M.E. Computer Science and Engineering
First Year Second Semester Examination 2018

NETWORK SECURITY

Time: 3 hours Full Marks: 100

Answer any **four questions** from the following

(All parts of the same question must be answered together)

1.

a. What is integrity? How it can be ascertained that information *I* has the property of integrity? What is *integrity policy*? How can *commercial security policy* be related to *integrity policy?*

b. What is *threat*? What are the broad categories of threat? Give an example of each with justification.

c. What is the difference between *security policy* and *security mechanism*?

d. What are the principles of operation regarding *duty* and *function*? How do these principles affect the security of a system?

(3+2+2+2)+(2+2+4)+3+(3+2)=25

2.

a. What are the issues regarding preservation of *anonymity*? What is *domain boundary crossing*?

b. What is *phishing*? Differentiate between *clone phishing* and *spear phishing.*

c. Why is *buffer overrun* considered to be *buffer overflow attack*? What measures may be taken to counter *buffer overflow attack*? What are the various ways of writing *safe* program code?

d. What is *IP address spoofing*?

(4+2)+(2+5)+(2+4+4)+2=25

3.

a. How can *Denial of Service (DoS)* attack be identified? How can *DoS* attack take place using *spoofing*? Can *Distributed DoS (DDoS)* also take place through *spoofing*? Justify your answer. Why is *DDoS* considered to be a more effective attack than *DoS*?

b. What is *SYN* flood? How does it affect the system?

c. How does *Reflection attack* use the *challenge-response* mechanism?

d. How can a *recursive DNS server* be used for *Amplification attack*?

(3+3+3+2)+(3+3)+4+4=25

4.

a. What services are provided by 802.11i Robust Security Network (RSN)? Mention any one cryptographic algorithm each that is used for each service. What schemes are used for protected data transfer? State their functionalities.

b. What does a SIM of a mobile device contain? How is *User and Signaling Data confidentiality* provided in GSM? What is the requirement of generating *session key*? Which component generates the session key? What is TMSI?

(3+3+4)+(3+6+2+2+2)=25

5.

a. What is *cryptosystem*? What type of cipher is *DES*? Justify.

b. Why and where can you use *digital certificate*? What are the contents of *digital certificate*? What are the desirable qualities of *Certification Authority (CA)*?

c. What is the problem with *Classical Cryptographic Key Exchange protocol*? What is the working principle of *Needham-Schroeder protocol*? Why is it required in *Kerberos*? How does *Ticket Granting Server (TGS)* in Kerberos work?

(3+2)+(3+2+3)+(2+4+2+4)=25

6.

a. What are the security measures in *Transport Layer Security (TLS)*? What is *Cipher Suite*? What is *record*? What operations are done on the *record*?

b. Show how Diffie-Hellman algorithm can be used for generating symmetric key.

c. What is *security association* in IPsec and how is it maintained? What is *tunnel mode* used for? How does IPsec work in *tunnel* mode?

(4+2+2+3)+6+(4+1+3)=25

7.

a. How is authentication done in *Pretty Good Privacy (PGP)*? When are the signature generated and message encrypted in PGP and why? What is *key ring* and how is it used in *PGP*?

b. What algorithms are used for security in *Secure Multipurpose Internet Mail Extension (S/MIME)*? What functions are offered by *S/MIME*? What are the enhanced security services of *S/MIME*? How is confidentiality provided in *S/MIME*?

c. What is *Message Digest*?

(3+3+4)+(3+3+3+3)+3=25