1. Which of the following is not a one-way algorithm?
   a. RC2
   b. DSA
   c. MD2
   d. SHA-1

2. Of the following, which uses a key of the same length as the message?
   a. Running key cipher
   b. Cipher block chaining
   c. Steganography
   d. One-time pad

3. In what type of attack does an attacker try, with only several encrypted messages, to figure out the key used in the encryption process?
   a. Known-Ciphertext attack
   b. Chosen-Ciphertext attack
   c. Ciphertext-only attack
   d. Known-plaintext attack

4 Cryptography does NOT help in:
   a. Detecting fraudulent insertion.
   b. Detecting fraudulent disclosure.
   c. Detecting fraudulent deletion.
   d. Detecting fraudulent modification.

5. What is the RESULT of a hash algorithm being applied to a message?
   a. A ciphertext
   b. A message digest
   c. A plaintext
   d. A digital signature

6. Which of the following statements pertaining to key management is incorrect?
   a. Keys should be backed up or escrowed in case of emergencies.
   b. A key's lifetime should correspond with the sensitivity of the data it is protecting.
   c. When not using the full keyspace, the key should be extremely random.
   d. The more a key is used, the shorter its lifetime should be.

7. Which of the following issues is not addressed by digital signatures?
   a. confidentiality
   b. authentication
   c. data integrity
   d. nonrepudiation

8. How many bits is the effective length of the key of the Data Encryption Standard algorithm?
    a. 168
    b. 68
    c. 56
    d. 128

9. Of the asymmetric algorithms, which algorithm is considered to have the highest strength per bit of key length?
    a. Elliptic Curve Cryptography (ECC)
    b. Rivest, Shamir, Adleman (RSA)
    c. Advanced Encryption Standard (AES)
    d. El Gamal

10. Which of the following is *NOT* a symmetric key algorithm?
    a. Triple DES (3DES)
    b. RC5
    c. Digital Signature Standard (DSS)
    d. Blowfish

11. The Data Encryption Algorithm performs how many rounds of substitution and permutation?
    a. 16
    b. 4
    c. 54
    d. 64

12. Of the following, which is an operation that can not be reversed?
    a. DES
    b. Substitution
    c. One-way hash
    d. Transposition

13. Which of the following is true about a digital certificate?
    a. Electronic credential proving that the certificate holder is who they claim to be
    b. It is the same as digital signature
    c. Can't contain geography data.
    d. Can only be gotten from Verisign or RSA.

14. Electronic signatures can PREVENT messages from being:
    a. Erased
    b. Disclosed
    c. Repudiated
    d. Forwarded

15. Which of the following statements pertaining to message digests is incorrect?
    a. Messages digests are usually of fixed size.
    b. The original file cannot be created from the message digest.
    c. Two files should not have the same message digest.
    d. The message digest should be calculated using at least 128 bytes of the file.

16. Which of the following statements concerning digital signatures is most accurate?
    a. It is the art of transferring handwritten signature to electronic media.
    b. It is a method used to encrypt confidential data.
    c. It allows the recipient of data to prove the source and integrity of data.
    d. It can be used as a signature system and a cryptosystem.

17. Which of the following binds a subject name to a public key value?
    a. A private key
    b. A Certificate Authority
    c. A public key infrastructure
    d. A public-key certificate

18. Which of the following is best provided by symmetric cryptography?
    a. Confidentiality
    b. Availability
    c. Non-repudiation
    d. Integrity

19. What can be defined as a value computed with a cryptographic algorithm and appended to a data object in such a way that any recipient of the data can use the that data to verify the data's origin and integrity?
    a. A digital envelope
    b. A cryptographic hash
    c. A Message Authentication Code
    d. A digital signature

20. For what is the Diffie-Hellman algorithm used?
    a. Encryption
    b. Key exchange
    c. Digital signature
    d. Non-repudiation

21. What type of encryption method does Kerberos employ?
    a. Blowfish cryptography.
    b. El Gamal cryptography.
    c. Secret Key cryptography.
    d. Public Key cryptography.

22. What is the maximum allowable key size of the Rijndael encryption algorithm?
    a. 128 bits
    b. 192 bits
    c. 512 bits
    d. 256 bits

23. Cryptography does NOT concern itself with:
    a. Authenticity
    b. Confidentiality
    c. Integrity
    d. Availability

24. Which of the following is the primary purpose for using one-way hashing of user passwords within a password file?
    a. It prevents an unauthorized person from trying multiple passwords in one logon attempt.
    b. It minimizes the amount of storage required for user passwords.
    c. It minimizes the amount of processing time used for encrypting passwords.
    d. It prevents an unauthorized person from reading or modifying the password.

