

System Security – May 2005

Time : 3 Hrs.]

[Marks : 100

- N.B. :**
- (1) Q. No. 1 is compulsory.
 - (2) Solve any **five** of the remaining.
 - (3) Use of calculator is allowed.

1. The following questions are based on a scenario in which encrypted data are passed between Alice and Bob using the RSA algorithm. Alice's public key is {17,321} and Bob's public key is {5, 321}. Assume that no one knows the private keys but the original owners. [20]
 - (a) Encrypt the message $M = 7$ using Bob's public key.
 - (b) What should Alice have to do to decrypt the message from part a?
 - (c) What would Bob have to do to decrypt the message from part a?
 - (d) What is Alice's private key?
 - (e) What is Bob's private key?
2. Design and explain a policy to exchange the session key " K_{session} " using public key cryptography. It should support the followings. [16]
 - (a) Confidentiality
 - (b) Integrity
 - (c) authentication of sender
 - (d) non - repudiation on sender's and receiver's side
 - (e) No possibility of reply attack.
3. Answer the following. [8]
 - (a) Preserving confidentiality, integrity and availability of data is a restatement of the concern over interruption, interception, modification and fabrication. How do first three concept relate to the last four ? [8]
 - (b) Explain the use of temporal separation and physical separation for security in computing environment. [8]
4. Answer the following. [6]
 - (a) Every covert timing channel can be transformed into an equivalent covert storage channel. Explain how this transformation can be done. [6]
 - (b) List nonmalicious program errors. Explain one of them in detail. Also suggest the controls for the same. [8]
 - (c) Differentiate between a fault and failure. [2]
5. Answer the following. [6]
 - (a) What are the security requirements of the database management systems. [6]
 - (b) What are multilevel databases? Discuss the designs of multilevel secure databases. [10]
Discuss the designs of multilevel secure databases.
6. Answer the following. [6]
 - (a) Is a social engineering attack more likely to succeed-in person, over the telephone or through email ? Justify your answer. [6]
 - (b) Compare copper wire, microwave, optical fiber, infrared and radio frequency wireless in their resistance to passive and active wiretapping. [10]
7. Answer the following. [6]
 - (a) Why is segmentation recommended for network design ? [6]
 - (b) Can link and end-to-end encryption both be used on same communication ? What would be advantages of that ? Cite a situation in which both forms of encryption might be desirable. [5]
 - (c) Why does a stealth mode IDS [Intrusion Detection System] need a separate network to communicate alarms and to accept management commands ? [5]
8. Answer the following. [8]
 - (a) Discuss the legal issues in computer security. [8]
 - (b) Dave works as a programmer for a large software company. He writes and tests utility programs. His company operates two computing shifts : during the day program development and online applications are run ; at night batch production jobs are completed. Dave has access to workload data and learns that the evening batch runs are complementary to daytime programming tasks; that is, adding programming work during the night shift would not adversely affect performance of the computer to other users. So, Dave comes back after normal hours to develop a program to manage his own stock portfolio. His derain on system is minimal, and he uses very few expendable supplies. [8]
 - (i) Is Dave's behaviour ethical ?
 - (ii) Discuss it on grounds of principals of ethics as ownership of resources, effect on others, universalism principal, possibility of detection and punishment,
 - (iii) Give codes of ethics for programmer.

○ ○ ○

System Security – December 2005

Time : 3 Hrs.]

[Marks : 100

- N.B. :** (1) Q. No. 1 is compulsory.
 (2) Solve any five from remaining questions.

1. (a) Define and discuss which of the following security services are attempted to be implemented by the following two protocols ? [10]

Service :

Confidentiality.
 Authentication of the sender.
 Authentication of the receiver.
 Non-repudiation of sender.
 Non-repudiation of the receiver.
 Integrity.

Protocol 1 :

- (i) A sends a message M to B that is encrypted under B's public key.

$$A \rightarrow B : E_{B_{\text{Public key}}} [M]$$

- (ii) B sends a message M to A encrypted under public key of A.

$$B \rightarrow A : E_{A_{\text{Public key}}} [M]$$

Protocol 2 :

- (i) A sends to B a message M and his name encrypted under the public key recipient.

$$A \rightarrow B : E_{B_{\text{Public key}}} [A, M]$$

- (ii) B sends to A a message M and his name encrypted under the public key of recipient.

