Faculty of Engineering and Technology			
Ramaiah University of Applied Sciences			
Department	Computer Science and Engineering	Programme	B. Tech. (CSE)
Semester/Batch	3rd/2017		
Course Code	CSC201A	Course Title	Discrete Mathematics-1
Course Leader(s)	Prof. N. D. Gangadhar		

Assignment – 02			
Reg.No.		**Name of Student**	

Sections	Marking Scheme		Marks		
			Max Marks	First Examiner Marks	Moderator
Part A					
	A 1	Deffie-Hellman Key Exchange and its Applications	5		
		Part-A Max Marks	**5**		
Part B.1					
	B 1.1	Solution of the recurrence relation	5		
	B 1.2	Verification of correctness of the solution	3		
	B 1.3	Computation and plotting the amount of data transferred	2		
		B.1 Max Marks	**10**		
Part B.2					
	B 2.1	Solution of the simultaneous equations	6		
	B 2.2	Determining the complete set of solutions	2		
	B 2.3	Verification of the set of solutions	2		
		B.2 Max Marks	**10**		
		Total Assignment Marks	**25**		

Course Marks Tabulation

Component-1 (B) Assignment	First Examiner	Remarks	Moderator	Remarks
A				
B.1				
B.2				
Marks (Max 25)				

Signature of First Examiner **Signature of Moderator**

Please note:

1. Documental evidence for all the components/parts of the assessment such as the reports, photographs, laboratory exam / tool tests are required to be attached to the assignment report in a proper order.
2. The First Examiner is required to mark the comments in RED ink and the Second Examiner's comments should be in GREEN ink.
3. The marks for all the questions of the assignment have to be written only in the **Component – CET B: Assignment** table.
4. If the variation between the marks awarded by the first examiner and the second examiner lies within +/- 3 marks, then the marks allotted by the first examiner is considered to be final. If the variation is more than +/- 3 marks then both the examiners should resolve the issue in consultation with the Chairman BoE.

Assignment - 02

Term - 2

Instructions to students:

1. The assignment consists of 3 questions: Part A – **1** Question, Part B – **2** Questions.
2. Maximum marks is 2**5**.
3. The assignment has to be neatly word processed as per the prescribed format.
4. The maximum number of pages should be restricted to **20**.
5. Restrict your report for Part-A to 2 pages only.
6. Restrict your report for Part-B to a maximum of 8 pages.
7. The printed assignment must be submitted to the course leader.
8. **Submission Date:** 22/10/2018
9. **Submission after the due date is not permitted.**
10. **IMPORTANT**: It is essential that all the sources used in preparation of the assignment must be suitably referenced in the text.
11. Marks will be awarded only to the sections and subsections clearly indicated as per the problem statement/exercise/question

Preamble

This subject is intended to teach the principles, concepts and applications of logic and discrete mathematical structures. Set theory, relations, functions, ordering, induction and modular integer arithmetic are covered. Theory and application of Propositional, Predicate and Hoare Logics for verification of computing systems are discussed. Abstract algebraic structures of Boolean algebras, lattices, groups, rings and fields are taught along with their computer science and engineering applications. Students are trained to solve and analyse logical and algebraic structures arising in computing contexts.

Part-A (05 Marks)

Deffie-Hellman Key Exchange solved one of the fundamental problems in cryptography, namely, the exchange of shared keys over public channels thus enabling Public Key Cryptography. It is employed in a wide variety of cryptography applications.

In this context, the student is required to develop an essay on **"Deffie-Hellman Key Exchange and its Applications"**.

Part B (20 Marks)

B.1 **(10 Marks)**

The amount of data transferred to and from a hard disk is highly dynamic. For the purposes of optimising a hard disk performance, an analyst decided to use an empirical model of the amount of data transferred. The model is given by the following recurrence relation:

$$s_n = a_1 s_{n-1} + a_2 s_{n-2} + a_3 s_{n-3}$$

(where s_n denotes the data transferred during n^{th} hour of the operation) with the initial conditions $s_0 = s0, s_1 = s1, s_2 = s2$. The parameters a_1, a_2 and a_3 are obtained using measured data transfers. The student needs to perform the following:

B.1.1 Solve the recurrence relation and obtain an explicit formula for s_n.

B.1.2 Verify the correctness of the derived solution.

B.1.3 Compute and plot the amount of data transferred during the first 50 hours.

Note: Contact the Subject Leader for parameter and initial condition data.

B.2 **(10 Marks)**

A number theory algorithm in a cryptography application employs the solution to a simultaneous set of Linear Congruence relations:

$$a_1x + b_1y \equiv c_1 (\text{mod } m)$$

$$a_2x + b_2y \equiv c_2 (\text{mod } m)$$

The student needs to perform the following:

B.2.1 Solve the simultaneous equations for a particular pair of values.

B.2.2 Determine the complete set of solutions.

B.2.3 Verify the correctness of set of solutions obtained.

Note: Contact the Subject Leader for student specific data.