

Code :R7320504

1

III B.Tech II Semester(R07) Regular & Supplementary Examinations, April/May 2011  
**INFORMATION SECURITY**  
(Computer Science & Engineering)

Time: 3 hours

Max Marks: 80

Answer any FIVE questions  
All questions carry equal marks

\*\*\*\*\*

1. (a) Why are some attacks called as Passive? Why others are called active? Give examples for each.  
(b) With an example, explain how format string exploits work?
2. (a) Explain the types of attacks on Encrypted messages.  
(b) What is the difference between link and end-to-end Encryption?
3. (a) With a neat diagram explain how public key cryptosystem offers secrecy.  
(b) What are characteristics of user certificates generated by a certification authority (CA)?
4. (a) What are the reasons for generating signatures before compression?  
(b) With flow diagrams explain the transmission and reception of PGP messages.
5. Explain briefly how IPSec documents are categorized.
6. (a) Discuss in detail about SSL architecture.  
(b) Explain about SSL record protocol and discuss briefly about its operation.
7. Illustrate the role of SNMP with the help of neat diagram.
8. (a) List the design goals for a firewall.  
(b) What are the limitations of firewall?

\*\*\*\*\*

Code :R7320504

2

III B.Tech II Semester(R07) Regular & Supplementary Examinations, April/May 2011  
INFORMATION SECURITY  
(Computer Science & Engineering)

Time: 3 hours

Max Marks: 80

Answer any FIVE questions  
All questions carry equal marks

\*\*\*\*\*

1. (a) List and briefly define categories of Passive and Active security attacks?  
(b) Why do buffer overflows exist? How can you find buffer overflows in code?
2. (a) Explain Brute-force attack.  
(b) Illustrate the operation of HMAC and Explain.
3. (a) Discuss the applications for public key crypto system.  
(b) Explain how Kerberos supports interrealm authentication.
4. (a) Explain in detail Radix-64 conversion.  
(b) Describe S/MIME functionality in detail.
5. Explain about security associations and how SA is uniquely identified.
6. (a) Discuss in detail about SSL record format.  
(b) Also discuss in detail about SSL record Protocol payload.
7. Compare SNMPv1 and SNMPv2 protocol data units.
8. (a) Discuss on service controls on which firewalls focused.  
(b) Explain capabilities within the scope of a firewall.

\*\*\*\*\*

Code :R7320504

3

III B.Tech II Semester(R07) Regular & Supplementary Examinations, April/May 2011  
**INFORMATION SECURITY**  
(Computer Science & Engineering)

Time: 3 hours

Max Marks: 80

Answer any FIVE questions  
All questions carry equal marks

\*\*\*\*\*

1. (a) Define Security Service. Explain the Categories of Security Services.  
(b) Explain TCP session Hijacking with an example.
2. (a) With a neat diagram explain Fiestal cipher.  
(b) Explain Cipher feedback mode with an illustration.
3. (a) With a neat sketch explain how public key crypto system offers secrecy and authentication.  
(b) Explain the approaches to security in a distributed architecture.
4. (a) Give the general format of PGP messages and explain each field.  
(b) With an example explain MIME multipart message.
5. Discuss in detail about transport and tunnel mode in the context of AH and ESP.
6. (a) What does SSL Alert protocol convey?  
(b) List alerts that are always fatal from SSL specification.
7. (a) What are different obstacles created by the way SNMP works.  
(b) How do long routing tables have a negative impact on SNMP protocols?
8. Describe about packet filtering routing in detail.

\*\*\*\*\*

Code :R7320504

4

III B.Tech II Semester(R07) Regular & Supplementary Examinations, April/May 2011  
**INFORMATION SECURITY**  
(Computer Science & Engineering)

Time: 3 hours

Max Marks: 80

Answer any FIVE questions  
All questions carry equal marks

\*\*\*\*\*

1. (a) What Security services are needed to enhance security of the information? Explain each with an example.  
(b) Explain Route table modification in detail.
2. (a) "Exact realization of a symmetric Block cipher depends on the choice of certain parameters and design features" What are they? Explain.  
(b) Explain various ways of achieving key distribution.
3. (a) Distinguish between symmetric key and asymmetric key crypto systems.  
(b) List and briefly define three uses of public-key Cryptosystem.
4. (a) Explain the approaches to public key management in PGP.  
(b) What are the limitations of SMTP/822 scheme?
5. Explain about tunnel and transport functionality in detail.
6. (a) Discuss about SSL hand shake protocol Message types.  
(b) Explain about change cipher Spec protocol.
7. Why does SNMP use unreliable UDP datagram? What would be the reason for the designers to choose UDP instead of TCP for transport protocol for SNMP?
8. Describe application level gateway in detail.

\*\*\*\*\*