UNIVERSITY OF MINES AND TECHNOLOGY, TARKWA

SECOND SEMESTER EXAMINATIONS, MAY 2018

COURSE NO: CE 372
COURSE NAME: **INFORMATION SECURITY**
CLASS: III TIME: 3hrs

Name**:** _____Index Number: _____

Carefully read all questions in section A and Circle your answers. Answer any other two questions in section B

1. Which of the following describes the first step in establishing an encrypted session using a Data Encryption Standard (DES) key?
   a. Key clustering
   b. Key compression
   c. Key signing
   d. Key exchange
2. In a typical information security program, what is the primary responsibility of information (data) owner?
   a. Ensure the validity and accuracy of data
   b. Determine the information sensitivity or classification level
   c. Monitor and audit system users
   d. Ensure availability of data.
3. What type of cryptanalytic attack where an adversary has the least amount of information to work with?
   a. Known-plaintext
   b. Ciphertext-only
   c. Plaintext-only
   d. Chosen-ciphertext
4. Which of the following is the most effective method for reducing security risks associated with building entrances?
   a. Minimize the number of entrances
   b. Use solid metal doors and frames
   c. Brightly illuminate the entrances
   d. Install tamperproof hinges and glass
5. A type cryptographic attack where it is based on the probability of two different messages using the same hash function to produce the same message digest is?
   a. Birthday attack
   b. Statistic attack
   c. Differential cryptanalysis attack
   d. Known ciphertext attack
6. Which of the followings is an example of simple substitution algorithm?

a. Rivest, Shamir, Adleman (RSA)
b. Data Encryption Standard (DES)
c. Caesar cipher
d. Blowfish

7. Which of the following refers to a series of characters used to verify a user's identity?
   a. Token serial number
   b. User ID
   c. Password
   d. Security ticket
8. A hacker gains access to a webserver and can view a file on the server containing credit card numbers. Which principle of the credit card file is violated?
   a. Availability
   b. Confidentiality
   c. Integrity
   d. Non Repudiation
9. Which of the following virus types changes its characteristics as it spreads?
   a. Boot sector
   b. Parasitic
   c. Stealth
   d. Polymorphic
10. The three primary methods for authenticating users to a system or network are…
    a. passwords, tokens, and biometrics
    b. authorization, identification, and tokens
    c. passwords, encryption, and identification
    d. identification, encryption, and authorization
11. Which of the following is not a symmetric key algorithm?
    a. RC4.
    b. Blowfish
    c. DES.
    d. RSA.
12. Which of the following feature does a digital signature provide?
    a. It provides the ability to encrypt an individual's confidential data
    b. It ensures an individual's privacy
    c. It identifies the source and verifies the integrity of data
    d. It provides a framework for law and procedures
13. Computer security is generally considered to be the responsibility of…?
    a. everyone in the organization
    b. corporate management
    c. the corporate security staff
    d. everyone with computer access
14. The practice of embedding a message in a document, image, video or sound recording so that its very existence is hidden is called?
    a. Anonymity.
    b. Steganography
    c. Shielding
    d. Data diddling

15. Cipher that scrambles letters into different positions is referred to as what?
    a. Substitution
    b. Stream
    c. Running key
    d. Transposition
16. What type of malware is self-contained and it does not need to be part of another computer program to propagate?
    a. Computer virus
    b. Trojan house
    c. Computer worm
    d. Polymorphic virus
17. A timely review of system access records would be an example of which basic security function?
    a. Avoidance
    b. Deterrence
    c. Prevention
    d. Detection
18. Which of the following does a Non-repudiation provide?
    a. It provides the ability to encrypt an individual's confidential data
    b. It ensures sources of messages are not denied
    c. It identifies the source and verifies the integrity of data.
    d. It provides a framework for law and procedure
19. What role does biometrics have in logical access control?
    a. Certification
    b. Authorization
    c. Authentication
    d. Confirmation
20. What best describes two-factor authentication?
    a. Something you know
    b. Something you have
    c. Something you are
    d. A combination of two listed above
21. Risk management helps you do all of the followings except
    a. Identify risks
    b. Assess risks
    c. Reduce risk to an acceptable level
    d. Completely avoid risk
22. What is an example of a human threat?
    a. Lightning strike
    b. Fire
    c. Phishing
    d. All of the above
23. Cryptography does not concern itself with
    a. Availability
    b. Authenticity
    c. Integrity
    d. Confidentiality

24. The art of making an information unintelligent to whoever comes across is called

a. Decryption
b. Encryption
c. Steganography
d. Cryptography

25. Hackers are unethical people who

a. Access databases that they have no right to be in
b. Create programs intending to destroy other computer systems
c. Do not respect the rights or privacy of others
d. All of the above

26. Ethics are

a. Official rules
b. Personal beliefs
c. Moral principles
d. Community guidelines

27. Ethical responsibilities of IT professionals include

a. concern for persons other than clients
b. minimizing cost
c. maximizing profit
d. maximizing profit

28. Ray got a text message from Keith saying that if he tries to join the soccer team, he will tell everyone that he still sleeps with a teddy bear at night. What type of cyberbullying is this?

a. Gossip
b. Threat
c. Exclusion
d. Impersonation

29. When an employee transfers within an organization …

a. The employee must undergo a new security review
b. The old system IDs must be disabled
c. All access permission should be reviewed
d. The employee must turn in all access devices

30. What is 'establishing whether someone's identity is correct' called?

a. Authentication
b. Authorization
c. Identification
d. None of the above

SECTION B.

1a. Define the following

i. Computer Security
ii. Computer Network Security
iii. Information Security

b. What is the difference between passive and active security threats? Hence, list and briefly define categories of passive and active security attacks.

c. What is the difference between a block cipher and a stream cipher? Using Caesar Cipher and a key of 5. Encrypt a message "UMAT is the best University in Ghana" to a friend

2a. Discuss any three types of Virus. Hence, differentiate between a Computer Virus and Worm

b. State the Ten Commandments of Computer Ethics

c.. What is a Firewall? Give a brief classification of Firewall.

3a. Perform encryption and decryption using the RSA algorithm as taught in the class, for the following:

i. $p = 3$; $q = 11$, $e = 7$; $M = 5$

ii. $p = 5$; $q = 11$, $e = 3$; $M = 9$

iii. $p = 7$; $q = 11$, $e = 17$; $M = 8$

iv. $p = 11$; $q = 13$, $e = 11$; $M = 7$

v. $p = 17$; $q = 31$, $e = 7$; $M = 2$.

.

b. Explain the difference between fabrication and modification attacks.

C. When shopping at Costco, after you have selected your purchases you take your cart full of goods to one of the registers. The check-out clerk scans your goods, totals what you owe, and upon receiving payment from you gives you an itemized receipt. However, you cannot then simply exit the building with your goods. At the exit you are required to go by a staff member who inspects your receipt. If the receipt looks okay (appears to match the number

and types of items in your cart), the staff member draws a line with a permanent marker down the receipt and hands it back to you. At this point, you can exit the building and take the goods to your car. Identify two security principles illustrated by Costco's approach. For each, describe in a single sentence what aspect of Costco's approach reflects the principle.

Examiner: Prof B. K. Alese