St. Thomas' College of Engineering & Technology

B. Tech. 7th Semester, 1st Internal Examination, May 2021

Cryptography & Network Security(CS801D)

Full Marks : 25 **Time : 50 Min.**

Group – A

Choose the correct option(s) from the list of options provided with each part of the following question. **(1×10=10)**

1. i) The _____ attack is related to availability.
   a) interception
   b) fabrication
   c) modification
   d) interruption

   ii) A _____ replicates itself by creating its own copies, in order to bring the network to a halt.
   a) virus
   b) worm
   c) trojan horse
   d) bomb

   iii) A probabilistic study for implementing different attacks based on the knowledge of English language is performed by a cryptanalyst when he/she encounters a ciphertext that has been encrypted using
   a) homophonic substitution cipher
   b) polygram substitution cipher
   c) mono-alphabetic cipher
   d) polyalphabetic substitution cipher

   iv) _____ increases the redundancy of plaintext by spreading it across rows & columns.
   a) confusion
   b) diffusion
   c) both (a) & (b)
   d) neither of them

   v) DES encrypts blocks of _____ bits.
   a) 32
   b) 56
   c) 64
   d) 128

   vi) CHAP stands for?
   a) Challenge Handshake authentication protocol
   b) Challenge Hardware authentication protocol
   c) Circuit Hardware authentication protocol
   d) Circuit Handshake authentication protocol

vii) In asymmetric key cryptography, The private key _____.
a) must be distributed
b) must be shared with everyone
c) must remain secret with an individual
d) none of the above

viii) The full form of Malware is _____
a) Malfunctioned Software
b) Multipurpose Software
c) Malicious Software
d) Malfunctioning of Security

ix) When there is an excessive amount of data flow, which the system cannot handle, _____ attack takes place.
a) Database crash attack
b) DoS (Denial of Service) attack
c) Data overflow Attack
d) Buffer Overflow attack

x) This attack can be deployed by infusing a malicious code in a website's comment section. What is "this" attack referred to here?
a) SQL injection
b) HTML Injection
c) Cross Site Scripting (XSS)
d) Cross Site Request Forgery (XSRF)

Group – B

2. a) Citing specific examples explain the concepts of Phishing & Pharming.
b) Explain the concept of Vignere Cipher. (3+2)

3. a) Consider a scheme involving the replace of alphabets as follows:

Original	A	B	C	…	X	Y	Z
Changed to		Z	Y	X	…	C	B	A

If Alice sends a message EWPYMOWZAYQ to Bob, what will he infer from this?
b) Discuss the differences between Confusion & Diffusion. (3+2)

4. Distinguish between Symmetric & Asymmetric Key cryptographic techniques by citing suitable examples & drawing appropriate diagrams whenever necessary. (5)

OUTCOME BASED EDUCATION (OBE)						
CO mapping With Bloom's Level						
Question No.	**Q1**	**Q2**		**Q3**		**Q4**
		a	**b**	**a**	**b**	
Course Outcome	**1**	**1**	**2**	**2**	**2**	**3**
Bloom's Level (in fig)	**1**	**3**		**5**		**4**