

Total number of printed pages – 4

B. Tech

PECS 3406

Eighth Semester Examination – 2008

COMPUTER SECURITY

Full Marks – 70

Time : 3 Hours

Answer Question No. 1 which is compulsory
and any **five** from the rest.

The figures in the right-hand margin
indicate marks.

1. Answer the following questions : 2×10
- (a) Alice meets Bob and says **BRXDUHP-
BIULHDG** using Caesar cipher, what does
she want to convey ?
- (b) The message **let us go for coffee** uses
a simple transposition cipher with a key
24153. Find the cipher text.

P.T.O.

- (c) Differentiate between confidentiality and integrity.
- (d) Discuss the information security model
- (e) What is logic bomb ?
- (f) Define web spoofing.
- (g) What is session hijacking ?
- (h) Decrypt *HWKSWXSLGNTCG* using Vigenere cipher with key *Pascal*.
- (i) Distinguish between AES and DES encryption.
- (j) What is assurance in trusted OS ?
2. (a) Define RSA Cryptosystem. Hence for cipher text $C = 10$, public key $e = 5$ and $n = 35$, find the plain text. 5
- (b) Discuss the security aspects of RSA. 5

3. (a) What are the different possible computer crimes ? 5
- (b) How do the cyber criminal commit crimes? 5
4. (a) Discuss different cyber laws. How intellectual property law is enforced to protect copyright violation. 5
- (b) What are the differences between admissible and inadmissible evidence ? 5
5. (a) What is Firewall ? What types of firewalls are used and for what purpose ? 5
- (b) What DMZ stands for ? How does it work ? 5
6. (a) Distinguish between worms and viruses. 5
- (b) Discuss the buffer overflow attack in programs. 5

7. (a) State the steps for design of a trusted OS. 5
- (b) What is database security ? Hence discuss multilevel database security. 5
8. Write notes on : 5×2
- (a) Ethical issues in computer security
- (b) Intrusion detection system.

IWL