|  |  |
| --- | --- |
| **School of Computing and Engineering** | Description: Description: Macintosh HD:Users:borsmia:Desktop:WordLogo.jpg |

**Assessment**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Course | BSc (Hons) Cyber Security | | | | |
| Module | Applied Cryptography (Level 5) | | | | |
| Module Code | CP50087E | | | | |
| Module Leader: | Waqar Asif | | | | |
| Set by: | Waqar Asif | | | | |
| Moderated by: | Abel Yeboah | | | | |
| Assignment | First-sit assignment | | | | |
| Hand in arrangements | Online submission to Turnitin within Blackboard | | | | |
| Structure of assignment | There are two assignments for this module, each of which has a specific weighting and its own criteria. You must achieve an overall mark of at least 40% to pass this module. | | | | |
| **Assessment** | | **Type** | **Weighting** | **Week due** |
| Assignment 1  Assignment 2 | | Crypto RSA  Online Test 1  Online Test 2 | 60%  20%  20% | 24/01/2023  6/12/2022  13/12/2022 |
| Extensions will be for 10 days or less. Documentary evidence will be required. Submissions up to one week late with no extension will be marked with a maximum mark of 40%. | | | | |
| **Learning outcomes** | 1 | Critically evaluate different encryption algorithms; | | | |
| 2 | Demonstrate mastery in independently designing encryption/decryption algorithms; | | | |
| 3 | Understand the essential concepts and critically evaluate mechanisms and processes involved in securing information in an enterprise system environment | | | |
| 4 | Critically demonstrate the ability to apply security protocols. | | | |

**Assignment 1**

**Weighting:** 60%

**Date/time of submission:** 24/01/2021

**Feedback:**

Feedback will be provided within 15 days of the date of submission.

**Group Membership:** No more than **three** members of each group

Assessment brief:

In this element you need to implement RSA encryption in python. The objective is to make an application that will allow the user to encrypt files using RSA encryption. The tool will have a front which can be a simple terminal. The user will have options to encrypt or decrypt a file. A user should have the liberty to select any .txt file and encrypt and decrypt it. You need to show in your code how you encrypt the data and how you decrypt the data. Your report should have screen captures of the whole tool and the different steps that you take on. There are bonus marks for adding some extra capability in the tool. As this is a group report, you will be accessed based on work conducted by the group and individual efforts. Your individual effort will be assessed with interview questions.

You can use the following link as a guide:

- https://www.section.io/engineering-education/rsa-encryption-and-decryption-in-python/

The detailed marking criteria for this assignment can be referred in the table below:

Marking grid:

|  |  |  |  |
| --- | --- | --- | --- |
| **Criteria** | **Issues** | **Mark** | **Marking breakdown where appropriate** |
| **Crpto RSA** | Background of RSA and explanation of how it works  Implementation of the basic tool  Adding file read write capability and front end  Adding extra capability  Explaining all steps properly  Is the report well-structured and easy to follow?, Including an introduction and conclusion sections? (5) Referencing (5)  Individual interview questions | 10  10  10  5  5  10  10 |  |

**Online test**

**Weighing:** 40%

**Online test date:** 6/12/2022 and 13/12/2022

**Feedback:** Feedback will be provided within 15 days of the submission date.

**Online test topic:**

You need to understand the principles of lecture topics in detail in order to achieve well for the online test. Of course, I will be giving a revision on the topics being examined.