BRAINWARE UNIVERSITY

Term End Examination 2020 - 21

Programme – Master of Science in Computer Science

Course Name – Cryptography and Network Security

Course Code - MCS304

Semester / Year - Semester III

Time allotted : 75 Minutes | Full Marks : 60

[The figure in the margin indicates full marks. Candidates are required to give their answers in their own words as far as practicable.]

Group-A

(Multiple Choice Type Question) 1 x 60=60

1. *(Answer any Sixty)*

(i) If the principle of ___ is to be ensured, the contents of a message must not be modified while in transit.

a) Confidentiality
b) Authentication
c) Integrity
d) Access control

(ii) What is the size of the key in the SDES algorithm?

a) 24
b) 20
c) 16
d) 10

(iii) The ___ attack is related to confidentiality.

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

(iv) Which of the following is a passive attack?

a) Masquerade
b) Replay
c) Denial of Service
d) Traffic analysis

(v)

Use Caesar's Cipher to decipher the following

HQFUBSWHG WHAW

a) ABANDONED LOCK
b) ENCRYPTED LOCK
c) ENCRYPTED TEXT
d) ABANDONED TEXT

(vi) Caesar Cipher is an example of

a) Poly-alphabetic Cipher
b) Multi-alphabetic Cipher
c) Mono-alphabetic Cipher
d) Bi-alphabetic Cipher

(vii) Choose from among the following cipher systems, from best to the worst, with respect to ease of decryption using frequency analysis.

a) Random Polyalphabetic, Plaintext, Playfair
b) Random Polyalphabetic, Playfair, Vignere
c) Random Polyalphabetic, Vignere, Playfair, Plaintext
d) Random Polyalphabetic, Plaintext, Beaufort, Playfair

(viii) A symmetric cipher system has an IC of 0.041. What is the length of the key 'm'?

a) 1
b) 3
c) 2
d) 5

(ix) When a hash function is used to provide message authentication, the hash function value is referred to as

a) Message field
b) Message digest
c) Message score
d) Message leap

(x) In cryptography, what is cipher?

a) encrypted message
b) both algorithm for performing encryption and decryption and encrypted message
c) Decrypted message
d) none of these

(xi) In asymmetric key cryptography, the private key is kept by

a) sender
b) receiver

c) sender and receiver

d) public

(xii) Which one of the following algorithms is NOT used in asymmetric-key cryptography?

a) RSA

b) Diffie Hellman algorithm

c) CBC

d) ECB

(xiii) In cryptography, the order of the letters in a message is rearranged by

a) transposition ciphers

b) substitution ciphers

c) both transposition ciphers and substitution ciphers

d) none of these

(xiv) Cryptanalysis is used

a) to find some insecurity in a cryptographic scheme

b) to increase the speed

c) to encrypt the data

d) All of these

(xv) How many modes of operation are there in DES and AES?

a) 4

b) 3

c) 2

d) 5

(xvi) Which one of the following modes of operation in DES is used for operating short data?

a) Cipher Feedback Mode (CFB)

b) Cipher Block chaining (CBC)

c) Electronic code book (ECB)

d) Output Feedback Modes (OFB)

(xvii) In the DES algorithm the Round Input is 32 bits, which is expanded to 48 bits via

a) Scaling of the existing bits

b) Duplication of the existing bits

c) Addition of zeros

d) . Addition of ones

(xviii) Firewall is a specified form of

a) bridge

b) disc

c) router

d) printer

(xix) Which is used to verify the integrity of a message?

a) message digest

b) decryption algorithm

c) digital envelop

d) encryption algorithm

(xx) DES encrypts blocks of ____ bits

a) 32

b) 64

c) 56

d) 128

(xxi) If A wants to send an encrypted message to B, the plaintext is encrypted with the public key of

a) A

b) B

c) the network

d) either A or B

(xxii) If A wants to send a message to B for authentication, it is encrypted with the private key of

a) A

b) B

c) The network

d) Either A or B

(xxiii) Homophonic substitution cipher is ____ to break as compared to mono alphabetic cipher

a) easier

b) the same

c) difficult

d) Easier or same

(xxiv) The Plaintext for the Ciphertext 00100010, given that the key is 1111111111 is

a) 01100111
b) 00001010
c) 01001000
d) 01001100

(xxv) Which mode of operation has the worst “error propagation” among the following?

a) OFB
b) CFB
c) CBC
d) ECB

(xxvi) The number of rounds in RC5 can range from 0 to _____

a) 127
b) 63
c) 255
d) 31

(xxvii) The total number of subkeys t used in the RC5 algorithm is given by the formula (r corresponds to number of rounds)

a) t=2r+4
b) t=2r
c) t=2r-2
d) t=2r+2

(xxviii) RC5 uses 2 magic constants to define their subkeys. These are

a) Base of natural Logarithm and Golden ratio
b) Base of natural Logarithm and Pi
c) Golden Ratio and Pi
d) Pi and Golden Ration

