MAY 2015 **P/ID 77820/PMG01**

Time : Three hours Maximum : 100 marks

PART A — (5 × 6 = 30 marks)

Answer any FIVE questions.

1. List the key features of secure transaction.
2. What are the approaches to threat modeling?
3. State the importance of generic technology in secure web applications.
4. What are the important steps for securing web application?
5. What is OWASP? Explain the purpose of OWASP.
6. What are the risks in interfacing with payment gateways?
7. What is digital forensics? How does it differ from data recovery?
8. Define cipher. What are the difference between stream cipher and block cipher?

PART B — (5 × 10 = 50 marks)

Answer any FIVE questions.

9. What is cross site scripting? How to prevent cross site scripting security issues?

10. Describe the various phases of web development life cycle.

11. Explain the types of honeypot. What are the ethical issues concerning honeypot?

12. Explain various key management techniques.

13. Why is it critical to perform periodic web application vulnerability assessments and penetration tests?

14. Who can attack cryptosystems? Explain different categories of attacks on cryptosystems.

15. What are the different types of Data Encryption Standard? How is the security aspect maintained in DES?

16. Explain the digital forensic capability on web applications.

PART C — (1 × 20 = 20 marks)

Compulsory.

17. You intercept the coded message 'DXM SCE DCCUVGX", which was enciphered using an affine map on diagraphs in a 30 letter alphabet, in which A - Z have numerical equivalents 0 - 25, blank = 26, ? = 27, ! = 28, ' = 29. A frequency analysis shows that the most common digraphs in earlier ciphertexts are "M", "U", and "IH", in that order.

Suppose that in the English language the most frequently occurring digraphs (in this particular 30 letter alphabet) are 'E', 'S', and "T" in that order.

(a) Find the deciphering key and read the message.

(b) Find the enciphering key and encrypt the message "YES I'M JOKING!".
