NED UNIVERSITY OF ENGINEERING AND TECHNOLOGY, KARACHI
MASTER OF COMPUTER SCIENCE AND INFORMATION TECHNOLOGY
FALL SEMESTER EXAMINATION -2007

Dated: 06-12-2007

Time: 3 Hours **Max Marks: 70**

CRYPTOGRAPHY & NETWORK SECURITY
(CT-522)

Do all questions from SECTION-A & SECTION-B

SECTION-A

Q: Multiple Choice questions. **(50-Marks)**

1. **Any action that compromises the security of information is called:**

a) Security Attack b) Passive Attack
c) active attack d) Interruption

2. **An attack on availability of data is called:**

a) Interruption b) Passive Attack
c) active attack d) Interception

3. **An attack on confidentiality of data is called:**

a) Interruption b) Passive Attack
c) active attack d) Interception

4. **An attack on integrity of data is called:**

a)Modification b) Interruption
c) active attack d) Interception

5. **An attack on authenticity of data is called:**

a) Modification b) Interruption
c) Fabrication d) Interception

6. **Cryptology is the branch of mathematics which encompasses:**

a) Cryptography b) Cryptanalysis
c) Cryptography and Cryptanalysis d) Security and Mechanisms

7. **Security depends on the secrecy of :**

a) secrecy of key b) secrecy of algorithm
c) both secrecy of key and Algorithm d) Security Mechanisms

8. **The method that conceals the existence of the message, and render the message unintelligible to outsider by different transforms such as use of invisible ink is:**

a) Caesar Cipher b) Cryptanalysis
c) Steganograpghy d) Transposition

9. **For the plaintext "want", find the Ciphertext using Caesar Cipher:**

10. Apply Transposition Cipher to the plaintext below, to find the Ciphertext:

COMPUTER GRAPHICS MAY BE SLOW

11. Original intelligible message or data that is fed into the algorithm as input is:

a) Plaintext
b) Ciphertext
c) Decryption algorithm
d) Secret Key

12. An algorithm that performs various substitutions & transformations on the Plaintext:

a) Decryption Algorithm
b) Encryption Algorithm
c) Ciphertext & Algorithm
d) Cryptography

13. The scrambled message produced as o/p is:

a) Ciphertext
b) Plaintext
c) Ciphertext & Algorithm
d) Cryptography

14. Ciphertext depends on:

a) Plaintext & Secret Key.
b) Plaintext
c) Ciphertext & Algorithm
d) hy

15. The encryption Algorithm run in reverse is:

a) Decryption Algorithm
b) Plaintext
c) Ciphertext
d) Cryptography

16. Ciphertext + Secret Key produces:

a) Original Plaintext
b) Decipher text
c) Encryption Algorithm
d) Ciphertext

17. Message = X, Encryption Key = K Ciphertext =C.
We can write for the Ciphertext.

a) $C=E_k(X)$
b) D=C(X)
c) C = P (E)
d) C=D(X)

18. Two general approaches to attacking a conventional encryption scheme:

a) Cryptanalysis & Brute force attack
b) Cryptology & Cryptography
c) Monoalphabetic & polyalphabetic
d) Passive attack & Passive Attack

19. With the exception of a scheme known as the one-time pad, there is no encryption algorithm that is unconditionally secure.

a) True
b) False

20. In Brute force approach, on average, half of all possible keys must be tried, to achieve success.
a) True
b) False

21. DES algorithm uses 56-bit key size. No. of alternative keys used is:

a) $2^{56} = 7.2 \times 10^{16}$
b) 2^{55}
c) 55
d) 168

22. AES uses _____ bit key size.

a) 128 bit
b) 56
c) 32
d) 168

23. Triple DES uses _____ key size.
a) 128 bit
b) 56
c) 32
d) 168 bit

24. General Caesar algorithm is :

a) C= (P+K) mod (26)
b) E= (P+3)mod 26
c) 32
d) 168 bit

25. The Decryption algorithm is :

a) P= D(C) = (C – K) mod (26).
b) D= (P+3)mod 26
c) C= (P+K) mod (26)
d) C= (P-K) mod (26)

26. Use one time Pad: to find Ciphertext.

Plaintext: Mustard
Key: pxlmvms

a) Ciphertext: csegwew
b) D= (P+3)mod 26
c) C = lsxnbtj
d) C= (P-K) mod (26)

27. Because a different key is used on each side of the process, public key syst
are also known as _____

a) Private Systems

b) Secure Systems

c) Asymmetric Systems

d) Symmetric Systems.

