2/53

2504N045

Candidate's Seat No :________

M.Sc. I.T. (Sem.-2) (N.S.) Examination

MSCNS 410

Fundamentals of Cryptography

April 2019

Time : 2-30 Hours] [Max. Marks : 70

Instructions:-

1) Figures to the right indicates full marks

2) Neat diagrams must be drawn wherever necessary.

Q:1 Select right answer. **[14]**

1. In Asymmetric-Key Cryptography, two keys, e and d, have a special relationship to
a) Others b) Data
c) Keys d) Each other

2. MITM attack can endanger security of Diffie-Hellman method if two parties are not
a) Authenticated b) Joined
c) Submit d) Separate

3. We use Cryptography term to transforming messages to make them secure and immune to
a) Change b) Idle
c) Attacks d) Defend

4. A straight permutation cipher or a straight P-box has same number of inputs as
a) cipher b) Frames
c) Outputs d) Bits

5. An asymmetric-key (or public-key) cipher uses
a) 1 Key b) 2 Key
c) 3 Key d) 4 Key

6. DES stands for
a) Data Encryption Standard b) Data Encryption Subscription
c) Data Encryption Solutions d) Data Encryption Slots

7. Heart of Data Encryption Standard (DES), is the
a) Cipher b) Rounds
c) Encryption d) DES function

8. Substitutional ciphers are
a) Monoalphabatic b) Sami alphabetic
c) polyalphabetic d) both a and c

9. Shift cipher is sometimes referred to as the
a) Caesar cipher b) Shift cipher
c) cipher d) cipher text

P.T.O

N045-2

10. In Cryptography, original message, before being transformed, is called

a) Simple Text b) Plain Text

c) Empty Text d) Filled Text

11. An encryption algorithm transforms plaintext into

a) Cipher text b) Simple Text

c) Plain Text d) Empty Text

12. A substitution cipher substitutes one symbol with

a) Keys b) Others

c) Multi Parties d) Single Party

13. Cryptography algorithms (ciphers) are divided into

a) two groups b) four groups

c) one single group d) None

14. A substitution cipher replaces one symbol with

a) same symbol b) provide two symbols for each

c) another d) All of them

Q:2 **[14]**

1) Explain RSA Algorithm with example. [7]

2) Explain Symmetric & asymmetric algorithm. [7]

OR

2) What is JAVA cryptography Explain with Example.

Q:3 **[14]**

1) What is Vigenere cipher? Explain vigenere cipher using Example. [7]

2) What is Playfair cipher? Explain Playfair cipher using example. [7]

OR

2) Write the principal of security & Explain in detail.

Q:4 **[14]**

1) Explain Password Authentication mechanisms & comparisons. [7]

2) Explain MD5 Algorithm with implementation step. [7]

OR

2) What is KDC? Explain with example.

Q:5 **[14]**

1) What is cryptography? Explain with timeline. [7]

2) Explain SHA-1 Algorithm with step. [7]

OR

2) Draw neat Diagram of DES algorithm & Explain.

—X—