SVKM
Mithibai College (Arts, Sci & Comm)

Programme: B.Sc (Computer Science) - (CBCGS)
Year: III/Semester V(Exam Year: 2023-2024)
Subject: INFORMATION AND NETWORK SECURITY
Date: 21 Oct 2023 **Time: 10:30 am to 01:00 pm (02:30 Hrs.)**
Max. Marks: 75

FINAL EXAMINATION (Acad. Year:**2023-2024)**

Instructions:

1. This question paper contains 2 pages.
2. Answer to each new question to be started on a fresh page.
3. Figure in right hand side indicates full marks

Q1.	**ATTEMPT ANY 3 FROM THE FOLLOWING**	**(15)**
A	Describe OSI security architecture and principles of security.	**5**
B	State and explain any 2 modes of operations on Block Cipher with a diagram.	**5**
C	Perform encryption and decryption using RSA Algorithm for the following. P=17; q=11; e=7; M=88.	**5**
D	Define transposition cipher. Illustrate rail-fence cipher technique using suitable example.	**5**
Q2.	**ATTEMPT ANY 3 FROM THE FOLLOWING**	**(15)**
A	What is Targeted Malicious code? Discuss Salami Attack in detail with an example.	**5**
B	Explain the various Controls against program threats.	**5**
C	What is a worm? How it is different from virus explain with an example.	**5**
D	Describe the following types of malicious programs: a) Trojan Horses **b)** Backdoor	**5**
Q3.	**ATTEMPT ANY 3 FROM THE FOLLOWING**	**(15)**
A	Discuss SHA-512 algorithm.	**5**
B	Describe the contents of a Digital certificate.	**5**
C	What is MAC? Explain HMAC.	**5**
D	Describe IEEE 802.11 Wireless Security with Wi-Fi Protected Access (WPA).	**5**
Q4.	**ATTEMPT ANY 3 FROM THE FOLLOWING**	**(15)**
A	Discuss IPSec authentication header.	**5**
B	What is the purpose of a firewall? Explain firewall configurations.	**5**
C	What is the purpose of PGP? Discuss any three PGP operations.	**5**
D	Explain Intrusion Detection System in detail.	**5**
Q5.	**ATTEMPT ANY 3 FROM THE FOLLOWING**	**(15)**

A Discuss the Denial of Service attack with an example. **5**

B Would message integrity on its own ensure that the contents of a message are not changed during transit? Does something more need to be done? **5**

C Summarize Demilitarized zone. **5**

D Discuss the phases of Secure Socket Layer. **5**

SVKM'S
Mithibai College of Arts, Chauhan Institute of Science &
Amrutben Jivanlal College of Commerce and Economics (Autonomous)
Academic Year (2022-23)
Class: Third Year Semester: V

Program: B.Sc. Computer Science	**Max. Marks: 75**
Course Name: Information & Network Security	**Time: 10:30 a.m to 1:00 p.m**
Course Code: USMACS503	**Duration: 2 hrs 30 minutes**
Date: 18 OCT 2022	

REGULAR EXAMINATION

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

1) **This question paper contains 2 page.**
2) **Answer to each new question to be started on a fresh page.**
3) **Figures in brackets on the right hand side indicate full marks.**
4) **Assume Suitable data if necessary**
5) **Use of simple calculator is allowed.**

Q-1 Answer Following (Any Three) **[21]**

a. Explain principles of security with possible attack example on each of them. [07]

b. Consider the message "THIS IS A MESSAGE TO SHOW HOW A COLUMNAR TRANSPOSITION WORKS". Apply simple columnar transposition technique to encrypt it. Detail the steps. [07]

c. Differentiate between block cipher and stream cipher. Explain any two modes of operations for block cipher. [07]

d. Explain single round function of DES with suitable diagram and key generation. [07]

Q-2 Answer Following (Any Three) **[21]**

a. Brief Diffie-Hellman key exchange algorithm. Person A and B want to establish a secret key using the diffie-Hellman key exchange protocol. Assuming the values as n=11, g=5, x=2 and y=3, find out the values of A, B and secret key. [07]

b. Discuss hash function with its requirements. Explain birthday paradox and attack with respect to hash function. [07]

c. Explain kerberos in details. [07]

d. Describe the contents of Digital certificate. [07]

Q-3 Answer Following (Any Three) **[21]**

a. Discuss the working of SSL record and alert protocol. [07]

b. What is PGP protocol used for? Explain its operations. [07]

c. What is ESP used for? Explain ESP header format in detail. [07]

d. Describe types of firewall. [07]

Q-4 Answer Following (Any Three) **[12]**

a. Use the Vigenere cipher with keyword 'WEALTH' to encipher the message, 'Computer'. [04]

b. Is a message authentication code(MAC) function is similar to encryption? Does MAC provide authentication or confidentiality? Justify your answer [04]

c. What is DMZ? Explain in brief. [04]

d. Discuss active attack and passive attack. [04]

Extra +15

13 JAN 2023

SVKM'S
Mithibai College of Arts, Chauhan Institute of Science &
Amrutben Jivanlal College of Commerce and Economics (Autonomous)
Academic Year (2022-23)
Class:Third Year Semester: V

Program: B.Sc. Computer Science	Max. Marks: 75
Course Name: Information & Network Security	Time: 10:30 a.m to 1:00 p.m
Course Code: USMACS503	Duration: 2 hrs 30 minutes
Date:	

RE(-- - EXAMINATION

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

1) This question paper contains 2 page.
2) Answer to each new question to be started on a fresh page.
3) Figures in brackets on the right hand side indicate full marks.
4) Assume Suitable data if necessary
5) Use of simple calculator is allowed.

Q-1 Answer Following (Any Three) **[21]**

a. Describe OSI security architecture and principles of security. [07]

b. Discuss playfair cipher. Generate cipher text for "REPUBLIC DAY IS IN JANUARY" using LOTUS as the key. [07]

c. Explain general structure of DES algorithm with its key generation. [07]

d. Summarize various modes of operations on block cipher. [07]

Q-2 Answer Following (Any Three) **[21]**

a. Explain Diffie-Hellman algorithm. For Diffie-Hellman algorithm, two publicly known numbers are prime number 353 and 3. Person A selects the random integer 97 and Person B selects 233. Compute common secret key. [07]

b. Discuss SHA-512 algorithm. [07]

c. Summarize Kerberos Authentication System. [07]

d. Describe X.509 authentication service. [07]

Q-3 Answer Following (Any Three) **[21]**

a. Where SSL is placed in TCP/IP? Describe SSL handshake protocol in detail. [07]

b. What is the purpose of PGP? Explain PGP operations. [07]

c. Discuss IPSec authentication header. [07]

d. Explain and compare packer filter and application gateways. [07]

Q-4 Answer Following (Any Three) **[12]**

a. Encrypt the message “MOONMISSION IS TESTED” with the key “KEYWORD” using simple columnar transposition. [04]

b. Is a message authentication code(MAC) function is similar to encryption? Does MAC provide authentication or confidentiality? Justify your answer [04]

c. Explain different types of intruders. [04]

d. What is Digital signature? Explain with figure. [04]