M.Sc. Examination 2018
Semester-III
Computer Science
Course : MCSC-32
(Cryptography and Network Security)

Time : 3 Hours **Full Marks : 40**

Questions are of value as indicated in the margin

Answer Question No. **1** and **any four** from the rest.

1. a) Briefly describe Substitution cipher and suggest a suitable mechanism to break it.
   b) What is tiny fragment attack? (3+3)+2=8
2. a) Write an efficient program to find the multiplicative inverse of a given number.
   b) Describe Affine cipher algorithm for encryption and decryption. 3+(2.5×2)=8
3. a) Prove that the decryption is the reverse of encryption in RSA crypto-system.
   b) Why do we take the very big prime numbers in RSA?
   c) What is PGP? 4+2+2=8
4. a) Design a suitable method to authenticate a web page. Write the sequential steps to execute your design.
   b) What is public key crypto system? 6+2=8
5. a) Briefly describe and comment on the IPSec architecture.
   b) State different functionalities provided by S/MIME? 4+4=8
6. a) Write down the sequential steps to form a digital signature.
   b) What is the job of SSL record protocol? 4+4=8
7. Write short notes on the following :
   a) Packed-Filtering router
   b) Access Control 4+4=8

———