BRAINWARE UNIVERSITY

ODD Semester Examinations 2021- 22

Programme – Master of Computer Applications - 2020 [MCA]

Course Name – Cryptography & Network Security

Course Code – MCA304A

(Semester III)

Time allotted : 1 Hour 15 Minutes | Full Marks : 60

(Multiple choise type question) | 60 x 1 = 60

Choose the correct alternative from the following

(I) Polygraphic substitution is a cipher in which-

A) a uniform substitution is performed on blocks of letters
B) a random substitution is performed on blocks of letters
C) a uniform substitution is performed on sequence of numbers
D) a random substitution is performed on sequence of numbers

(II) ElGamal encryption system is _____

A) symmetric key encryption algorithm
B) asymmetric key encryption algorithm
C) not an encryption algorithm
D) block cipher method

(III) The numerical version of READY modulo 26 is

A) 17 04 00 03 24
B) 16 04 00 03 24
C) 17 03 00 03 24
D) 17 04 00 03 23

(IV) The Permutation Cipher is another form of-

A) Rijndael cipher
B) AES block cipher
C) DES block cipher
D) Transposition Cipher

(V) The private key in asymmetric key cryptography is kept by

A) Sender
B) Receiver
C) Sender and receiver
D) All the connected devices to the network

(VI) DES has an initial and final permutation block and _____ rounds.

A) 14
B) 15
C) 16
D) 17

(VII) This was commonly used in cryptography during World War II.

A) tunneling
B) personalization
C) van Eck phreaking
D) one-time pad

(VIII) In a reverse brute-force attack, _____against multiple usernames or encrypted files

A) Random passwords are tested
B) a finite set of pre-generated passwords are tested
C) a single (usually common) password is tested
D) none of these

(IX) In Cryptography, the original message, after being transformed, is called _____

A) cipher text
B) plain text
C) decrypted text
D) key text

(X) Caesar cipher is a form of-

A) Rijndael cipher
B) block cipher
C) Substitution cipher
D) Transposition Cipher

(XI) The Advanced Encryption Standard (AES), has three different configurations with respect to the number of rounds and _____

A) data size
B) round size
C) key size
D) encryption size

(XII) In_____ cipher, the same key is used by the sender and the receiver.

A) symmetric-key
B) asymmetric-key
C) either private or public
D) neither private nor public

(XIII) Voice privacy in GSM cellular telephone protocol is provided by _____

A) A5/2 cipher
B) b5/4 cipher
C) b5/6 cipher
D) b5/8 cipher

(XIV) In a Shift cipher, the plaintext MIDNIGHT has been changed with a key 11. what will be the Ciphertext?

A) TRSETXOY
B) XTOYTRSE
C) TRSERSE
D) all of tese

(XV) To encrypt the plaintext, a cryptographic algorithm works in combination with a key _____

A) Word, number, or phrase
B) Special Symbols
C) Function Keys
D) All of these

(XVI) The Rijndael S-box is a substitution box (lookup table) used in the_____

A) Rijndael cipher
B) AES block cipher
C) DES block cipher
D) Transposition Cipher

(XVII) _____was first described in 1991, as an intended replacement for DES.

A) IDEA
B) RC5
C) ESA
D) RSA

(XVIII) The Data Encryption Standard (DES) is an example of a _____

A) Conventional cryptosystem
B) Asymmetric cryptosystem
C) Caesar's cryptosystem
D) All of these

(XIX) _____ is a free and open-source C++ class library of cryptographic algorithms and schemes written by Wei Dai.

A) Crypto++ (also known as CryptoPP, libcrypto++, and libcryptopp)
B) Cipher++ (also known as CipherPP)
C) both, Cipher++and Crypto++
D) none of these

(XX) In password protection, this is a random string of data used to modify a password hash.

A) sheepdip
B) salt
C) bypass
D) dongle

(XXI) DES works by using

A) Permutation and substitution on 64 bit blocks of plaintext
B) Only permutations on blocks of 128 bits
C) Exclusive ORing key bits with 64 bit blocks
D) 4 rounds of substitution on 64 bit blocks with 56 bit keys

(XXII) The _____ cipher reorders the plaintext characters to create a cipher text.

A) substitution
B) transportation
C) either substitution or transportation
D) neither substitution nor transportation

(XXIII) Public-key cryptography, also known as-

A) cryptography
B) secured cryptography
C) symmetric cryptography
D) asymmetric cryptography,

(XXIV) This is a trial and error method used to decode encrypted data through exhaustive effort rather than employing intellectual strategies.

A) chaffing and winnowing
B) cryptanalysis
C) serendipity
D) brute force cracking

(XXV) Cipher block chaining (CBC) is a mode of operation for a _____

A) shift cipher
B) block cipher
C) modern cipher
D) ceascer cipher

(XXVI) A mechanism used to encrypt and decrypt data is called-

A) Cryptography
B) Algorithm
C) Data flow
D) None of these

(XXVII) Which of the following is not a type of symmetric-key cryptography technique?

A) Caesar cipher
B) Data Encryption Standard (DES)

C) Diffie Hellman cipher
D) Playfair cipher

(XXVIII) This is the inclusion of a secret message in otherwise unencrypted text or images.

A) masquerade
B) steganography
C) spoof
D) eye-in-hand system

(XXIX) Generally S-box is a _____ m-bits input to n-bits output.

