SHRIMATHI DEVKUNVAR NANALAL BHATT VAISHNAV COLLEGE FOR WOMEN (AUTONOMOUS)
(Affiliated to the University of Madras and Re-accredited with 'A+' Grade by NAAC)
Chromepet, Chennai — 600 044.
M.Sc. END SEMESTER EXAMINATION APRIL/NOV - 2021
SEMESTER - III
20PCSET3CN3 -Cryptography and Network Security

Total Duration : 3 Hrs		**Total Marks : 75**	
MCQ	: 30 Mins	MCQ	: 15
Descriptive	: 2 Hrs.30 Mins	Descriptive	: 60

Section B

Answer any **SIX** questions $(6 \times 5 = 30$ Marks)

1. Explain the two basic functions used in encryption algorithms.
2. Describe the Conventional encryption model.
3. Show that DES decryption is, in fact, the inverse of DES encryption.
4. Briefly explain the Diffie Hellman Key Exchange algorithm.
5. Interpret the function for message authentication code.
6. Explain the arbitrated digital signature techniques.
7. With a neat diagram, describe the IP security architecture.
8. Illustrate with example, the Wireless application protocol.

Section C

Part A

Answer any **TWO** questions $(2 \times 10 = 20$ Marks)

9. Give the structure of AES. Explain how Encryption/Decryption is done in AES.
10. Using the playfair matrix:

M	O	N	A	R
C	H	Y	B	D
E	F	G	I	K
L	P	Q	S	T
U	V	W	X	Z

Encrypt the message: "The enemy must be stopped".

11. Evaluate the operations for Secure Hash algorithm.
12. In detail explain , the functional flow of DKIM.

Part B

Compulsory question $(1 \times 10 = 10$ Marks)

13. Apply RSA algorithm and compute encryption and decryption to the system with p=3 q=11 e=7 and M=5. Explain RSA algorithm.