$$B \rightarrow A : E_{A_{\text{Public key}}} [B, M]$$

- (b) Redesign any of the given protocol to implement the services, which at the moment it is falling to do so. [10]
2. (a) What is the purpose of encryption in multilevel secure data bases ? Explain how is it implemented ? Is it a good technique to implement the separation in data bases ? Justify. [8]
 (b) Explain the disadvantages of partitioning as a means of implementing multilevel security for data base. [8]
3. (a) (i) Discuss the difference between a digital signature and digital certificate. [10]
 (ii) Upon reception of a digital certificate, how one can decide whether to trust that or not?
 (iii) How the certification authorities take care of compromised certificates ?
 (b) Describe a social engineering attack you could use to obtain a user's password ? [6]
4. (a) Discuss the security in IP sec protocol. [6]
 (b) What is a denial of service attack ? What are the ways in which an attacker can mount a DOS attack on the system. [10]
5. (a) List the controls against program threats. Explain Developmental Control in detail. [8]
 (b) Explain in detail the steps in risk analysis. [8]
6. (a) (i) Why the user authentication is required ? [8]
 (ii) What techniques are used for authentication ?
 (iii) What are the flows in the user authentication process ?
 (iv) Suggest controls over them.
 (b) Discuss any two techniques of memory and address protection. [8]
7. (a) What are the characteristics of a good Security Policy ? [6]
 (b) Patty workers as a programmer in a Corporation. David, her Supervisor, tells her to write a program to allow people to post entries directly to company's accounting files. Patty knows that ordinarily programs that affect the accounting files involve several steps, all of which have to balance. Patty realizes that with the new program, it will be possible for one person to make changes to crucial amounts, and there will be no way to trace who made these changes, with what justification, or when.
 Patty raises these concerns to David, who tells her not to be concerned, that her job is simply to write the programs as he specifies. He says that he is aware of the potential misuse of these programs, but he justifies his request by nothing that periodically a figure is mistakenly entered in the accounting files and the company needs a way to correct the inaccurate figure.
 This is an example where a person is asked to do fraudulent things. Discuss the ethical issues involved in this case. [10]

○○○

System Security – May 2006**Time : 3 Hrs.]****[Marks : 100**

- N.B. :**
- (1) Q. No. 1 is **compulsory** and attempt any **four** from remaining questions.
 - (2) Answer to the point.
 - (3) Assumptions should be highlighted and justified.
 - (4) Draw diagram to explain the theory wherever necessary.
 - (5) Start major question on new page and maintain the order of questions.
 - (6) For every question and its answer, title it with details e.g. Q./a/2/i if there are subsections.
 - (7) While stapling the supplements, take care that questions numbers and answers are not obscured.
1. (a) (i) Authentication means proving identities between entities which happens in different layers of network protocol stack for different reasons. Identify these entities and state them. [10]
(ii) State five design principles of any cryptographic algorithm.
 - (b) (i) Suppose bubbly has got message M, private key sk1, and public key pk1 and Bunty has got private key sk2 and public key pk2. Bubbly computes $x = E_{sk1}(E_{pk2}(M))$, where E is encryption. Now she sends this x to Bunty. State the security goals achieved and not achieved. [10]
(ii) Make most suitable 10 comments (or features) about PEM. i.e. privacy enhanced mail.
 2. (a) Draw only activity diagrams showing Server authentication and Client Authentication in SSL. [10]
(b) Classify and list the viruses and state them. [10]
 3. (a) Explain SQL level support for Database Security [10]
(b) List the 10 clauses of IT laws. (Preferably in Indian IT law) [10]
 4. (a) Explain Access control, Flow control, Inference Control and Encryption in Data Base security. [10]
(b) As security administrator, identify 10 critical assets (Servers and / or Equipments) and 10 security policies for organization. [10]
 5. (a) How to carry out the Risk analysis in the company ? [10]
(b) State five types of firewalls, draw the diagrams and label them. [10]
 6. (a) Compare AES, SHA and RSA Cryptography. [10]
(b) How does OS protect files in Main memory and on Secondary device. [10]
 7. (a) List the code of Ethics you know. (IEEE, ACM etc) [10]
(b) List the fields of digital certificate. [10]

