same message digest.
    3. The message digest should be calculated using at least 128 bytes of the file.
    4. Messages digests are usually of fixed size.
51. Which of the following is not an encryption algorithm?
    1. Skipjack
    2. SHA-1
    3. Twofish
    4. DEA
52. Which of the following standards concerns digital certificates?
    1. X.400
    2. X.25
    3. X.509
    4. X.75
53. What can be defined as an instance of two different keys generating the same ciphertext from the same plaintext?
    1. Key collision
    2. Key clustering
    3. Hashing
    4. Ciphertext collision
54. What can be defined as secret communications where the very existence of the message is hidden?
    1. Clustering
    2. Steganography
    3. Cryptology
    4. Vernam cipher
55. What type of attack against confidentiality uses algorithm and algebraic manipulation weaknesses to reduce complexity?
    1. Brute force
    2. Statistical
    3. Analytic
    4. Codebook
56. What is the maximum key size for the RC5 algorithm?
    1. 128 bits
    2. 256 bits
    3. 1024 bits
    4. 2040 bits

1. Which of the following is not defined within the Wireless Application Protocol (WAP) protocol stack?
   1. Wireless Data Link Protocol (WDLP)
   2. Wireless Transaction Protocol (WTP)
   3. Wireless Session Protocol (WSP)
   4. Wireless Datagram Protocol (WDP)
2. What encryption algorithm is best suited for communication with handheld wireless devices?
   1. ECC
   2. RSA
   3. SHA
   4. RC4
3. Which of the following elements is not included in a Public Key Infrastructure (PKI)?
   1. Timestamping
   2. Lightweight Directory Access Protocol (LDAP)
   3. Certificate revocation
   4. Interne t Key Exchange (IKE)
4. What kind of certificate is used for user authentication?
   1. Public key certificate
   2. Attribute certificate
   3. Root certificate
   4. Codesigning certificate
5. Which DES modes can best be used for authentication?
   1. Cipher Block Chaining and Electronic Code Book
   2. Cipher Block Chaining and Output Feedback
   3. Cipher Block Chaining and Cipher Feedback
   4. Output Feedback and Electronic Code Book
6. SSL (Secure Sockets Layer) has two possible 'session key' lengths, what are they?
   1. 40 bit & 64 bit
   2. 40 bit & 128 bit
   3. 64 bit & 128 bit
   4. 128 bit & 256 bit
7. Simple Key Management for Internet Protocols (SKIP) is similar to Secure Sockets Layer (SSL), except that it requires no prior communication in order to establish or exchange keys on a session-by-session basis. Therefore, no connection setup overhead exists and new keys values:
   1. are continually generated.
   2. are not continually generated.
   3. are not continually granted.
   4. are continually granted.
8. What principle involves encryption keys being separated into two components, each of which does not reveal the other (covered in chapter 3)?
   1. Dual control
   2. Separation of duties
   3. Split knowledge
   4. Need to know
9. What is the role of IKE within the IPsec protocol?
   1. peer authentication and key exchange
   2. data encryption
   3. data signature
   4. enforcing quality of service
10. Which of the following statements pertaining to PPTP (Point-to-Point Tunnelling Protocol) is incorrect?
    1. PPTP is able to handle protocols other than IP.
    2. PPTP does not provide strong encryption.
    3. PPTP does not support any token-based authentication method for users.
    4. PPTP is derived from L2TP.
11. Public Key Infrastructure (PKI) is the use of asymmetric key encryption between parties in which the originator encrypts information using the intended recipient's "public" key. The recipients use their own "private" key to decrypt the information. The "Infrastructure" of this methodology assumes that:
    1. The sender and recipient have reached a mutual agreement on the encryption key exchange that they will use.
    2. The channels through which the information flows are secure.
    3. The recipient's identity can be positively assured to the sender.
    4. The sender of the message is the only other person with access to the recipient's private key.
12. What are two types of ciphers?
    1. Transposition and Permutation
    2. Transposition and Shift
    3. Transposition and Substitution
    4. Substitution and Replacement
13. Which of the following does not concern itself with key management?
    1. ISAKMP
    2. Diffie-Hellman
    3. Cryptology
    4. KEA
14. Which of the following is best provided by symmetric cryptography?
    1. Confidentiality
    2. Integrity
    3. Availability
    4. Non-repudiation
15. How long is a DES key sequence?
    1. 6 bytes
    2. 8 bytes
    3. 56-bits
    4. 128-bits
16. Which of the following is true about digital certificate?
    1. same as digital signature
    2. electrical credential proving that the certificate holder is who they said they are
    3. You can only get digital certificate from Verisign, RSA.
    4. Can't contain geography data.
17. Which of the following cryptographic attacks describes when the attacker has a copy of the plaintext corresponding to the ciphertext?
