Unit Test | Data: Security and Encryption

Fill in the blank:

1. Convert the following ASCII values to a word without extra spaces (**66 65 78 71**)
   _____.
2. 348 mod 201 = _____
3. 71048 mod 3483555 = _____
4. 24985729 mod 2 = _____
5. 473747542 mod 2 = _____

Multiple Choice

6. A(n) _____ is the generic term for a technique that performs encryption.
   a. Cipher
   b. Encrypter
   c. Key
   d. Decoder
   e. Algorithm

7. The process of encoding messages to keep them secret is known as _____.
   a. Encryption
   b. Decryption
   c. Ciphering
   d. Keying
   e. Steganography

8. A problem that is _____ is a difficult problem for a computer to solve in a reasonable amount of time.
   a. Computationally hard
   b. Complex
   c. Prime
   d. Heuristic
   e. Locked

9. _____ (or clock arithmetic) is a mathematical operation that returns the remainder after integer division.
    a. Modulus
    b. Remaindering
    c. Discrete Cosine
    d. Integer Division
    e. Tic toc

10. _____ Key encryption uses asymmetric encryption and allows for secure messages to be sent without having to agree on a secret key.
    a. Public-Private
    b. Secret
    c. Double
    d. Hidden
    e. Shared

11. When someone tries to get you to give up personal information through email or a bogus website it is called a(n) _____ scam.
    a. Phishing
    b. DDoS
    c. Spamming
    d. Trojan Horse
    e. Worm

12. When someone attempts to compromise a target by flooding it with requests from multiple systems it is called a(n) _____ attack.
    a. DDoS
    b. Phishing
    c. Trojan Horse
    d. Spamming
    e. Noah's Ark

13. The German machine that was used to encrypt secret messages during WWII was called _____.
    a. Enigma Machine

b. Bombe Machine
c. Turing Machine
d. Hitler Machine
e. Bletchley Park Machine

14. The _____ is a technique for encryption that shifts the alphabet by some number of characters.
    a. Caesar Cipher
    b. Diffie-Hellman
    c. Vigenere Cipher
    d. Random substitution cipher
    e. RSA Algorithm
    f. Asymmetric Encryption

15. _____ is the public key cryptosystem that can used only for key exchange (like mixing paint).
    a. Caesar Cipher
    b. Diffie-Hellman
    c. Vigenere Cipher
    d. Random substitution cipher
    e. RSA Algorithm
    f. Asymmetric Encryption

16. The _____ is an encryption technique that maps each letter of the alphabet to randomly chosen other letters of the alphabet.
    a. Caesar Cipher
    b. Diffie-Hellman
    c. Vigenere Cipher
    d. Random substitution cipher
    e. RSA Algorithm
    f. Asymmetric Encryption

17. Which encryption technique involves shifting the alphabet differently per character in the key?
    a. Caesar Cipher
    b. Diffie-Hellman
    c. Vigenere Cipher
    d. Random substitution cipher
    e. RSA Algorithm
    f. Asymmetric Encryption
18. Which of these is a reason why asymmetric encryption is useful?
    a. It allows for people who haven't agreed in advance on a key to build one without having to share it in secret.
    b. It allows both sender and receiver to use the same shared key.
    c. It allows the receiver to decrypt messages using only the public key.
    d. It allows the sender and receiver to share their private keys.
19. What type of math is used in public key encryption that makes it so hard to reverse?
    a. One-way functions
    b. Two-way Functions
    c. Polynomials Functions
    d. Linear Functions
20. Fill in the blank of the following statement: "_____ encryption is a method of encryption involving one key for both encryption and decryption."
    a. Symmetric
    b. Asymmetric
    c. Public Key
    d. SSL
21. A coffee shop is considering accepting orders and payments through their phone app and have decided to use public key encryption to encrypt their customers' credit card information. Is this a secure form of payment
    a. Yes, public key encryption is built upon computationally hard problems that even powerful computers cannot easily solve.
    b. No, public key encryption allows the credit card information to be read by the public.
    c. No, the internet protocols are open standards and thus everything sent over the internet is sent "in the clear".
    d. Yes, public key encryption is secure because it transmits credit card information in binary.

22. Which of the following statements best describes the properties of public key encryption?
    a. Public key encryption is an encryption method which relies on separate keys for encrypting and decrypting information.
    b. Public key encryption is a highly secure encryption scheme that in which a single shared key is used by both the sender and receiver of the message.
    c. Public key encryption makes use of certain types of problems which are easier for humans to solve than computers.
    d. Public key encryption makes use of mathematical problems which no algorithm can be used to solve.
23. Choose the answer that is NOT a feature of Public Key Cryptography:
    a. A Public Key database ensures 3rd party is accountable for the security of the communication
    b. Using public key guarantees that only the intended recipient can decrypt the message
    c. A key for decrypting is never made public
    d. Allows secure communication without establishing a *shared* encryption key ahead of time.
24. What is a Distributed Denial of Service (DDoS) attack?
    a. An attempt to compromise a single target by flooding it with requests from multiple systems.
    b. A coordinated effort by a group to simultaneously attempt to gain entry to foreign government's servers or systems
    c. An effort by network engineers to focus all systems on catching a user or computer that has illegally gained access.
    d. An attempt to harass or extort all customers of one or more Internet Service Providers (ISPs).
25. Which of the following scenarios is most characteristic of a phishing attack?
    a. You get an email from the IT support desk that asks you to send a reply email with your username and password to verify your account
    b. You accidentally run a piece of code that automatically spreads from one computer to another, exploiting a common vulnerability
    c. You get an unwanted email trying to sell you a low-quality product or service that seems "fishy."
    d. You accidentally install a piece of software that monitors your activity to steal personal information like your passwords, date of birth, social security number, etc.

26. Which of the following are true statements about digital certificates in Web browsers?
    a. Digital certificates are used to verify the ownership of encrypted keys used in secured communication
    b. Digital certificates are used to verify that the connection to a website is fault tolerant.
    c. Digital certificates are used to block viruses.
    d. Digital certificates are issued by the government.

Matching

A. **Trapdoor**
B. **Botnet**
C. **Virus**
D. **Worm**
E. **Trojan Horse**
F. **Logic Bomb**

27. Which type of malware provides a secret entry to a program or system for the attacker?
28. Which type of malware executes a malicious code whenever a condition is met?
29. Which type of malware is presented as a useful functioning program, by has malicious code embedded in it from when it was originally created?
30. Which type of malware spreads itself by embedding its malicious code into the body of other useful programs?
31. This type of malware can be used to perform a Distributed Denial of Service (DDos) attack.
32. This type of malware does not need a host program and spreads over entire networks

Multiple Response | pick all that apply

33. Which of the following types of malware reproduce and spread themselves to other files and computers?
    a. Trap doors
    b. Viruses
    c. Logic Bombs
    d. Botnet
    e. Trojan Horses
    f. Worms

Matching

A. **encryption**
B. **public key**
C. **decryption**
D. **Brute forcing**
E. **symmetric encryption**
F. **cipher**
G. **asymmetric encryption**

34. a process that reverses a secret message and reproduces the original plain text
35. a process of encoding messages to keep them secret, so only "authorized" parties can read it
36. the generic term for a technique (or algorithm) that performs encryption
37. an attempt to forcibly decode a secret message without knowing the specifics of the cipher
38. the key that is used to decrypt information in asymmetric encryption
39. used prevalently on the web, it allows for secure messages to be sent between parties without having to agree on, or share, a secret key
40. an encryption process where both parties agree to use a single shared key to encrypt and decrypt data