USN | | | | | | | | | | |

10SCN14

First Semester M.Tech. Degree Examination, June 2012
Information Security

Time: 3 hrs. Max. Marks:100

Note: *Answer any FIVE full questions.*

Important Note : 1. On completing your answers, compulsorily draw diagonal cross lines on the remaining blank pages.
2. Any revealing of identification, appeal to evaluator and /or equations written eg, 42+8 = 50, will be treated as malpractice.

1 a. A successful organization should have multiple layers of security. Identify any five of them and describe. **(10 Marks)**

b. Identify any five critical characteristics of information and explain. **(10 Marks)**

2 a. Draw the diagram of Dual–Homed host firewall and give description. **(10 Marks)**

b. Define the terms honey pot and honey nets. Identify two advantages of each. **(10 Marks)**

3 a. Define the term "Security management models". What are the basic components of technical configuration and change management model defined by ISO? **(10 Marks)**

b. Under the maintenance model, briefly discuss the topic "planning and risk assessment". **(10 Marks)**

4 a. Define the following in a computer network application:
(i) Authentication (ii) Data confidentiality
(iii) Integrity (iv) Replay attack
(v) Non–repudiation. **(10 Marks)**

b. Draw the diagram of encryption part of fiestal network and explain. **(10 Marks)**

5 a. Using application diagram of SHA–512 processing of a single 1024–bit block and explain the details on how it works. **(10 Marks)**

b. Consider a Diffie–Hollman scheme with a common prime number q = 11 and its primitive roof "a" = 2
(i) If user A has public key $y_A = 9$, what is the private key of A (X_A)? **(04 Marks)**
(ii) If user B has public key $y_B = 3$, what is the shared key between them? **(06 Marks)**

6 a. Under PGP draw the block diagram depicting confidentiality and authentcation. Briefly describe. **(10 Marks)**

b. Distinguish between transport mode and tunnel mode in IP security. Illustrate with a figure, the format that includes ESP under tunnel mode in IPV_4. **(10 Marks)**

7 a Explain, with a diagram, the operation of SSL record protocol. **(10 Marks)**

b. Define the following terms in a typical secure electronic transaction (SET)
(i) Issuer (ii) Acquirer
(iii) Payment gateway (iv) Certification authority
(v) Dual signature. **(10 Marks)**

8 a. A flawed program in C language is shown below:

```
int main ( ) {
int buffer [10];
buffer [20] = 37;}
```

i) Identify the flaw in this program.
ii) What will be the effect of this flaw on the system? **(05 Marks)**

b. Under the topic software flaw define and explain the term " Race condition ". **(05 Marks)**

c. What is digital rights management (DRM)? Discuss in detail how DRM can be applied to streaming media. **(10 Marks)**

* * * * *

www.VTUPlanet.com