○ ○ ○

System Security – December 2006**Time : 3 Hrs.]****[Marks : 100**

- N.B.:**
- (1) Question No.1 is **compulsory**.
 - (2) Attempt any **four** questions from the remaining questions.
 - (3) Assumptions should be highlighted and justified.
1. (a) Explain the terms confidentiality, availability and integrity. [6]
(b) Why is segmentation required for network design? [6]
(c) Compare AES, SHA and RSA cryptography. [8]
 2. (a) List and explain the various malicious codes. [10]
(b) Classify and explain the viruses based on how they attach themselves. [10]
 3. (a) Compare stream Encryption algorithms and Block Encryption algorithms. [10]
(b) Compare secret key and Public key encryption. [10]
 4. (a) What are firewalls ? State and explain the types of firewalls with the help of diagrams. [10]
(b) Explain in detail the steps in Risk Analysis. [10]
 5. (a) Discuss the difference between a digital certificate and digital signature. [10]
(b) What are multilevel databases? Discuss the designs of multilevel secure databases. [10]
 6. (a) Explain and compare Link and End-to-End Encryption with the help of neat diagrams. [10]
(b) Discuss the security in IPsec protocol. [10]
 7. Write short notes on any **two** : [20]
(a) Virtual Private Networks
(b) File Protection Mechanism
(c) Threats in Networks

○ ○ ○

System Security – May 2007**Time : 3 hrs]****[Marks : 100**

- N.B.:** (1) Q. No. 1 is **compulsory**.
 (2) Attempt any **four** questions out of remaining **six** questions.
 (3) **Figures** to the **right** indicate **full** marks.
 (4) Assume any **suitable** data wherever **required** but justify the same.
1. (a) Distinguish among vulnerability, threat and control. [5]
 (b) Can a database contain two identical records without a negative effect on the integrity of the database? Why or why not. [5]
 (c) Explain how a fence register is used for relocating a user's program. [5]
 (d) Compare copyright, patent and trade secret protection. [5]
 2. (a) Answer the following : [10]
 (i) What is access control? How different is it from availability?
 (ii) What is worm? What is the significant difference between worm and virus.
 (b) Compare the following : [10]
 (i) AES, SHA and RSA cryptography.
 (ii) Secret key and public key encryption.
 3. (a) Consider a program to accept and tabulate votes in an elector. Who might want to attack the program? What types of harm might they want to cause? What kind of vulnerabilities might they exploit to cause harm? [10]
 (b) Explain the use of temporal separation and physical separation for security in computing environment. [10]
 4. (a) What are multilevel databases? Discuss the designs of multilevel secure databases. [10]
 (b) Explain in details the steps in risk analysis. [10]
 5. (a) Answer the following : [10]
 (i) What is the difference between a digital signature and digital certificate? Upon reception of a digital certificate, how one can decide whether to trust that or not?
 (ii) Is a social engineering attack more likely to succeed in person, over the telephone or through e-mail?
 (b) List the characteristics of a good firewall implementation. What are the limitations of a 10 firewall? [10]
 Give the comparison between the several types of firewalls such as packet filtering, stateful inspection, application proxy, guard and personal firewall.
 6. (a) Discuss the similarities and differences between signature based IDS and heuristic based IDS. What are the limitations of IDS? [10]
 (b) What is the Denial of Service (DOS) attack? What is the meaning of the term 'service1 in DOS? [10]
 What can possibly prevent DOS attacks?
 7. Write a details note on: (any two) [20]
 (a) Kerberos
 (b) Virtual Private Networks
 (c) E-mail Security

○ ○ ○

System Security – December 2007**Time: 3Hrs.]****[Marks : 100**

- N.B.:** (1) Question No.1 is **compulsory**.
 (2) Attempt any **four** questions from the remaining **six** questions.
 (3) **Figures** to the **right** indicate **full** marks.
 (4) Assume any **suitable** data wherever **required** but justify the same.
1. (a) Distinguish between vulnerability, threat and control. [5]
 (b) Compare secret key and public key encryption. [4]
 (c) What are Covert Channels? How potential Covert Channels can be identified? [4]
 (d) Explain how capabilities are used to control the access to general objects. [4]
 (e) 'Smurf is an "availability" attack. Justify. [3]
 2. (a) Compare AES and DES. Comment on Double and Triple DES. [10]
 (b) Compare stream encryption and block encryption algorithms. [10]
 3. (a) What are malicious codes? Explain the various types. [10]
 (b) Discuss the probable homes for virus. [10]
 4. (a) What are multi-level databases? Discuss the design of multi-level secure databases. [10]
 (b) Explain and compare Digital signatures and Digital certificates. [10]
 5. (a) Discuss the various threats in a network. [10]
 (b) Compare signature based and Heuristic based IDS. What are the limitations of IDS? [10]
 6. (a) Explain in detail, the steps in Risk Analysis. [10]
 (b) Discuss the legal issues in Computer Security. [10]
 7. Write short notes on any two : [20]
 (a) Kerberos
 (b) File Protection Mechanism
 (c) Firewalls