(xxix) The value of the base of natural logarithms is

a) e=2.7073
b) e=2.7183
c) e=3.7183
d) e=1.7273

(xxx) The matrix theory is used in

a) Hill cipher
b) Playfair cipher
c) Mono alphabetic cipher
d) Vigenere cipher

(xxxi) On comparing AES with DES, which of the following functions from

DES does not have an equivalent AES function?

a) f function
b) permutation p
c) swapping of halves
d) xor of subkey with function f

(xxxii) SHA-1 produces a hash value of

a) 256
b) 160
c) 180
d) 128

(xxxiii) A worm __ modify a program

a) does
b) does not
c) may
d) may or may not

(xxxiv) For the AES-128 algorithm there are _____ similar rounds and _____ round is different.

a) 2 pair of 5 similar rounds; every alternate
b) 9; the last
c) 8; the first and last
d) 10 ; no

(xxxv) In which attack, there is no modification in message contents?

a) Active
b) Passive
c) Both active and passive
d) None of these

(xxxvi) How many rounds are present in each iteration function of SHA-3?

a) 3
b) 4
c) 5
d) 6

(xxxvii) A virus that can't be detected by antivirus is

a) Parasitic
b) polymorphic
c) worm
d) stealth

(xxxviii) Which one of the following is not a RC5 mode of operation?

a) RC5 block cipher
b) RC5-Cipher Block Chaining

c) RC5-Cipher Padding
d) RC5-CipherText Stealing

(xxxix) Which of these is not a characteristic of block ciphers?

a) Variable key length / block size / number of rounds
b) Mixed operators, data/key dependent rotation
c) Key independent S-boxes
d) More complex key scheduling

(xl) Which one of the following RC4 algorithm not used in?

a) SSL
b) TLS
c) FTP
d) WEP

(xli) For an inputs key of size 128 bits constituting of all zeros, what is w(7) ?

a) {62 63 63 63}
b) {62 62 62 62}
c) {00 00 00 00}
d) {63 63 63 62}

(xlii) Digital signature cannot provide _____ for the message.

a) integrity
b) confidentiality
c) nonrepudiation
d) authentication

(xliii) Man in the middle attack can endanger the security of Diffie Hellman method if two

a) joined
b) authenticated
c) submitted
d) shared

(xliv) What is the name for Public Key Infrastructure certificate?

a) Man in the Middle attack
b) Certificate Authority
c) Resource Access Control facility
d) Script kiddy

(xlv) Which one of the following is active attack?

a) Masquerade
b) Traffic analysis.
c) Eavesdropping.
d) Shoulder surfing

(xlvi) The main goal of _____ attack is to obtain unauthorized access to the information.

a) Active
b) Caesar
c) Passive
d) Brute force

(xlvii) In IDEA key is of _____ bits

a) 128
b) 64
c) 256
d) 512

(xlviii) DES uses a key generator to generate sixteen _____ round keys.

a) 32-bit
b) 48-bit
c) 54-bit
d) 42-bit

(xlix) ECB and CBC are _____ ciphers.

a) block
b) stream
c) field
d) none of these

(l) Which security protocol is used to secure pages where users are required to submit sensitive information?

a) Secure Socket Layer
b) Transport Layer Security
c) Secure IP
d) Secure HTTP

(li) Which one of the following algorithms is not supported by the Digital Signature Standard?

a) Digital Signature Algorithm
b) RSA
c) El Gamal DSA
d) Elliptic Curve DSA

(lii) What type of cryptographic attack rendered Double DES (2DES) no more effective than standard DES encryption?

a) Birthday
b) Chosen ciphertext
c) Meet-in-the-middle
d) Man-in-the-middle

(liii) SET is

a) Electronic Payment System
b) Security Protocol
c) Credit card payment
d) Internet Payment System

(liv) The sub key length at each round of DES is

a) 32
b) 56
c) 48
d) 64

(lv) IDEA uses --- keys

a) 3
b) 4
c) 5
d) 2

(lvi) Message_____ means that the data must arrive at the receiver exactly as sent.

a) confidentiality
b) integrity
c) authentication
d) none of these

(lvii) Interception is an attack on

a) Availability
b) Confidentiality
c) Integrity
d) Authenticity

(lviii) In _____, the malicious code is installed on a personal computer or server misdirecting users to fraudulent website.

a) Phishing scam
b) Pharming scam
c) Spoofing
d) Sniffing

(lix) The number of unique substitution boxes in DES after the 48 bit XOR operation are

a) 8
b) 4
c) 6
d) 12

(lx) In triple DES, the key size is ___ and meet in the middle attack takes ___ tests to break the key.

a) 2192 ,2112
b) 2184,2111
c) 2168,2111
d) 2168,2112