K21U 0103

Reg. No. : .....

Name : .....

VI Semester B.Sc. Degree (CBCSS – Regular/Supplementary/Improvement) Examination, April 2021
(2014 – 2018 Admissions)
CORE COURSE IN COMPUTER SCIENCE
6B16CSC – E06 : Information Security

Time : 3 Hours Max. Marks : 40

SECTION – A

1. **One** word answer : **(0.5×8=4)**

   a) Confidentiality, _____ and availability are the three security goals.

   b) The word _____ with origin in Greek means "covered writing".

   c) _____ is the art of breaking cryptographic codes.

   d) In _____ key encryption, the locking and unlocking is done with the same key.

   e) _____ is the most widely used symmetric – key block cipher published by NIST.

   f) Expand RSA in RSA Algorithm.

   g) _____ attack involves trying all the possible private keys.

   h) Plain text can be converted into _____ using a key.

SECTION – B

Write short notes on **any seven** of the following questions : **(7×2=14)**

2. List and discuss any two passive attacks.
3. Discuss on principles of security.
4. List any four polyalphabetic ciphers.
5. List any four cryptanalysis attacks.
6. What is the number of rounds in DES ?
7. List any two known attacks conducted in DES and its conclusion.

P.T.O.

8. Discuss on cipher design weakness of DES.
9. What are the ingredients of a public key encryption scheme ?
10. What is the blinding process in RSA security ?
11. What are the three basic properties needed for a digital signature ?
12. Briefly explain about multiple encryption techniques with a DES perspective.
13. List the three kinds of attacks on digital signatures.
14. Which are the three security services provided by using digital signature and list the security service not provided by digital signature alone ?
15. What is selective forgery ?

SECTION – C

Answer **any four** of the following questions : **(4×3=12)**

16. Discuss on the security attacks threatening the integrity of data.
17. Discuss in detail about transposition ciphers.
18. Explain about stream ciphers and block ciphers in detail.
19. Explain why DES is more vulnerable to linear cryptanalysis than differential cryptanalysis.
20. Why does the DES function need an expansion permutation ?
21. What requirements must a public key cryptosystem fulfil to be a secure algorithm ?
22. Briefly explain about the digital signature process.
23. Distinguish between digital signature from conventional signature.

SECTION – D

Answer **any two** of the following questions : **(2×5=10)**

24. Explain about the need and principles of information security in detail.
25. Explain about attacks and its various types in detail.
26. Explain about substitution ciphers with suitable examples.
27. Explain about DES and multiple DES in detail.
28. Explain about the RSA algorithm and its security.
29. Explain about digital signature schemes in detail.

———————