KINGS

COLLEGE OF ENGINEERING

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

QUESTION BANK

SUBJECT CODE: CS1015 **YEAR : IV**

SUBJECT NAME: INFORMATION SECURITY **SEM : VIII**

UNIT I - INTRODUCTION TO INFORMATION SECURITY

PART – A (2 MARKS)

1. What is information security?
2. What are the types of attack? Compare.
3. What is meant by top-down approach to security implementation? Give its advantages.
4. What is meant by bottom-up approach to security implementation? Give its disadvantages.
5. What type of security was dominant in the early years of computing?
6. What are the three components of C.I.A. triangle? What are they used for?
7. What is security blue print?
8. What is the difference between a threat agent and a threat?
9. What is vulnerability?
10. Who is involved in the security development life cycle? Senior Management: Chief.
11. Name the multiple layers of security in a successful organization.
12. Define file-hashing.
13. Define E-mail Spoofing.
14. Give the measures that can be taken to protect confidentiality of information.
15. What are the critical characteristics of information?

16. When can a computer be a subject and an object of an attack respectively?

PART-B (16 MARKS)

1. Describe the critical characteristics of information. How are they used in the study of computer security? (16)
2. Briefly explain the components of an information system and their security. How will you balance security and access? (16)
3. (a) Describe the system development life cycle? (4)

   (b) Explain the security system development life cycle? (12)
4. What is Information security? Explain the NSTISSC security model and the top-down approach to security implementation. (16)

UNIT II – SECURITY INVESTIGATION

PART – A (2 MARKS)

1. Why is information security a management problem?
2. Why is data the most important asset an organization possesses?
3. How can a Service Level Agreement (SLA) provide a safeguard for Internet or web hosting services?
4. What is software piracy? Name two organizations that investigate allegations of software abuse.
5. Name the two categories of hackers and differentiate between them.
6. Who is a cyberactivist?
7. Who is a cyberterrorist?
8. How does a threat to information security differ from an attack?
9. What is a threat?
10. Define malware. Give examples.
11. In what way does the DDoS differ from the DoS attack?
12. How do worms differ from viruses?
13. What is spoofing?
14. What are the types of password attack?
15. What is the difference between criminal law & civil law?

16. What is tort law?
17. What are the primary examples of public law?
18. What is a policy? How does it differ from law?
19. How does tort law differ from public law?
20. Which law amended the computer Fraud and Abuse Act of 1986, and what did it change?
21. What are the three general categories of unethical and illegal behaviour?
22. What is DMCA?
23. What does CISSP stand for?

PART-B

1. (a) Explain the four important functions of information security in an organization? (8)

   (b) Explain the ethical concepts in Information Security and the deterrence to illegal and unethical behaviour. (8)

2. What is a threat? Explain in detail the various groups of threats facing an organization. (16)

3. Define an attack. Describe attack replication vectors & major types of attacks. (16)

4. Write detailed notes on Codes of Ethics, Certifications & Professional Organisations. (16)

5. Explain the relevant laws in Information Security in detail. (16)

UNIT III – SECURITY ANALYSIS

PART –A (2 MARKS)

1. What is risk management?
2. Who are responsible for risk management in an organization?
3. What are the four risk strategies for controlling risk?
4. Which community of interest usually takes the lead in Information security risk management? Why?
5. What is the formula for calculating risk?
6. Define risk avoidance?

7. Define risk transference?
8. Define risk mitigation?
9. What are the three types of plans that are involved in mitigation of risk?
10. Name three common methods of risk avoidance?
11. What is the difference between intrinsic value and acquired value?
12. What is annual loss expectancy?
13. What is cost benefit analysis?
14. What is the definition of single loss expectancy?
15. What is the difference between benchmarking and base lining?
16. What are vulnerabilities?
17. What is risk assessment?
18. What is a hot site? How is this useful in risk mitigation?
19. Compare and contrast preventive and detective controls.
20. What is a Delphi technique?
21. Define risk appetite.

PART-B (16 MARKS)

1. (a). What are the four basic steps in risk management? Describe. (8)
   (b). What are access controls and explain their types? (8)
2. Elaborate on
   a) Asset Identification & Valuation (8)
   b) Data Classification & Management (8)
3. Describe in detail the process of risk identification. (16)
4. Elaborate on risk assessment and the documentation of its results. (16)
5. What are the risk control strategies that guide an organization? Elaborate. (16)
6. Explain the components of asset valuation? (16)
7. Explain the various feasibility studies considered for a project of information security controls and safeguards? (16)

UNIT IV -LOGICAL DESIGN

PART-A (2 MARKS)

1. Differentiate between a mission & vision of an organization.
2. What is information security policy?
3. What is information security blueprint framework?
4. What is the difference between a policy, standard and procedure?
5. Define IRP.
6. Define DRP.
7. Define BCP.
8. What is crisis management?
9. What are the inherent problems with ISO 17799, and why hasn't the U.S. adopted it?
10. What are the two major components of the sphere of security?
11. What are the levels of testing strategies involved in incident response plan?
12. Mention Pipkin's three categories of incident indicators.
13. When does an incident become a disaster?
14. Write short notes on a mutual agreement.
15. State the options for Off-site Disaster Storage.
16. What is an Alert Roster? Mention its types?
17. What three outcomes or end cases you should prepare when creating attack success scenarios?
18. What are the types of ISSP Documents?

PART –B (16 MARKS)

1. Define a policy. What are the types of information security policies? Explain. (16)
2. Explain briefly
   a) VISA Security model (8)
   b) ISO17799/BS 7799 (8)
3. Explain in detail the NIST Security model? (16)
4. What are the components are used in design of security architecture? Explain. (16)
5. What are the types of contingency planning? Explain. (16)

6. Explain the major steps involved in contingency planning. (16)

7. State the four phases of an incident response? Describe them. (16)

8. Write short notes on

   a) DRP (8)

   b) BCP (8)

UNIT V – PHYSICAL DESIGN

PART –A (2 MARKS)

1. What is firewall?
2. What are packet filtering firewalls?
3. What are Application-Level Firewalls?
4. What are Stateful Inspection Firewalls?
5. What are Dynamic Packet Filtering Firewalls?
6. What is RADIUS?
7. What is network fingerprinting?
8. What are the main components of cryptology?
9. What is a Screened Subnet Firewall?
10. Define NAT.
11. What is a host based IDS?
12. How does false reject rate differ from false accept rate?
13. What are the two protocols designed to enable secure communications across the internet?
14. State the main components of cryptology.
15. What are the different types of attacks on cryptosystems?
16. In what ways the sophisticated heat sensor operates in the thermal detection systems?
17. What are the basic types of Fire detection systems?

PART-B (16 MARKS)

1. Discuss the generation of firewalls? (16)
2. Describe the structure of firewall architecture? (16)

3. Explain the various types of Intrusion Detection Systems. (16)
4. Explain in detail the cryptography and encryption based solutions. (16)
5. Explain the key difference between symmetric and asymmetric encryption with suitable examples. (16)
6. Briefly explain the components of cryptology. (16)
7. Discuss some of the popular cryptographic algorithms. (16)
8. Write short notes on various access controls used for providing physical security. (16)
9. Describe the various methods of power management & conditioning. (16)