



Name :

Roll No. :

Invigilator's Signature :

CS/M.Tech(ECE-COMM)/SEM-2/MCE-204A/2012
2012

CRYPTOGRAPHY & NETWORK SECURITY

Time Allotted : 3 Hours

Full Marks : 70

The figures in the margin indicate full marks.

*Candidates are required to give their answers in their own words
as far as practicable.*

Answer Question No. 1 and any *four* from the rest.

1. Choose the correct alternatives for the following : $7 \times 2 = 14$

i) The encryption of the text "A MAT" using Caesar cipher is

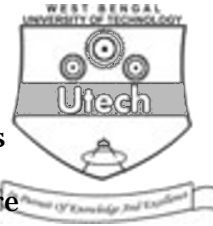
- | | |
|----------|-------------------|
| a) M TAA | b) D PDW |
| c) C OCV | d) none of these. |

ii) Cryptography is applied in

- | | |
|---------------------|------------------|
| a) military | b) E-Commerce |
| c) Network Security | d) all of these. |

iii) The ROT-13 Cipher is an example of

- | |
|--------------------------------|
| a) monoalphabetic substitution |
| b) polyalphabetic substitution |
| c) polygraphic substitution |
| d) none of these. |



- iv) An example of the transposition cipher is
- a) Grille
 - b) Vigenere
 - c) Caesar
 - d) None of these.
- v) The fifth layer in OSI model and in TCP/IP protocol are
- a) Presentation, Application
 - b) Application, Transport
 - c) Session, Application
 - d) Presentation, Transport.
- vi) Wired and wireless communications are secured using the respective security mechanism
- a) WPA, AES
 - b) AES for both
 - c) AES, WPA
 - d) WPA for both.
- vii) The CIA triad is a model of
- a) cracking encryption algorithms
 - b) digital signature
 - c) crypto-Linguistics
 - d) security mechanisms.
2. What is Cryptography ? Define Crypto system. Encrypt the following message "ATTACK BEGINS AT DAWN HOLD TIGHT" using a Route Cipher and the Key given as : Spiral Inwards, Clockwise, Starting from top Right. If a set X has five elements, then obtain the value of the set of all bijections. What is an Anagram ? Explain with an example.



3. A confidential message to be secured is given as “WE ARE DISCOVERED FLEE AT ONCE”. Encrypt the above message using a Columnar Transposition with the keyword ZEBRAS. Assume that another cryptographer encrypts the above confidential message with a different keyword TOMATO. Obtain the cipher text. What is this cryptosystem termed ? What is meant by Disrupted Transposition cipher ?
4. Briefly enumerate on the core principles of Network security. What is meant by Passive Attacks on a system ? Compare between Message Release and Traffic Analysis. Which type of Attack is easier to detect — Passive or Active and why ?
5. Explain in detail the operation of advanced encryption standard encryption and decryption process. Compare between AES and Data Encryption Standard (DES). What is the International Data Encryption Algorithm (IDEA) ?
6. Explain the Cipher Block Chaining Mode of operation for Block ciphers. Briefly discuss the encryption and decryption operation of RSA Algorithm. What is meant by Public and Private keys ? State an important application area of the public key cryptography.



7. Which one is more feasible, a fixed size digest or variable sizes digest ? Can we use a conventional lossless compression method as a hashing function ? A message is made of 10 numbers between 00 and 99. A Hash Algorithm creates a digest out of this message by adding all numbers modulo 100. The resulting digest is a number between 00 and 99. Examine whether this algorithm meets any of the three criteria required for a hash function.
8. Write short notes on any *two* of the following :
- a) Hashed Message Authentication Code
 - b) Comparison of Conventional and Digital Signatures
 - c) Replay Attack
 - d) Data Encryption Standard.

=====