    1. known plaintext
    2. brute force
    3. ciphertext only
    4. chosen plaintext
18. How many rounds are used by DES?
    1. 16
    2. 32
    3. 64
    4. 48
19. Virus scanning and content filtering of encrypted e-mail is:
    1. not possible
    2. is only possible with key recovery scheme of all user keys
    3. is possible with several key management methods
    4. is possible only by "brute force"-decryption
20. What can be defined as a value computed with a cryptographic algorithm and appended to a data object in such a way that any recipient of the data can use the signature to verify the data's origin and integrity?
    1. A digital envelope
    2. A cryptographic hash
    3. A Message Authentication Code
    4. A digital signature
21. Which of the following offers security to wireless communications?
    1. S-WAP
    2. WTLS
    3. WSP
    4. WDP
22. Which of the following algorithms is used today for encryption in PGP?
    1. RSA
    2. IDEA
    3. Blowfish
    4. RC5
23. Which of the following was developed in order to protect against fraud in electronic fund transfers (EFT)?
    1. Secure Electronic Transaction (SET)
    2. Message Authentication Code (MAC)
    3. Cyclic Redundancy Check (CRC)
    4. Secure Hash Standard (SHS)
24. Which of the following techniques is used in the encryption of data between a web browser and server?
    1. SSL
    2. PGP
    3. IPSec
    4. Kerberos
25. Compared to RSA, which of the following is true of elliptic curve cryptography?
    1. It has been mathematically proved to be more secure.
    2. It has been mathematically proved to be less secure.
    3. It is believed to require longer key for equivalent security.
    4. It is believed to require shorter keys for equivalent security.
26. Which of the following is defined as an Internet, IPsec, key-establishment protocol, partly based on OAKLEY, that is intended for putting in place authenticated keying material for use with ISAKMP and for other security associations?
    1. IPsec Key exchange
    2. Security Association Authentication Protocol
    3. Simple Key-management for Internet Protocols
    4. Key Exchange Algorithm
27. There are parallels between the trust models in Kerberos and in PKI. When we compare them side by side, Kerberos tickets correspond most closely to which of the following?
    1. public keys
    2. private keys
    3. public-key certificates
    4. private-key certificates
28. Which of the following statements pertaining to block ciphers is incorrect?
    1. It operates on fixed-size blocks of plaintext.
    2. It is more suitable for software than hardware implementations.
    3. Plain text is encrypted with a public key and decrypted with a private key.
    4. Block ciphers can be operated as a stream.
29. What enables users to validate each other's certificate when they are certified under different certification hierarchies?
    1. Cross-certification
    2. Multiple certificates
    3. Redundant certification authorities
    4. Root certification authorities
30. What kind of encryption is realized in the S/MIME-standard?
    1. Asymmetric encryption scheme
    2. Password based encryption scheme
    3. Public key based, hybrid encryption scheme
    4. Elliptic curve based encryption

1. Which of the following statements pertaining to Secure Sockets Layer (SSL) is false?
   1. The SSL protocol was developed by Netscape to secure Internet client-server transactions.
   2. The SSL protocol's primary use is to authenticate the client to the server using public key cryptography and digital certificates.
   3. Web pages using the SSL protocol start with HTTPS.
   4. SSL can be used with applications such as Telnet, FTP and email protocols.
2. Which of the following would best describe a Concealment cipher?
   1. Permutation is used, meaning that letters are scrambled.
   2. Every X number of words within a text, is a part of the real message.
   3. Replaces bits, characters, or blocks of characters with different bits, characters or blocks.
   4. Hiding data in another message so that the very existence of the data is concealed.
3. Which of the following is \*NOT\* an asymmetric key algorithm?
   1. RSA
   2. Elliptic Curve Cryptosystem (ECC)
   3. El Gamal
   4. Data Encryption System (DES)
4. Which of the following would best describe certificate path validation?
   1. verification of the validity of all certificates of the certificate chain till the root certificate
