Exam Date & Time: 05-Apr-2023 (01:30 PM - 02:30 PM)

**CHAROTAR UNIVERSITY OF SCIENCE AND TECHNOLOGY**

**CHAROTAR UNIVERSITY OF SCIENCE & TECHNOLOGY**
**6th Semester of B. Tech. (CSE) Unit Test-II**
**April 2023**
**CS361 Cryptography & Network Security**
**Date:05/04/2023, Tuesday**
**Time: 01.30 pm to 02.30 pm Maximum Marks: 30**

**CRYPTOGRAPHY AND NETWORK SECURITY [CS361]**

**Marks: 30** **Duration: 60 mins.**

**Section 1**

**Answer all the questions.**

| | | | | |
|---|---|---|---|---|
| 1 | | | Define Cryptographic Hash and MAC functions. | (2) |
| 2 | | | Implement how digital signature can be implemented using hashfunction. | (2) |
| 3 | | | If q=19,alpha=10 ,$X_A$=16 ,generate value of public key$Y_A$ if we use elgamal key generation. | (2) |
| 4 | | | Analyze the disadvantages of Needham Schroeder protocol. | (2) |
| 5 | | | State requirements of MAC functions. | (2) |

**Section 2**

**Answer 4 out of 5 questions.**

| | | | | |
|---|---|---|---|---|
| 6 | | | Using Blum Blum Shub Algorithm,find series of random numbers ifp=7,q=11 and s=12. | (5) |
| 7 | | | Which protocol is used to overcome the limitations of Simple KDCand Needham Schroeder Protocol? Briefly explain the protocol withneat and clean diagram. | (5) |
| 8 | | | How message integrity and message authentication can be achievedusing DSS. Explain with necessary steps and diagram. | (5) |
| 9 | | | Implement the scenario where authentication,digital signature andconfidentiality is maintained using Hash function. | (5) |
| 10 | | | John and Ted needs to communicate to each other. Both John and Teddecides not to use third party for key generation. John and Tedboth agrees on some public component p=27 and g=11. John choosessome random number X=5 and keeps it confidential to himself only.Ted chooses some random number Y=9 and keeps it confidential tohimself only. Calculate the shared session key K which can be usedbetween John and Ted. | (5) |

-----End-----