SVKM's
Dwarkadas J. Sanghvi College of Engineering
Acad .Year 2022-2023
YEAR III / Semester VI

Program: B.Tech in Computer Engineering
Subject/Course: Information Security
Date: 12.08.2023

Max. Marks: 75
Time: 10:00-13:00
Duration: 03:00 Hrs

RE-EXAMINATION

Instructions: Candidates should read carefully the instructions printed on the question paper and on the cover page of the Answer Book, which is provided for their use.

(1) This question paper contains **TWO** pages.
(2) All Questions are Compulsory.
(3) All questions carry equal marks.
(4) Answer to each new question is to be started on a fresh page.
(5) Figures in the brackets on the right indicate full marks.
(6) Assume suitable data wherever required, but justify it.
(7) Draw the neat labelled diagrams, wherever necessary.

Question No.		Max. Marks
Q1(a)	Explain in details DES algorithm? Discussed the significance following attack on DES algorithms. a) Brute Force Attack. b) Differential Cryptanalysis c) Linear Cryptanalysis. **OR** Explain in details Kerberos system that supports authentication in distributed system.	10 10
Q1(b)	Discussed in details verification process of Certificate Authority (CA)'s signature on certificate.	05
Q2 (a)	Explain key generation technique with diagram in simplified DES (S-DES) algorithm. Find out First round key k1 (8 bit) and round two k2 (8 bit) using simplified key generation technique.. Input Value (Cipher Key) to algorithm is 1011100110 (10 bit) Straight P Box	10

1	2	3	4	5	6	7	8	9	10
3	5	2	7	4	10	1	9	8	6

	Compression P Box 6 | 3 | 7 | 4 | 8 | 5 | 10 | 9	
Q2 (b)	Explain the strength of AES algorithm ? Discuss AES algorithms following steps with example. a)Substitution. b) Inv. Substitution	05
Q3 (a)	Discussed in details about birthday problem.	05
Q3 (b)	What do you mean message authentication code ? Explain the working of HMAC. **OR**	10
Q3 (b)	Explain in detail MD5 algorithm along with its vulnerabilities and attacks.	10
Q4 (a)	Explain ICMP and UDP flooding attack along with their mitigation techniques. **OR**	10
Q4 (a)	Explain IPSec protocol working in following modes. a) Transport mode. b) Tunnel mode.	10
Q4 (b)	Using RSA algorithm calculate following values , if p=7 and q=11 a) Public key (e,n) b) Private key (d,n) c) Encrypted value for input 4	05
Q5.	Write short note on any three. i. Buffer Overflow ii. SQL injection iii. Bots and Rootkits iv. Cross site scripting	 05 05 05 05