

**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 EXAMINATIONS NOVEMBER - 2022

SEMESTER - III

20PCSET3CN3 - Cryptography and Network Security

Total Duration : 2 Hrs 30 Mins.

Total Marks : 60

Section A

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

1. What is the difference between passive and active security threats?
2. Explain the types of attacks on encrypted messages.
3. Describe the concepts of DES encryption algorithm.
4. What is the difference between the AES decryption algorithm and the equivalent inverse cipher?
5. List out the attacks to RSA.
6. Determine the characteristics that are needed in a secure hash function.
7. Describe the set of criteria used by NIST to evaluate SHA-3 candidates.
8. Examine the five principal services provided by PGP.

Section B

Part A

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

9. Explain about OSI security architecture.
10. Sketch the detailed structure of AES Diagnose it and explain.
11. Appraise the classification of authentication function in detail.
12. Explain the architecture of IP Security.

Part B

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

13. Using RSA algorithm, Find n, d if $p=11$, $q=3$, $e=3$. Encrypt "Hello World" Message.

**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 EXAMINATIONS NOVEMBER - 2022

SEMESTER - III

20PCSET3CN3 - Cryptography and Network Security

Total Duration : 2 Hrs 30 Mins.

Total Marks : 60

Section A

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

1. What is the difference between passive and active security threats?
2. Explain the types of attacks on encrypted messages.
3. Describe the concepts of DES encryption algorithm.
4. What is the difference between the AES decryption algorithm and the equivalent inverse cipher?
5. List out the attacks to RSA.
6. Determine the characteristics that are needed in a secure hash function.
7. Describe the set of criteria used by NIST to evaluate SHA-3 candidates.
8. Examine the five principal services provided by PGP.

Section B

Part A

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

9. Explain about OSI security architecture.
10. Sketch the detailed structure of AES Diagnose it and explain.
11. Appraise the classification of authentication function in detail.
12. Explain the architecture of IP Security.

Part B

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

13. Using RSA algorithm, Find n, d if $p=11$, $q=3$, $e=3$. Encrypt "Hello World" Message.
