Date:21-11-2013

Module Name: PKI and Biometrics

Q. No. 1

Question: Which of the following is true about Public Key Infrastructure?

Answer Choices

A: PKI is a combination of digital certificates, public-key cryptography, and certificate authorities that provide enterprise wide security

B: PKI uses two-way symmetric key encryption with digital certificates, and Certificate Authority

C: PKI uses private and public keys but does not use digital certificates

D: PKI uses CHAP authentication

Q. No. 2

Question: 3DES (Triple Data Encryption Standard) is based on which of the following?

Answer Choices

A. Hashing algorithm B. Symmetric key-based algorithm

C. Asymmetric key-based algorithm D. None of these

Q. No. 3

Question: Which of the following can be used for secure exchange of email? [Choose 2 correct answers].

Answer Choices

A. HTTPS B. WEP C. S/MIME D. PGP

Q. No. 4

Question: Which of the following describes APIs for devices such as smartcards that contain other cryptographic information?

Answer Choices

A. PKCS #1 B. PKCS #5 C. PKCS #7 D. PKCS #11

Q. No. 5

Question. Which of the following is used for verifying whether a digital certificate is valid?

Answer Choices

A. PKCS#11 B. CRL C. S/MIME D. IPSec

Q. No. 6

Question You use mathematics to create a message digest, which is called

Answer Choices

a hashing algorithm. What do you use to encrypt this message

digest before transmission?

A. A Private key B. A Public key

C. Kerberos D. PKI

Q. No. 7

Question Which of the following applies to symmetric algorithms?

Answer Choices

A. Client and server keys are similar or shared
B. Client and server keys are dissimilar (private and public)
C. Even if a key is confiscated, symmetric algorithms are secure
D. Confidentiality is notan issue with symmetric algorithms

Q. No. 8

Question Which of the following uses symmetric encryption when

securing a Web site?

Answer Choices

A. RSA B. SSL C. ECC D. El Gamal

Q. No. 9

Question: Which of the following relates to stream cipher?

Answer Choices

A. Symmetric key B. Used for encryption

C. Asymmetric key D. Private key

Q. No. 10

Question: Rijndael is the basis for which of the following symmetric encryption algorithms?

Answer Choices

A. CAST B.ECC C. AES D.RC5

Q. No. 11

Question. Which of the following are known weaknesses of symmetric cryptography?

Answer Choices

A. Speed B. Limited security C. Scalability D. Key distribution

Q. No. 12

Question When using AES, or the Rijndael encryption algorithm, which of the following is the maximum allowable key size?

Answer Choices

A. 64 bits B. 128 bits C. 256 bits D.512 bits

Q. No. 13

Question Which of the following have key sizes of 128-bits, 192-bits, or 256-bits?

Answer Choices

A. DES B. 3DES C. MD5 D. AES

Q. No. 14

Question Your company wants to make use of a Public key algorithm that provides both encryption and is used as a digital signature. Which of the following meet these requirements?

Answer Choices

A. DES3 B. RSA C.DES D. IDEA

Q. No. 15

Question When dealing with network security, C.I.A. is an acronym that implies which of the following?

Answer Choices

A. Confidentiality, Integrity, and Availability
B. Confidentiality, Integrity, and Accountability
C. Certification, Integrity, and Authentication
D. Classified, Integrated, and Assessable

Q. No. 16

Question Which of the following is one of the primary reasons to use digital signatures in network operations?

Answer Choices

A. Digital signatures offer non-repudiation
B. Digital signatures maintain convenience
C. Digital signatures provide a code of ethics
D. Digital signatures support risk assessment

Q. No. 17

Question. Which of the following apply to PKI?

Answer Choices

A. Responsible for locating and issuing certificates
B. Responsible for trusting and renewing certificates
C. Responsible for revoking certificates
D. Stands for Private key infrastructure

Q. No. 18

Question You have a Certificate Authority (CA) that uses a Public key Infrastructure. How does the CA maintain network access?

(Select all that apply.)

Answer Choices

A. Through CRL B. Through ACL

C. Through OCSP D. Through PKI

Q. No. 19

Question. Which of the following types of cryptography is typically used to provide an integrity check?

