(2 ½ Hours) **[Total Marks: 75]**

N.B. 1) All questions are compulsory.
2) Figures to the right indicate marks.
3) Illustrations, in-depth answers and diagrams will be appreciated.
4) Mixing of sub-questions is not allowed.

Q. 1 **Attempt ANY FOUR from the following:** **(20M)**

(a) Discuss OSI Security model architecture highlighting the attacks, mechanisms and services.
(b) Differentiate between active and passive attacks.
(c) Encrypt the following using play fair cipher using the keyword MONARCHY. " SWARAJ IS MY BIRTH RIGHT". Use X as filler character.
(d) Explain in detail the transformations take place in AES encryption procedure.
(e) Describe the working principle of DES with a neat diagram.
(f) Perform encryption and decryption using RSA Algorithm for the following. P=7; q=11; e=17; M=8

Q. 2 **Attempt ANY FOUR from the following:** **(20M)**

(a) Discuss how Diffie Hellman key exchange algorithm is a practical method for public exchange of a secret key?
(b) What is Message Authentication code? Explain its functions and basic uses.
(c) Explain key management and distribution in detail.
(d) What is the purpose of digital signature? Explain its properties and requirements.
(e) Explain how authentication is performed in Kerberos.
(f) What is Public Key certificate? Explain its usage with X.509 certificates.

Q. 3 **Attempt ANY FOUR from the following:** **(20M)**

(a) Explain how email messages are protected using S/MIME signing and encryption?
(b) With a neat sketch explain the IPSec scenario and IPSec Services.
(c) Explain different Web security requirements.
(d) Discuss Intrusion detection in detail.
(e) Give the taxonomy of malicious programs. Define each one.
(f) What is a firewall? What is the need for firewalls? What is the role of firewalls in protecting networks?

Q. 4 **Attempt ANY FIVE from the following:** **(15M)**

(a) Compare stream cipher with block cipher with example.
(b) Differentiate MAC and Hash function.
(c) Why is asymmetric cryptography bad for huge data? Specify the reason.
(d) What is dual signature? What is its purpose?
(e) Define the role of different SSL protocols.
(f) What is meant by SET? What are its features?

****