○ ○ ○

System Security – May 2008**Time: 3Hrs.]****[Marks : 100**

- N.B.:** (1) Q. No. 1 is **compulsory**.
 (2) Attempt any **four** questions out of remaining **six** questions.
 (3) **Figures** to the **right** indicate **full** marks.
 (4) Answers to questions should be **grouped** and written **together**.
1. (a) What are the key principles of Security ? Explain with example. [5]
 (b) Explain the tagged Architecture in memory protection. Give example. [5]
 (c) List the limitations on the amount of information leaked per second through a covert channel in a multiaccess computing system. [5]
 (d) List three controls that could be applied to detect or prevent Salami attacks. [5]
 2. (a) What are the different types of Vulnerability, Threat and Control ? Give example of each. [10]
 (b) What is a denial of service attack ? What are the way in which an attacker can mount a DOS/DDOS attack on the system ? [10]
 3. (a) List and explain the various malicious codes and Non-malicious codes. [10]
 (b) What is a Firewall ? Describe the types of firewalls with their limitations. [10]
 4. (a) Explain the use of temporal, physical and logical separation for Security in computing environment. [10]
 (b) Explain the various facilities that a database management system provides to protect the sensitive data. [10]
 5. (a) Describe the types of IDSs and their limitations. Why we need hybrid IDSs ? [10]
 (b) Define the term Ethics. What is the difference between laws and Ethics? What is IEEE code for Ethics? [10]
 6. (a) What are the various forms of protection that operating system applies at the file level ? What are the difficulties involved with mechanism ? [10]
 (b) What is the purpose of encryption in multi-level secure data bases ? Explain how is it implemented ? Is it a good technique to implement the separation in databases ? Justify. [10]
 7. (a) What is the term Risk analysis ? Explain in detail the steps in Risk analysis. [10]
 (b) Explain Secure E-mail systems with examples. [10]

○ ○ ○

System Security – December 2008**Time: 3Hrs.]****[Marks : 100**

- N.B.:** (1) Q. No. 1 is **compulsory**.
 (2) Attempt any **four** questions out of remaining **six** questions.
 (3) **Figures** to the **right** indicate **full** marks.
 (4) Answers to questions should be **grouped** and written **together**.
1. (a) Compare secret key and public key encryption. [5]
 (b) Explain how a Fence register is used for relocating a user's program. [5]
 (c) Compare copyright, patent and trade secret protection. [5]
 (d) Why segmentation recommended for network design ? [5]
 2. The following questions are based on a scenario in which encrypted data are passed between Alice and Bon using the RSA algorithm. Alice's public key is {17, 321} and Bob's public key is {5, 321}. Assume that no one knows the private keys but the original owners. [20]
 (a) Encrypt the message $M = 7$ using Bob's public key.
 (b) What should Alice have to do to decrypt the message from part a ?
 (c) What would Bob have to do to decrypt the message from part a ?
 (d) What is Alice's private key ?
 (e) What is Bob's private key?
 3. (a) What are the legal issues in computer security ? Is a Social Engineering attack more likely to succeed in person, over the telephone or through email ? Justify your answer. [10]
 (b) What are the multilevel databases ? Discuss the designs of multilevel secure databases. [10]
 4. (a) Compare copper wire, microwave, optical fiber, infrared and radio frequency wireless in their resistance to passive and active wiretapping. [10]
 (b) Compare signature based and Heuristic based IDS. What are the limitations of IDS ? [10]
 5. (a) (i) The distinction between a covert storage channel and a covert timing channel is not clear-cut. Everything timing channel can be transformed into an Equivalent storage channel. Explain how this transformation could be done. [5]
 (ii) An Electronic mail system could be used to leak information. First, explain how the leakage could occur. Then, identify controls that could be applied to detect or prevent the leakage. [5]
 (b) (i) The discussion of base/bounds registers implies that program code is execute-only and that data areas are read-write-only. Is this ever not the case? Explain your answer. [5]
 (ii) Can any number of concurrent processes be protected from one another by just one pair of base/bounds registers ? Explain your answer. [5]

6. (a) A distributed denial-of-service attack requires zombies running on numerous machines to perform part of the attack simultaneously. If you were a system administrator looking for zombies on your network. What would you look for ? [10]
 (b) Explain the different issues in security plan. (Explain at least seven issues). [10]
7. (a) Explain the basic steps of risk analysis. [10]
 (b) Define the term Ethics. What is the difference between laws and Ethics? What is IEEE Code for Ethics? [10]

○ ○ ○

System Security – May 2009

Time: 3Hrs.]

