Faculty of Engineering and Technology			
Ramaiah University of Applied Sciences			
Department	Computer Science and Engineering	Programme	B. Tech. in CSE
Semester/Batch	6/2018		
Course Code	19CSC315A	Course Title	Information Security and Protection
Course Leader	Prof. N. D. Gangadhar		

Marking Scheme		Marks		
		Max Marks	First Examiner Marks	Moderator
1.1	Algorithm developed and Keys used	**10**		
1.2	C/Python Program	**05**		
1.3	Validation using Test Cases	**05**		
1.4	Conclusion	**05**		
	Part-A Max Marks	**25**		

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

Course Marks Tabulation				
Assignment	**First Examiner**	**Remarks**	**Moderator**	**Remarks**
1				
Marks (out of 25)				

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.

RAMAIAH UNIVERSITY OF APPLIED SCIENCES

Assignment 2

Instructions to students:

1. Maximum marks is **25**.
2. The assignment has to be neatly word processed as per the prescribed format.
3. The maximum number of pages should be restricted to 1**0**.
4. The printed assignment must be submitted to the course leader.
5. **Submission Date: 20 June 2021**
6. **Submission after the due date is not permitted.**
7. **IMPORTANT**: It is essential that all the sources used in preparation of the assignment must be suitably referenced in the text.
8. Marks will be awarded only to the sections and subsections clearly indicated as per the problem statement/exercise/question

Preamble

This course is aimed at preparing the students to understand, design, analyze, implement and integrate security provisions in an IT environment. Students are taught elements of information security, known attacks and counter measures. The module also introduces the students to IT policies, auditing and standards that enable them to understand and provide information security assurance. Scenario based case studies are employed. Students are trained to analyze a given scenario and propose security measures and policies and develop an analytical report documenting their effort.

Encryption / Decryption **(25 Marks)**

Symmetric encryption is a type of encryption where only one secret key is used to both encrypt and decrypt electronic information. The entities communicating via symmetric encryption must exchange the key so that it can be used in the decryption process. It is an old and best-known technique that uses a secret key that can either be a number, a word or a string of random letters. Some of the encryption algorithms include Blowfish, AES, RC4, DES, RC5 etc. Select any algorithm and perform encryption/decryption on any sample text. Use any appropriate key size. Your report should include the following:

A symmetric Encryption/Decryption that performs the following tasks

1. Encrypt (plaintext, group)–Return the encryption of the message for the given group, in the form of a string.

   Decrypt (cipher Text, group)–Return the decryption of the message for the given group, in the form of a string.
2. C/Python Program
3. Test case- Encryption and Decryption of any text document
4. Conclusion