Answer Choices

A. Public key B. Asymmetric C. Symmetric D. Hash

Q. No. 20

Question: What list does the Certificate Authority use when a Private key has become compromised?

Answer Choices

A. Expiration list B. Revocation list

C. Schindler's list D. Outdated list

Q. No. 21

Question. Which of the following is a standard for Information Security Management?

Answer Choices

A. ISO17799 B. X.509 C. X.400 D. PKCS #6

Q. No. 22

Question If a company thinks that a user's Private key has been compromised, what should it do?

Answer Choices

A. Turn the CA server on and off
B. Shut down the CA server
C. Revoke the person's key before expiration
D. Renew the person's key before expiration

Q. No. 23

Question You are reviewing the status of certificates and notice Mr. Brown has a Certificate Hold. What does this mean?

Answer Choices

A. Mr. Brown's key has been revoked
B. Mr. Brown's key has been suspended
C. Mr. Brown's key has expired
D. Mr. Brown's key has been recovered

Q. No. 24

Question The _____ attack can endanger the security of the Diffie-Hellman method if two parties are not authenticated to each other.

Answer Choices

A. Man-in-the-middle attack B. Ciphertext attack

C. Plaintext attack D. None of the above

Q. No. 25

Question. Which one of the following is a cryptographic protocol used to secure HTTP connection?

Answer Choices

A. stream control transmission protocol (SCTP)

B. transport layer security (TSL)

C. explicit congestion notification (ECN)

D. resource reservation protocol

Q. No. 26

Question ElGamal encryption system is

Answer Choices

A. symmetric key encryption algorithm

B. asymmetric key encryption algorithm

C. not an encryption algorithm

D. none of the mentioned

Q. No. 27

Question Cryptographic hash function takes an arbitrary block of data and returns

Answer Choices

A. fixed size bit string B. variable size bit string
C. both (a) and (b) D. none of the mentioned

Q. No. 28

Question. _____ is a collection of protocols designed by the IETF (Internet EngineeringTask Force) to provide security for a packet at the network level

Answer Choices

A. IPSec B.SSL C.PGP D. None of these

Q. No. 29

Question. In the _____ mode, IPSec protects information delivered from the transport layer to the network layer

Answer Choices

A. Transport B. Tunnel C. Either a or b D. None of these

Q. No. 30

Question Which of the following describes APIs for devices such as smartcards that contain other cryptographic information?

Answer Choices

A. PKCS #1 B. PKCS #5 C. PKCS #7 D.PKCS #11

Q. No. 31

Question In _____, there is a single path from the fully trusted authority to any certificate.

Answer Choices

A. X.509 B.PGP C.KDC D.none of these

Q. No. 32

Question In AES, the 16-byte key is expanded into_____

Answer Choices

A. 200 bytes B. 78 bytes C.176 bytes D.184 bytes

Q. No. 33

Question The _____ mode is normally used when we need host-to-host (end-to-end) protection of data.

Answer Choices

A. Transport B. tunnel C.either a or b D.none of these

Q. No. 34

Question _____ is a collection of protocols designed by the IETF (Internet Engineering Task Force) to provide security for a packet at the network level.

Answer Choices

A. IPSec B. SSL C.PGP D.None of these

Q. No. 35

Question IKE uses _____.
Answer Choices

A. Oakley B. SKEME C.ISAKMP D.all of the above

Q. No. 36

Question The combination of key exchange, hash, and encryption algorithms defines a _____ for each SSL session.

Answer Choices

A. List of protocols B. Cipher Suite
C. List of keys D.None of these

Q. No. 37

Question While creating digital envelope, we encrypt the _____with the ____.

Answer Choices

A. Sender's private key, one-time session key.
B. Receiver's public key, one-time session key.
C. one-time session key, sender's public key.
D. one-time session key, receiver's public key.

Q. No. 38

Question SSL works between _____and _____.

Answer Choices

A. Web browser, web server B. Web browser, application server
C. Web server, application server D. Application server, database server

Q. No. 39

Question Requesting for a certificate results into creation of a _____ file.

Answer Choices

A. PKCS#7 B. PKCS#9 C. PKCS#10 D. PKCS#12

Q. No. 40

Question Kerberos provides for _____.

Answer Choices

A. Encryption B. SSO C. remote login D. local login