APC - 5082

Second Year B.C.A (Semester - II) Examination
Paper - 15BCA210
Network Security

Time : Three hours] [Full Marks - 60

N.B. : i) All questions carry equal marks
ii) Question No. 1 is compulsory
iii) Assume suitable data wherever necessary.
iv) Illustrate your answer necessary with the help of neat sketches
v) Use Blue/Black ink/refill only for writing the answer book.

Q.1 Fill in the blanks and rewrite the following statements. 5

a) Vernam cipher is also called as
i) rail-fence techniques ii) one time pad
iii) hill cipher iv) play-fair cipher

b) _____ it increase the redundancy in plain text.
i) Confusion
ii) Diffusion
iii) Both confusion and diffusion
iv) Neither confusion nor diffusion

c) if p is a prime and a is positive integer then ($a^p = a \bmod p$) is an alternative form of which theorem.
i) Miller's algorithm ii) Euler's algorithm
iii) Fermat's theorem iv) Newton's theorem

d) _____ are very crucial for asymmetric key cryptography.
i) Integers ii) Prime number
iii) Negative numbers iv) Fractions

e) SSL works between ___ and ___
i) Web Browser, Web server
ii) Web Browser, Application server
iii) Web server, Application server
iv) Application server, Database server

Q.2 a) Explain the following substitution techniques with example. 6
i) Cipher ii) Caesar cipher
b) Explain the various security services. 5

OR

Q.3 a) Explain the following techniques with example. 6
i) rail-fence techniques i) one time padding
b) Explain the model for network security. 5

Q.4 a) Explain the DES encryption alogrithm. 6
b) Explain the structure of classical feistel network. 5

OR

Q.5 a) What are stream cipher and block cihpher ? 5
b) Explain advanced Encyption standard AES cipher. 6

Q.6 a) State and prove the fermat's theorem with example. 5
b) What is prime number ? 3
c) What is Euler's totient function ? 3

OR

Q.7 a) Explain the Eulidean Algorithm with finding GCD (1970,1066) 6
b) Explain testing for primality using Miller-Rabin algorithm. 5

Q.8 a) Explain RSA public-key Encryption Algorithm with example. 5
b) Explain the need of message authentication ? Explain message authentication code in brief. 6

OR

Q.9 a) Write importance and properties of digital signature. 6
b) What is Hash function ? Describe block diagram of hash function. 5

Q.10 a) Explain pretty good privacy in E-mail security. 5
b) Expalin the following. 6
i) Firewall
ii) Viruses

OR

Q.11 a) Explain the SSL Architecture. 5
b) What are MIME and S/MIME ? Explain in brief. 6

****