Information Security

SET-5

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. The DSS signature uses which hash algorithm?

A. md5
B. sha-2
C. sha-1
D. does not use hash algorithm

2. The main difference in MACs and digital signatures is that, in digital signatures the hash value of the message is encrypted with a user's public key.

A. True
B. false

3. Message authentication code is also known as

A. key code
B. hash code
C. keyed hash function
D. message key hash function

4. When a hash function is used to provide message authentication, the hash function value is referred to as

A. message field
B. message digest
C. message score
D. message leap

5. ECC stands for

A. elliptic curve cryptography
B. enhanced curve cryptography
C. elliptic cone cryptography
D. eclipse curve cryptography

6. A digital signature needs ____ system

A. symmetric-key
B. asymmetric-key

C. either (a) or (b)
D. neither (a) nor (b)

7. Extensions to the X.509 certificates were added in version _____.

A. 1
B. 2
C. 3
D. 4

8. _____function creates a message digest out of a message.

A. Encryption
B. Decryption
C. Hash
D. none of the above

9. ECC encryption system is _____.

A. symmetric key encryption algorithm.
B. asymmetric key encryption algorithm
C. not an encryption algorithm
D. block cipher method

10. How many rounds does the AES-192 perform?

A. 10
B. 12
C. 14
D. 16

11. The procedure to add bits to the last block is termed as_____.

A. Decryption
B. Hashing
C. Tuning
D. padding

12. Conventional cryptography is also known as _____ or symmetric-key encryption.

A. secret-key
B. public key
C. protected key
D. primary key

13. Cryptographic algorithms are based on mathematical algorithms where these algorithms use _____ for a secure transformation of data.

A. secret key
B. external programs
C. add-ons
D. secondary key

14. _____ is a means of storing & transmitting information in a specific format so that only those for whom it is planned can understand or process it.

A. malware analysis
B. cryptography
C. reverse engineering
D. exploit writing

15. _____ is the process or mechanism used for converting ordinary plain text into garbled non- human readable text & vice-versa.

A. malware analysis
B. exploit writing
C. reverse engineering
D. cryptography

16. In asymmetric key cryptography, the two keys e and d, have special relationship to

A. Others
B. Data
C. Keys
D. each other

17. A asymmetric-key (or public key) cipher uses

A. 1 key
B. 2 key
C. 3 key
D. 4 key

18. What is data encryption standard (DES)?

A. block cipher
B. stream cipher
C. bit cipher
D. byte cipher

19. In cryptography, the order of the letters in a message is rearranged by_____.

A. transpositional ciphers
B. substitution ciphers
C. both transpositional ciphers and substitution ciphers
D. quadratic ciphers

20. Which one of the following algorithm is not used in asymmetric-key cryptography?

A. rsa algorithm
B. diffie-hellman algorithm
C. electronic code book algorithm
D. dsa algorithm

21. In asymmetric key cryptography, the private key is kept by_____

A. Sender
B. Receiver
C. sender and receiver
D. all the connected devices to the network

22. In cryptography, what is cipher?

A. algorithm for performing encryption and decryption
B. encrypted message
C. both algorithm for performing encryption and decryption and encrypted message
D. decrypted message

23. Which is the largest disadvantage of the symmetric Encryption?

A. more complex and therefore more time-consuming calculations.
B. problem of the secure transmission of the secret key.
C. less secure encryption function.
D. isn\t used any more.

24. Which of the following Algorithms not belong to symmetric encryption.

A. 3des (tripledes)
B. Rsa
C. rc5
D. idea

25. What type of attack uses a fraudulent server with a relay address?

A. Ntlm
B. Mitm
C. Netbios
D. smb

ANSWER						
1.	C		11.	D	21.	B
2.	B		12.	A	22.	A
3.	B		13.	A	23.	B
4.	D		14.	B	24.	B
5.	A		15.	D	25.	B
6.	B		16.	D		
7.	C		17.	B		
8.	C		18.	A		
9.	B		19.	A		
10.	B		20.	C		

Information Security with Bharat Sir, BSTI, Kokar, Ranchi