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: 29.05.2023

Max. Marks: 75
Time: 09:00-12:00
Duration: 03:00 Hrs

FINAL 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)	Convert following input text into cipher form using Mix Column technique of AES algorithm. **Input Text** 2a 4c 3b 5d **Cont. Matrix** 02 03 01 02	10
	OR	
	Using Knapsack problem, a) Generate public key from private key {1,2,4,9 } b) Convert following data into cipher text. 1) 0101 2) 0011 c) Convert Cipher Text into plain text.	10

<table>
<tr><td>Q1(b)</td><td>Discuss in details how e mail contents is protected by PGP protocol.</td><td>05</td></tr>
<tr><td>Q2 (a)</td><td>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
<table><tr><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td></tr><tr><td>4</td><td>6</td><td>3</td><td>10</td><td>5</td><td>9</td><td>2</td><td>8</td><td>7</td><td>1</td></tr></table>Compression P Box
<table><tr><td>6</td><td>3</td><td>7</td><td>4</td><td>8</td><td>5</td><td>10</td><td>9</td></tr></table></td><td>10</td></tr>
<tr><td>Q2 (b)</td><td>Explain ARP protocol along with its vulnerabilities.</td><td>05</td></tr>
<tr><td>Q3 (a)</td><td>Explain the steps of message digest generation in MD5 algorithm.</td><td>05</td></tr>
<tr><td>Q3 (b)</td><td>What do you mean message authentication code ? Explain the working of HMAC.
OR</td><td>10</td></tr>
<tr><td>Q3 (b)</td><td>Explain working of SHA and also discuss the difference between Md5 and SHA.</td><td>10</td></tr>
<tr><td>Q4 (a)</td><td>What do you mean by IP spoofing ? Explain the defense mechanism of IP Spoofing attack.
OR</td><td>10</td></tr>
<tr><td>Q4 (a)</td><td>Explain Tunnel mode of IPSec protocol ? Justify, How Encapsulating Security Payload (ESP) provides better security than AH (Authentication Header).</td><td>10</td></tr>
<tr><td>Q4 (b)</td><td>Using RSA algorithm calculate following values , if p=5 and q=7
a) Public key (e,n)
b) Private key (d,n)
c) Encrypted value for input 5</td><td>05</td></tr>
<tr><td>Q5.</td><td>Write short note on any three.
i. SYN Flooding Attack
ii. SQL injection
iii. Salami Attack.
iv. IDS</td><td>
05
05
05
05</td></tr>
</table>