25. What is a characteristic of using DES in Electronic Code Book?
    a. Individual characters are encoded by combining output from earlier encryption routines with plaintext.
    b. The previous DES output is used as input.
    c. Repetitive encryption obscures any repeated patterns that may have been present in the plaintext.
    d. A given block of plaintext and a given key will always produce the same ciphertext.

26. Which encryption algorithm is BEST suited for communication with handheld wireless devices?
    a. ECC (Elliptic Curve Cryptosystem)
    b. RSA
    c. SHA
    d. RC4

27. What is the size of an MD5 message digest (hash)?
    a. 160 bytes
    b. 160 bits
    c. 256 bits
    d. 128 bits

28. Which is NOT a suitable method for distributing certificate revocation information?
    a. Distribution point CRL
    b. Delta CRL
    c. OCSP (online certificate status protocol)
    d. CA revocation mailing list

29. What is the maximum number of different keys that can be used when encrypting with Triple DES?
    a. 4
    b. 3
    c. 2
    d. 1

30. Which of the following statements related to a private key cryptosystem is FALSE?
    a. Data Encryption Standard (DES) is a typical private key cryptosystem.
    b. Two different keys are used for the encryption and decryption.
    c. The encryption key should be secure.
    d. The key used for decryption is known to the sender

31. Where parties do not have a shared secret and large quantities of sensitive information must be passed, the most efficient means of transferring information is to use a hybrid encryption technique. What does this mean?
    a. Use of elliptic curve encryption.
    b. Use of the recipient's public key for encryption and decryption based on the recipient's private key.
    c. Use of software encryption assisted by a hardware encryption accelerator.
    d. Use of public key encryption to secure a secret key, and message encryption using the secret key.

32. Which of the following BEST provides e-mail message authenticity and confidentiality?

a. Signing the message using the sender's private key and encrypting the message using the receiver's public key

b. Signing the message using the receiver's private key and encrypting the message using the sender's public key

c. Signing the message using the receiver's public key and encrypting the message using the sender's private key

d. Signing the message using the sender's public key and encrypting the message using the receiver's private key

33. Which of the following standards concerns digital certificates?
    a. X.400
    b. X.25
    c. X.509
    d. X.75

34. Which of the following was not designed to be a proprietary encryption algorithm?
    a. RC2
    b. Skipjack
    c. Blowfish
    d. RC4

35. Which of the following asymmetric encryption algorithms is based on the difficulty of factoring large numbers?
    a. International Data Encryption Algorithm (IDEA)
    b. RSA
    c. Elliptic Curve Cryptosystems (ECCs)
    d. El Gamal

36. Which of the following is NOT a mode of the Data Encryption Standard (DES)?
    a. Output Feedback (OFB)
    b. Cipher Block Chaining (CBC)
    c. Substitution
    d. Electronic Code Book (ECB)

37. Which of the following standards concerns digital certificates?
    a. X.400
    b. X.75
    c. X.509
    d. X.25

38. Which of the following statements is true about data encryption as a method of protecting data?
    a. It requires careful key management.
    b. It is usually easily administered.
    c. It makes few demands on system resources.
    d. It should sometimes be used for password files.

39. Brute force attacks against encryption keys have increased in potency because of increased computing power. Which of the following is often considered a good protection against the brute force cryptography attack?
    a. Nothing can defend you against a brute force crypto key attack.
    b. Algorithms that are immune to brute force key attacks.
    c. The use of good key generators.
    d. The use of session keys..

40. Which type of attack is based on the probability of two different messages using the same hash function producing a common message digest?
    a. Differential linear cryptanalysis
    b. Birthday attack
    c. Statistical attack
    d. Differential cryptanalysis

41.—50. *Fill in the name of the service.*

Service	**Mechanism**	**Definition**
	MAC Digital Signature Certificates PKI	Provides assurance of the origin of data to both the receiver and a third party. The objective is to provide evidence to counter denials that the sender participated in a specified transaction. (NIST 800-21)
	Hash MAC Digital Signature Certificates PKI	Protects a communication system against acceptance of a fraudulent transmission or simulation by establishing the validity of the information content and the originator. (NIST 800-21)
	Hash/Digest MAC Digital Signatures	The property that sensitive data has not been modified or deleted in an unauthorized and undetected manner. (FIPS 140-2)
	encryption/ decryption	The property that sensitive information is not disclosed to unauthorized individuals, entities, or processes. (FIPS 140-2)