   2. verification of the integrity of the associated root certificate
   3. verification of the integrity of the concerned private key
   4. verification of the revocation status of the concerned certificate
5. A public key algorithm that does both encryption and digital signature is which of the following?
   1. RSA
   2. DES
   3. IDEA
   4. DSS
6. Which of the following identifies the encryption algorithm selected by NIST for the new Advanced Encryption Standard?
   1. Twofish
   2. Serpent
   3. RC6
   4. Rijndael
7. How many bits is the effective length of the key of the Data Encryption Standard algorithm?
   1. 16
   2. 32
   3. 56
   4. 64
8. What is the primary role of smartcards in a PKI?
   1. Transparent renewal of user keys
   2. Easy distribution of the certificates between the users
   3. Fast hardware encryption of the raw data
   4. Tamperproof, mobile storage and application of private keys of the users
9. What is the main problem of the renewal of a root CA certificate?
   1. The required key recovery of all end user keys
   2. The authentic distribution of the new root CA certificate to all PKI participants
   3. The collection of the old root CA certificates from the users
   4. The issuance of the new root CA certificate
10. What is a characteristic of using the Electronic Code Book mode of DES encryption?
    1. A given block of plaintext and a given key will always produce the same ciphertext.
    2. Repetitive encryption obscures any repeated patterns that may have been present in the plaintext.
    3. Individual characters are encoded by combining output from earlier encryption routines with plaintext.
    4. The previous DES output is used as input.
11. Which of the following is an Internet IPsec protocol to negotiate, establish, modify, and delete security associations, and to exchange key generation and authentication data, independent of the details of any specific key generation technique, key establishment protocol, encryption algorithm, or authentication mechanism?
    1. OAKLEY
    2. Internet Security Association and Key Management Protocol (ISAKMP)
    3. Simple Key-management for Internet Protocols (SKIP)
    4. IPsec Key exchange (IKE)
12. What is called the substitution cipher that shifts the alphabet by 13 places?
    1. Cesar cipher
    2. Polyalphabetic cipher
    3. ROT13 cipher
    4. Transposition cipher
13. Which of the following binds a subject name to a public key value?
    1. A public-key certificate
    2. A public key infrastructure
    3. A Certificate Authority
    4. A private key
14. Which of the following best provides e-mail message authenticity and confidentiality?
    1. Signing the message using the sender's public key and encrypting the message using the receiver's private key
    2. Signing the message using the sender's private key and encrypting the message using the receiver's public key
    3. Signing the message using the receiver's private key and encrypting the message using the sender's public key
    4. Signing the message using the receiver's public key and encrypting the message using the sender's private key
15. In what type of attack does an attacker try, from several encrypted messages, to figure out the key used in the encryption process?
    1. Known-plaintext attack
    2. Ciphertext-only attack
    3. Chosen-Ciphertext attack
    4. Known-Ciphertext attack
16. The primary purpose for using one-way encryption of user passwords within a system is which of the following?
    1. It prevents an unauthorized person from trying multiple passwords in one logon attempt.
    2. It prevents an unauthorized person from reading or modifying the password list.
    3. It minimizes the amount of storage required for user passwords.
    4. It minimizes the amount of processing time used for encrypting passwords.
17. Which of the following mail standards relies on a "Web of Trust"?
    1. Secure Multipurpose Internet Mail Extensions (S/MIME)
    2. Pretty Good Privacy (PGP)
    3. MIME Object Security Services (MOSS)
    4. Privacy Enhanced Mail (PEM)
18. Which of the following can best be defined as a key distribution protocol that uses hybrid encryption to convey session keys that are used to encrypt data in IP packets?
    1. Internet Security Association and Key Management Protocol (ISAKMP)
    2. Simple Key-management for Internet Protocols (SKIP)
    3. Diffie-Hellman Key Distribution Protocol
    4. IPsec Key exchange (IKE)
19. What is NOT true with pre shared key authentication within IKE / IPsec protocol?
    1. pre shared key authentication is normally based on simple passwords
    2. needs a PKI to work
    3. Only one preshared key for all VPN connections is needed
    4. Costly key management on large user groups
20. Which of the following can be best defined as computing techniques for inseparably embedding unobtrusive marks or labels as bits in digital data and for detecting or extracting the marks later?