28. In case of Public Key Encryption scheme, _____ Key(s) is used
encryption.

a) Private

b) Public

c) Single

d) Both a & b

29. In case of Public Key Encryption scheme, _____ Key(s) is used
decryption.

a. Private

b. Public

c. Master

d. None of the above

30. _____ Algorithm is used for calculation of Public and Private Key

a. Euler

b. RC4

c. RSA

d. None of the above

31. RSA scheme is a _____ in which the plain text and cipher text are
integers between 0 and n-1 for some n.

a. Block Ciphers

b. Stream of bits

c. Clock + Stream of Bits

d. None of the above.

32. Size of key in case of Public key is _____ bits

a. 50-250

b. 250-500

c. 1000-5000

d. 500-2500

33. Relative speed of Public key is _____ Single key

a. Faster than
b. Slower than
c. Almost equal to
d. Depend on

34. _____ is a mathematical formula used for Public Key encryption which is easy to work in forward direction but difficult to work in backward direction

a. Factorization
b. Trapdoor
c. Multiplication of prime number
d. Addition of relative prime numbers

35. A typical size for n in RSA is _____bit or _____ decimal digits

a. 24, 8
b. 500, 150
c. 80, 25
d. 1024, 309

36. Prime numbers are divisible by _____ and _____.

a. 1, 10
b. 1, itself
c. itself, all its factors
d. any odd number, any even number

37. Two number are relative prime if they share only one factor namely _____.

a. Itself
b. 1 x 3
c. 1
d. None of the above

38. Encryption in RSA is of _____ form.

a. $C = M^e \bmod n$
b. $E = M^c \bmod n$
c. $C = M^d \bmod n$
d. $M = D^c \bmod n$

39. Decryption in RSA is of _____ form.

a. $C = M^e \bmod n$

b. $E = M^c \bmod n$

c. $C = M^d \bmod n$

d. $M = C^d \bmod n$

40. $Ed = 1 \bmod \Phi(n)$ where 0 ___ d___ n.

a. <,>

b. >=, =

c. =, =

d. <, <

41. 'e' relative prime to z is used for encryption must meet two conditions _____ & _____.

a. $e < n$, $\gcd(e, \Phi(n)) = 1$

b. $e < n$, $\gcd(n, \Phi(n)) = 1$

c. $e > n$, $\gcd(e, \Phi(n)) > 1$

d. $n > e$, $\gcd(e, \Phi(n)) > 1$

42. Product of e & d is congruent to _____.

a. $1 \bmod ((p-1)(q-1))$

b. $1 \bmod ((1/p)(1/q))$

c. $n \bmod ((1-p)(1-q))$

d. None of the above

43. e & n together form _____ Key.

a. Public

b. Private

c. Single

d. None of the above.

44. d & n together form _____ Key.

a. Public

b. Private

c. Symmetric

d. None of the above

45. z=(p-1)(q-1) is the quotient function of _____.

a. Φ(e)

b. Φ(d)

c. Φ(M)

d. Φ(n)

46. RSA is susceptible to _____, _____ & _____ attacks.

a. Brute force, mathematical, timing

b. Dictionary, timing, brute force

c. Mathematical, timing, dictionary

d. Timing, dictionary, brute force

47. _____ is a practical method for public exchange of a secret key.

a. DES

b. Diffie Hellman Key Exchange

c. Advance Encryption Scheme

d. brute force

48. The Diffie-Hellman algorithm uses_____ in a finite (Galois) field (modulo a prime or a polynomial), and depends for its effectiveness on the difficulty of computing discrete logarithms.

a. RSA

b. exponentiation

c. Advance Encryption Scheme

d. Encryption

49. In the Diffie-Hellman key exchange algorithm, there are two_____ known numbers: a prime number q and an integer "a" that is a primitive root of q.

a. publicly

b. secretly

c. Privately

d. Commonly

50. A digital signature is an authentication mechanism that enables the creator of a message to attach a code that acts as a signature.

a. publicly b. secretly c. Privately d. Commonly

SECTION-B (Choice given in Q2 & Q4)

(20marks)

Q1. Why is PGP popular? Name the five PGP services, and the Algorithms used to perform these services. (5marks)

Q2. What is a dual Signature and what is its purpose? (5marks)

OR

Discuss the types of Web Security Threats, and the Protocols that provide Web Security.

Q3 : What is a Message Authentication Code? What is the difference between a message authentication code and a one way Hash function? (5marks)

Q4: In a Public key system using RSA, P = 7, q = 11, e = 17, and M = 8. Perform encryption and decryption. (5marks)

OR

Consider a Diffie Hellman scheme with a common prime q = 71 and a primitive root $\alpha = 7$.

(a) If user A has a private key $X_A = 5$, what is A's public key Y_A?

(b) If user B has a private key $X_B = 12$, what is B's public key Y_B?

(c) What is the shared secret key? (5marks)