Information Security

SET-4

By

BHARAT BHUSHAN @ B. K. NAL

Assistant Professor (Computer Science)

Director, BSTI, Kokar

&

SUPRIYA BHARATI

Assistant Professor (Computer Science)

Asst. Director, BSTI, Kokar

Buddha Science and Technical Institute (BSTI), Kokar

www.bharatsir.com

1. What is full form of DDoS?

A. derived denial of service
B. distributed denial of service
C. denial of service
D. none of these

2. Which One of them is Passive attack?

A. denial of service
B. modify message in
C. transit modify message in transit
D. obtain message contain

3. Protection against Denial by one of these parties in a communication refers to?

A. non-repudiation
B. data integrity
C. authentication
D. none of these

4. Prevention of the unauthorized used of Resources refers too?

A. data integrity
B. data confidentiality
C. access control
D. none of these

5. _____means knowledge obtained from investigation, study, intelligence new ,facts .

A. security
B. Data
C. Information
D. none of these

6. Security Measures Needed to protect _____ during their transmission.

A. File
B. Data
C. Packet
D. all of above

7. S/MIME is abbreviated as _____.

A. secure/multimedia internet mailing extensions
B. secure/multipurpose internet mailing extensions
C. secure/multimedia internet mail extensions
D. secure/multipurpose internet mail extensions

8. In SSL, what is used for authenticating a message?

A. mac (message access code)
B. mac (message authentication code)
C. mac (machine authentication code)
D. mac (machine access code)

9. What is the key size allowed in PGP?

A. 1024-1056
B. 1024-4056
C. 1024-4096
D. 1024-2048

10. PGP makes use of which cryptographic algorithm?

A. Des
B. Aes
C. Rsa
D. rabin

11. ISAKMP stands for _____.

A. internet system association and key management packet

B. internet security association and key management protocol
C. interchange system and key modeling protocol
D. internet security association and key modeling protocol

12. In _____, the cryptographic algorithms and secrets are sent with the message.

A. Ipsec
B. Ssl
C. Tls
D. pgp

13. In _____, there can be multiple paths from fully or partially trusted authorities.

A. x509
B. pgp
C. kdc
D. none of the above

14. _____ provides privacy, integrity, and authentication in e-mail.

A. Ipsec
B. Ssl
C. Pgp
D. none of the above

15. _____ uses the idea of certificate trust levels.

A. x509
B. pgp
C. kdc
D. none of the above

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

A. x509
B. pgp
C. kdc
D. none of the above

17. IKE uses _____.

A. Oakley
B. Skeme
C. isakmpall of the above
D. all of the above

18. SSL provides _____.

A. message integrity
B. confidentiality
C. compression
D. all of the above

19. IKE creates SAs for _____.

A. Ssl
B. Pgp
C. Ipsec
D. vp

20. PGP encrypts data by using a block cipher called _____.

A. international data encryption algorithm
B. private data encryption algorithm
C. internet data encryption algorithm
D. local data encryption algorithm

21. PGP encrypts data by using a block cipher called _____.

A. international data encryption algorithm
B. private data encryption algorithm
C. internet data encryption algorithm
D. local data encryption algorithm

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

A. man-in-the-middle
B. ciphertext attack
C. ciphertext attack
D. none of the above

23. He _____ method provides a one-time session key for two parties.

A. diffie-hellman
B. rsa
C. des
D. aes

24. One commonly used public-key cryptography method is the _____ algorithm.

A. Rss
B. Ras
C. Rsa
D. raa

25. What is the size of the RSA signature hash after the MD5 and SHA-1 processing?

A. 42 bytes
B. 32 bytes
C. 36 bytes
D. 48 bytes

ANSWER							
1.	B			B		21.	B
2.	D		12.	D		22.	A
3.	A		13.	B		23.	A
4.	C		14.	C		24.	C
5.	C		15.	B		25.	C
6.	B		16.	A			
7.	D		17.	D			
8.	B		18.	D			
9.	C		19.	C			
10.	C		20.	A			