[Marks : 100

- N.B.:** (1) Question No. 1 is compulsory.
 (2) Attempt any **four** questions out of remaining **six** questions.
 (3) **Figures** to the **right** indicate **full** marks.
 (4) Answers to the questions should be **grouped** and written **together**.
 (5) Assume any **suitable data** wherever **required** but **justify** the **same**.

1. (a) What is Brain Virus? How it passes on its infection? [5]
 (b) Compare signature-based and anomaly-based IDS. What the strengths and limitations of IDS? [5]
 (c) List two disadvantages of each of the following : [5]
 (i) Physical separation (ii) Temporal separation
 In computing system.
 (d) How is the encryption key generated from password in Kerberos? [5]
2. (a) (i) Compare Secret Key and Public Key encryption in terms of number of keys, Protection of key, Best uses, Key distribution and Speed. [5]
 (ii) List and briefly define three applications of a public-key cryptosystem. [5]
 (b) In RSA system, the public key of a given user is $e = 7$, and $n = 187$.
 (i) What is the private key of this user? [4]
 (ii) You intercept the ciphertext $C = 11$ sent to a user whose public key is $e = 7$, and $n = 187$. What is the plaintext M ? [4]
 (iii) What are two possible approaches to defeating the RSA algorithm. [2]
3. (a) List and explain the various malicious and non-malicious codes with examples. [10]
 (b) Which are the three types of controls against program threats? Explain each with examples. [10]
4. (a) What is file protection mechanism? List and compare the basic forms of protection? [10]
 (b) Describe each of the following four kinds of access control mechanisms in terms of (1) ease of determining authorized access during execution, (2) ease of adding access for a new subject, (3) ease of deleting access by a subject, and (4) ease of creating a new object to which all subjects by default have access. [10]
 (i) per-subject access control list (iii) access control matrix
 (ii) per-object access control list (iv) capability
5. (a) What is interference problem? Which are the various ways to determine the sensitive data values from a database using interference problem? [10]
 (b) What are the basic requirements for database security? Briefly examine each of the requirement. [10]
6. (a) What is denial of service attack? What are the way in which an attacker can mount a DOS/DDOS attack on the system? [10]
 (b) List the threats to E-Mail and what the various requirements and solutions for secure E-Mail. [10]
7. (a) Compare copyright, patent and trade secret in terms of protects, protected object made public, requirement to distribute, ease of filling, duration and legal protection. Which are the various issues relating to information? [10]
 (b) Explain the basic steps of risk analysis. [10]

○ ○ ○

System Security – December 2009

Time: 3Hrs.]

[Marks : 100

- N.B.:** (1) Question No. 1 is compulsory.
 (2) Attempt any **four** questions out of remaining **six** questions.
 (3) **Figures** to the **right** indicate **full** marks.
 (4) Answers to the questions should be **grouped** and written **together**.
 (5) Assume any **suitable data** wherever **required** but **justify** the **same**.

1. (a) Distinguish among vulnerability, threat and control. [5]
 (b) Explain threat precursors with example. [5]
 (c) Does a PKI use symmetric or asymmetric encryption ? Explain your answer. [5]
 (d) Does VPN use Link or End to End encryption ? Justify your answer. [5]

2. (a) What is the difference between a digital signature and digital certificate ? How one can decide whether to trust that or not, upon reception of a digital certificate ? [10]
(b) Write a note on Data Encryption Standard (DES). [5]
(c) Compare between DES, AES and RSA encryption algorithms. [5]
3. (a) How memory and address protection is done by different methods as fence, relocation and Base and Bound register ? [10]
(b) Explain nonmalicious program errors with examples. [10]
4. (a) How is multilevel security provided to database ? Explain in terms of separation, encryption, integrity lock, sensitivity lock. [10]
(b) Explain denial of service or DOS attack in networks. [10]
5. (a) List functions of Intrusion Detection System. Explain and differentiate signature based and anomaly based IDS. [10]
(b) List and explain the issues of security plan for administrative security. [10]
6. (a) Write a note on Kerberos system that supports authentication in distributed system. [10]
(b) What is file protection mechanism ? List and explain basic forms of protection. [10]
7. (a) How risk analysis is done to provide effective security planning ? Present examples of risk analysis methods. [10]
(b) Define the term Ethics. What is the difference between Laws and Ethics ? What is IEEE code for Ethics ? [10]

○ ○ ○