    1. Steganography
    2. Digital watermarking
    3. Digital enveloping
    4. Digital signature
21. Which of the following statements pertaining to stream ciphers is correct?
    1. A stream cipher is a type of asymmetric encryption algorithm.
    2. A stream cipher generates what is called a keystream.
    3. A stream cipher is slower than a block cipher.
    4. A stream cipher is not appropriate for hardware-based encryption.
22. The Diffie-Hellman algorithm is used for:
    1. Encryption
    2. Digital signature
    3. Key exchange
    4. Non-repudiation
23. Which of the following is not a known type of Message Authentication Code (MAC)?
    1. Hash function-based MAC
    2. Block cipher-based MAC
    3. Signature-based MAC
    4. Stream cipher-based MAC
24. What is the primary role of a PKI within the application domain?
    1. Key management of private and public keys
    2. Distribution of public keys to the users
    3. Issuance of attribute certificates
    4. Key exchange between peers
25. What is the length of an MD5 message digest?
    1. 128 bits
    2. 160 bits
    3. 256 bits
    4. varies depending upon the input
26. What is the key size of the International Data Encryption Algorithm (IDEA)?
    1. 64 bits
    2. 128 bits
    3. 160 bits
    4. 192 bits
27. Which of the following is true about Kerberos?
    1. It utilizes public key cryptography.
    2. It encrypts data after a ticket is granted, but passwords are exchanged in plain text.
    3. It depends upon symmetric ciphers.
    4. It is a second party authentication system.
28. In a known plaintext attack, the cryptanalyst has knowledge of which of the following?
    1. the ciphertext and the key
    2. the plaintext and the secret key
    3. both the plaintext and the associated ciphertext of several messages
    4. the plaintext and the algorithm
29. What is called the standard format that was established to set up and manage Security Associations (SA) on the Internet in IPSec?
    1. Internet Key Exchange
    2. Secure Key Exchange Mechanism
    3. Oakley
    4. Internet Security Association and Key Management Protocol
30. What is NOT an authentication method within IKE and IPsec?
    1. CHAP
    2. Pre shared key
    3. Certificate based authentication
    4. Public key authentication
31. Why does a digital signature contain a message digest?
    1. To detect any alteration of the message
    2. To indicate the encryption algorithm
    3. To confirm the identity of the sender
    4. To enable transmission in a digital format
32. What is used to bind a document to its creation at a particular time?
    1. Network Time Protocol (NTP)
    2. Digital Signature
    3. Digital Timestamp
    4. Certification Authority (CA)
33. Which of the following is not a property of the Rijndael block cipher algorithm?
    1. Resistance against all known attacks
    2. Design simplicity
    3. 512 bits maximum key size
    4. Code compactness on a wide variety of platforms
34. Which of the following is less likely to be used in creating a Virtual Private Network?
    1. L2TP
    2. PPTP
    3. IPSec
    4. L2F
35. In a Public Key Infrastructure, how are public keys published?
    1. They are sent via e-mail.
    2. Through digital certificates.
    3. They are sent by owners.
    4. They are not published.
36. In which phase of IKE protocol (IPsec) is peer authentication performed?
    1. Pre Initialization Phase
    2. Phase 1
    3. Phase 2
    4. No peer authentication performed
37. What uses a key of the same length as the message?
    1. Running key cipher
    2. One-time pad
    3. Steganography
    4. Cipher block chaining
38. What is the primary role of cross certification?
    1. Creating trust between different PKIs
    2. Build an overall PKI hierarchy
    3. set up direct trust to a second root CA
    4. Prevent the nullification of user certificates by CA certificate revocation
39. Which of the following is NOT true of SSL?
    1. By convention it uses 's-http://' instead of 'http://'.
    2. It stands for Secure Sockets Layer.
    3. It was developed by Netscape.
    4. It is used for transmitting private documents over the Internet.
40. Who vouches for the binding between the data items in a digital certificate?
    1. Registration authority
    2. Certification authority
    3. Issuing authority
    4. Vouching authority
41. Which of the following protocols provides non-repudiation in IPSec?
    1. Authentication Header (AH)
    2. Encapsulating Security Payload (ESP)
    3. Secure Sockets Layer (SSL)
    4. Secure Shell (SSH-2)
42. Which of the following is \*NOT\* a symmetric key algorithm?
    1. Blowfish
    2. Digital Signature Standard (DSS)
    3. Triple DES (3DES)
    4. RC5
43. The Data Encryption Algorithm performs how many rounds of substitution and permutation?
    1. 4
    2. 16
    3. 54
    4. 64
44. Which is NOT a suitable method for distributing certificate revocation information?
    1. CA revocation mailing list
    2. Delta CRL
    3. OCSP (online certificate status protocol)
    4. Distribution point CRL
45. Which of the following is best at defeating frequency analysis?
    1. Substitution cipher
    2. Polyalphabetic cipher
    3. Transposition cipher
    4. Steganography
46. Which of the following offers confidentiality to an e-mail message?
    1. The sender encrypting it with its private key.
    2. The sender encrypting it with its public key.
    3. The sender encrypting it with the receiver's public key.
    4. The sender encrypting it with the receiver's private key.
47. Which of the following statements is most accurate of digital signature?
    1. It is a method used to encrypt confidential data.
    2. It is the art of transferring handwritten signature to electronic media.
    3. It allows the recipient of data to prove the source and integrity of data.
    4. It can be used as a signature system and a cryptosystem.
48. Which of the following should be used as a replacement for Telnet for secure remote login over an insecure network?
    1. S-Telnet
    2. SSL
    3. Rlogin
    4. SSH