A) combination or set of combinations of private keys
B) permutation or set of permutations mapping
C) combination or set of combinations of secret keys
D) none of these

(XXX) Security Goals of Cryptography are _____

A) Confidentiality
B) Authenticity
C) Data integrity
D) All of these

(XXXI) This is the encryption algorithm that will begin to supplant the Data Encryption Standard (DES) - and later Triple DES - over the next few years as the new standard encryption algorithm.

A) Rijndael
B) Kerberos
C) Blowfish
D) IPsec

(XXXII) The relationship between a character in the plaintext to a character is

A) one-to-many relationship
B) many-to-one relationship
C) many-to-many relationship
D) none

(XXXIII) A straight permutation cipher or a straight P-box has the same number of inputs as _____

A) outputs
B) cipher
C) frames
D) bits

(XXXIV) In a public key encryption if A wants to send an encrypted message

A) A encrypts message using his private key
B) A encrypts message using B's private key
C) A encrypts message using B's public key
D) A encrypts message using his public key

(XXXV) A cryptographic hash function (CHF) is a

A) Invertible function
B) One way function
C) Bijective function(
D) none of these

(XXXVI) _____is a tool that changes the order of the input bits and they appear in the output. In this case, the key is order transmission of input bits in output bits.

A) P-Box
B) S-Box
C) T-Box
D) none of these

(XXXVII) _____ is a symmetric block cipher chosen by the U.S. government to protect classified information

A) Diffie-Hellman
B) Rotation cipher
C) The Advanced Encryption Standard (AES)
D) XOR cipher

(XXXVIII) Today, many Internet businesses and users take advantage of cryptography based on this approach.

A) public key infrastructure
B) output feedback
C) Encrypting File System
D) single signon

(XXXIX) Public key system is useful because

A) It uses two keys
B) There is no key distribution problem as public key can be kept in a commonly accessible database
C) Private key can be kept secret
D) It is symmetric key system

(XL) The ciphers of today are called round ciphers because they involve

A) Single round
B) Double rounds
C) Multiple round
D) Round about

(XLI) The cipher block chaining process uses a l_____ to administer this process of observation.

A) Logical gate called XOR
B) Logical gate called AND
C) Logical gate called NOR
D) Logical gate called NOT

(XLII) What is data encryption standard (DES)?

A) stream cipher
B) bit cipher

C) block cipher D) byte cipher

(XLIII) This is a mode of operation for a block cipher, with the characteristic that each possible block of plaintext has a defined corresponding ciphertext value and vice versa.

A) footprinting B) hash function

C) watermark D) Electronic Code Book

(XLIV) The numerical version 11 17 00 08 13 22 00 17 04 in modulo 26 denotes

A) ABCDE B) BRAINWARE

C) AQ0HMV0D D) none of these

(XLV) An S-box is a basic component which performs _____.

A) Permutation B) substitution

C) transposition D) DES function

(XLVI) "A key is a string of bits used by a cryptographic algorithm to transform plain text into ciphertext." Which of the following is capable of becoming a key in a cryptographic algorithm?

A) An integer values B) A square matrix

C) An array of characters (i.e. a string) D) All of these

(XLVII) The Advanced Encryption Standard (AES) was designed

A) National Institute of Standards and Technology B) IBM

C) HP D) Intel

(XLVIII) This is an encryption/decryption key known only to the party or parties that exchange secret messages.

A) e-signature B) digital certificate

C) private key D) security token

(XLIX) A transposition cipher reorders (permutes) symbols in a

A) block of packets B) block of slots

C) block of signals D) block of symbols

(L) The Caesar cipher is a _____ cipher that has a key of 3

A) transportation B) additive

C) shift D) none of these

(LI) Cryptography, a word with Greek origins, means

A) Corrupting Data B) Secret Writing

C) Open Writing D) Closed Writing

(LII) Cryptographic hash function takes an arbitrary block of data and returns _____

A) fixed size bit string B) variable size bit string

C) both fixed size bit string and variable size bit string D) variable sized byte string

(LIII) The initial value of the LFSR is called the _____

A) seed B) data

C) Zero value D) none of these

(LIV) A cryptographic hash function (CHF) is a

A) mathematical algorithm that maps data of arbitrary size to a bit array of a fixed size B) mathematical algorithm that maps data of fixed size to a bit array of a arbitrary size

C) mathematical algorithm that maps data of binary size to a bit array of a binary size D) none of these

(LV) Public key cryptography is a _____ cryptosystem.

A) Symmetric B) Asymmetric

C) Symmetric & Asymmetric both D) None of these

(LVI) Which of the following security attacks is not an active attack?

A) Masquerade B) Modification of message

C) Denial of service D) Traffic analysis

(LVII) Which one of the following is a cryptographic protocol used to secure HTTP connection?

A) stream control transmission protocol (SCTP) B) transport layer security (TLS)

C) explicit congestion notification (ECN) D) resource reservation protocol

(LVIII) The cipher feedback (CFB) mode was created for those situations in which we need to send or receive r bits of

A) Frames B) Pixels

C) Data D) Encryption

(LIX) The _____ cipher is the simplest monoalphabetic cipher. It uses modular arithmetic with a modulus of 26.

A) transportation B) additive

C) shift D) none of these

(LX) In Cryptography, when text is treated at the bit level, each character is replaced by

A) 4 Bits B) 6 Bits

C) 8 Bits D) 10 Bits