

**Computer and Network Security
Fall Semester 2002**

Midterm Test

October 6, 2002

Time Allowed: One Hour

Instructions: Answer ALL questions by circling the correct choice. Each correct response carries two points.

Name: _____

Total: 100 Points

1. The requirement that only authorized parties can modify the computer system assets is called:
a. *Integrity* b. *Availability* c. *Secrecy* d. *Authenticity*
2. Interruption is an attack on the:
a. *Integrity* b. *Availability* c. *Secrecy* d. *Authenticity*
3. Attacks which are difficult to detect because there is no modification of data are called:
a. *Replay Attacks* b. *Dictionary Attacks* c. *Active Attacks* d. *Passive Attacks*
4. Which of the following is a passive attack:
a. *Interruption* b. *Traffic Analysis* c. *Modification* d. *Fabrication*
5. Encryption can protect from Traffic Analysis.
a. *True* b. *False*
6. Data padding and filler sequences can protect from Traffic Analysis.
a. *True* b. *False*
7. DES is a security mechanism.
a. *True* b. *False*
8. Computer security is constrained by societal factors.
a. *True* b. *False*
9. The type of attack in which an entity pretends to be another entity is called:
a. *Masquerade* b. *Replay* c. *Modification of* d. *Denial of service*
Messages
10. The art of breaking ciphers, i.e. retrieving the plaintext without knowing the proper key is called:
a. *Message Authentication* b. *Digital Signature* c. *Cryptanalysis* d. *Cryptography*
11. A mathematical formula that is easy to work forward but very hard to work backward is called:
a. *Backdoor* b. *Euler's Totient Function* c. *Trapdoor* d. *Logic Bomb*
12. The person who designs cryptographic algorithms and cryptosystems is called a
a. *Cryptanalyst* b. *Cryptologist* c. *Cryptographer* d. *Cypherpunk*

13. Generally, asymmetric algorithms are much faster to execute on a computer than symmetric ones.
 a. *True* b. *False*
14. Caesar's cipher is an example of a mono-alphabetic transposition cipher.
 a. *False* b. *True*
15. The Scytale cipher is an example of a mono-alphabetic transposition cipher.
 a. *False* b. *True*
16. If the strength of your new cryptosystems relies on the fact that the attacker does not know the algorithm's inner workings, you are sunk. This principle is called:
 a. *Al-Kindi's Rule* b. *Ceaser's Principle* c. *Scytale's Algorithm* d. *Kerchoff's Principle*
17. Concatenation of various ciphers is called:
 a. *Poly-alphabetic cipher* b. *Polymorphic cipher* c. *Product cipher* d. *Sum cipher*
18. Which of the following is not a constituent of a cipher mode?
 a. *Feedback* b. *Simple Operation* c. *Encryption Algorithm* d. *Noise*
19. To encrypt 1 MB of plain-text using a One Time Pad (OTP) how long a truly random key would be required?
 a. *64 bits* b. *128 bits* c. *10 MB* d. *1 MB*
20. Data Encryption Standard uses a key length and block size of respectively
 a. *64 and 56 bits* b. *56 and 64 bits* c. *56 and 56 bits* d. *64 and 64 bits*
21. According to the shift schedule for the encipherment key the number of left shifts for the key in round 11 in DES is
 a. *2* b. *3*
22. A mode of use that can be employed to prevent subversion of DES when used as a block cipher is:
 a. *ECB* b. *CBC* c. *OFB* d. *RC5*
23. Which of the following is not a mode of use of DES
 a. *OFB* b. *CFB* c. *ECB* d. *RC5*
24. When using DES in Cipher Block Chaining mode, the repetitions in message can be reflected in ciphertext.
 a. *True* b. *False*
25. With a 128 bit key length for a block cipher, the number of possible keys is:
 a. 10^{128} b. 3.40×10^{128} c. 2×10^{38} d. 3.40×10^{38}
26. Data Encryption Standard when used in electronic codebook mode is a mono-alphabetic block substitution cipher.
 a. *False* b. *True*

