University of Mumbai Examination June 2021 Examination: 9th June 2021 Program: Computer Engineering Curriculum Scheme: Rev2016 Examination: TE Semester VI Course Code: CSC604 Course Name: CSS Time:1Hour20Minutes Max. Marks: 40(Descriptive)

Total points 36/40

TE Comp

Email *

mailofvivekanand@gmail.com

Name of Student

Vivekanand Kumar

Seat Number

2162023

✓ 1. _____ defines a security service as a service that is provided by a protocol layer of communicating open systems and that ensures adequate security of the systems or of data transfers. 2/2

- (●) X.800 ✓
- ( ) X.809
- ( ) X.832
- ( ) X.802

✓ 2._____are fundamental to a number of public-key algorithms, including and the digital signature algorithm (DSA). 2/2

- (●) Discrete logarithms ✓
- ( ) Chinese remainder theorem
- ( ) Fermat's theorem
- ( ) Miller and Rabin algorithm

✓ 3. Plain text message is: "meet me after the toga party" with a rail fence of depth 2. Compute cipher text. 2/2

- (●) MEMATRHTGPRYETEFETEOAAT ✓
- ( ) MEMATRHTGPRYETEFETFOAAT
- ( ) MEMATRHTHPRYETEFETEOAAT
- ( ) MEMATRHTGPRYETEFFTEOAOT

✓ 4. In_____ mode, the same plaintext value will always result in the same cipher text value. 2/2

- ○ Cipher Block Chaining
- ○ Cipher Feedback
- ◉ Electronic code book ✓
- ○ Output Feedback

✓ 5. DES encrypting the plaintext as block of _____ bits. 2/2

- ◉ 64 ✓
- ○ 56
- ○ 128
- ○ 32

✓ 6. _____ is a symmetric block cipher that is intended to replace DES as the approved standard for a wide range of applications. 2/2

- ◉ AES ✓
- ○ RSA
- ○ MD5
- ○ RC5

✓ 7. The number of rounds in RC5 can range from 0 to _____ 2/2

- 127
- 63
- 31
- 255 ✓

✓ 8. How many rounds does the AES-192 perform? 2/2

- 10
- 14
- 16
- 12 ✓

✓ 9. For the Knapsack: {1 6 8 15 24}, Find the cipher text value for the plain text 10011. 2/2

- 40 ✓
- 15
- 14
- 39

✗ 10. Which of the following is not possible through hash value? 0/2

- ○ Password check
- ○ Data integrity check
- ◉ Data retrieval ✗
- ○ Digital signature

✓ 11. Which of the following is not an element/field of the X.509 certificates? 2/2

- ○ Issuer Name
- ◉ Serial Modifier ✓
- ○ Issue unique identifier
- ○ Signature

✓ 12. _____ is responsible for distributing keys to pairs of users (hosts, processes, applications) as needed 2/2

- ◉ Key distribution center ✓
- ○ Key analysis center
- ○ UKey storing center
- ○ HKey storing center

✓ 13. A digital certificate system is _____. 2/2

- (●) uses third-party CAs to validate a user's identity ✓
- ( ) uses digital signatures to validate a user's identity
- ( ) uses tokens to validate a user's identity
- ( ) are used primarily by individuals for personal correspondence

✓ 14. Hashed message is signed by a sender using 2/2

- ( ) His public key
- (●) His private key ✓
- ( ) Receivers public key
- ( ) Receivers private key

✓ 15. The man-in-the-middle attack can endanger the security of the Diffie-Hellman method if two parties are not 2/2

- (●) Authenticated ✓
- ( ) Joined
- ( ) Submit
- ( ) Separate

✗ 16. Which of the following does authorization aim to accomplish?. 0/2

- ○ Restrict what operations/data the user can access
- ○ Determine if the user is an attacker
- ○ Flag the user if he/she misbehaves
- ◉ Determine who the user is ✗

✓ 17. _____ operates in the transport mode or the tunnel mode. 2/2

- ◉ IPSec ✓
- ○ SSL
- ○ PGP
- ○ BGP

✓ 18. When a hash function is used to provide message authentication, the hash function value is referred to as 2/2

- ○ Message Field
- ◉ Message Digest ✓
- ○ Message Score
- ○ Message Leap

✓ 19. Which of the following tool would NOT be useful in figuring out what spyware or viruses could be installed on a client's computer? 2/2

- (●) Wireshark ✓
- ( ) Malware Bytes
- ( ) HighjackThis
- ( ) HitmanPro

✓ 20. What is honey pot attack? 2/2

- (●) dummy device put into the network to attract attackers ✓
- ( ) single line threat
- ( ) Ip spoofing bypass
- ( ) recognition attack