27. Diffusion is achieved through permutations.
 a. *True* b. *False*
28. Diffusion is achieved through substitutions.
 a. *True* b. *False*
29. In which stream mode does an error during data transmission propagate to future bytes?
 a. *ECB* b. *CBC* c. *CFB* d. *OFB*
30. A mathematical formula that is easy to work forward but very hard to work backward is called
 a. *Backdoor* b. *Euler's Totient Function* c. *Trapdoor* d. *Logic Bomb*
31. There are infinitely many prime numbers.
 a. *False* b. *True*
32. 7 is relatively prime to 11
 a. *True* b. *False*
33. Generally, asymmetric encryption algorithms are much faster to execute on a computer than symmetric ones.
 a. *True* b. *False*
34. Which of the following is a primitive root of 11?
 a. 3 b. 5 c. 7 d. 9
35. The list of all the primitive roots of 7 is?
 a. 2, 3, 4, 5, 6 b. 2, 3, 5, 6 c. 2, 3, 5 d. 3, 5
36. Which of the following is the discrete logarithm of 5 mod 13 if the primitive root 2 is used as the base?
 a. 3 b. 6 c. 9 d. 12
37. $(\phi(11) + \phi(7)) \bmod \phi(5) =$
 a. 0 b. 1 c. 2 d. 3
38. The first public-key scheme which was capable of signatures as well as encryption was
 a. *DES* b. *RSA* c. *Diffie-Hellman* d. *Merkle Knapsack*
39. The modular inverse of 7 mod 13 is
 a. 3 b. 5 c. 2 d. 12
40. In a Diffie-Hellman Key Exchange for a common Secret Key K between users A and B first $q = 11$ a prime number and $\alpha = 2$ a primitive root of q are agreed upon. Then A chooses a private value $X_A = 3$ and generates and transmits a Public value Y_A . B on the other hand chooses a Private value $X_B = 6$ and generates and transmits a Public value Y_B . What is the Secret Key K generated by users A and B?
 a. 2 b. 3 c. 6 d. 9

41. The first ten letters of the encryption of the following plain-text with the given poly-alphabetic cipher of period 2 would be:

Plain-text: An attorney who defends himself has a fool for a client

Key:

 abcdefghijklmnopqrstuvwxyz
M1: PQRSTUVWXYZABCDEFGHI
M2: HJKLMNQRSTUWXYZOMEGAPIBCDF

- a. *YPAPZBYZDT* b. *HWABAOEWNG* c. *PYPABZZYTD* d. *None of the other given choices*

42. In a public key system using RSA, you intercept the ciphertext $C = 13$ sent to a user whose public key is $\{e = 7, n = 55\}$. What is the plaintext M ?

- a. 7 b. 23 c. 40 d. 52

43. SHA-1 produces an output of:

- a. 128 bits b. 160 bits c. 256 bits d. 512 bits

44. The first standard by the US Government for implementing Message Authentication was:

- a. *DES* b. *DESMAC* c. *RSA* d. *Diffie-Hellman*

45. $15 \times 5 \bmod 4 \bmod 5 \bmod 7 =$

- a. 0 b. 1 c. 6 d. 3

46. Which of the following requires the real-time involvement of the trusted third party in order to complete the protocol?

- a. *Adjudicated Protocol* b. *Arbitrated Protocol*

47. Which of the following characters is the trusted arbitrator in security protocols?

- a. *Eve* b. *Bob* c. *Mallory* d. *Trent*

48. Encryption of the following plaintext using a single transposition cipher with the keyword "NED" results in the following first ten characters. Using "Z" for padding, if required.

A quick brown fox jumped over the lazy dog

- a. *OFJPOREZOZ* b. *AIBWOUEVTL* c. *AQUICKBROW* d. *None of the other given choices*

49. In the Diffie-Hellman Key Exchange for a common Secret Key K between users A and B first q a prime number and α a primitive root of q are agreed upon. Then A chooses a private value X_A and generates and transmits a Public value Y_A . B on the other hand chooses a Private value X_B and generates and transmits a Public value Y_B . What is the formula for the Secret Key generation for the user B?

- a. $K = \alpha^{X_B} \bmod q$ b. $K = (Y_B)^{X_A} \bmod q$ c. $K = (Y_A)^{X_B} \bmod q$ d. $K = \alpha^{X_A} \bmod q$

50. Which of the following hash functions is big endian?

- a. *SHA-1* b. *MD-5* c. *RIPEMD-160* d. *a and b*