National College of Ireland

MSC in Cyber Security-Year 1- MSCCYB1_JAN21I
PG Diploma in Cyber Security-Year 1- PGDCYB_JAN

Semester Three – 2021

Terminal Assessment Release Date: Tuesday, 10th August 2021
Terminal Assessment Solution Submission Date: Friday, 20th August 2021

Cryptography
Terminal Assignment-based Assessment
Weighting: 60%

Examiners
Mrs. Chetna Sharma
Dr Evgeniia Jayasekera
Dr Nhien An Le Khac

Instructions

1. This is an open book TABA.
2. You are allowed to use your class notes. If the lecture notes are used as a resource for this assignment, do not copy them directly but rather paraphrase them (write in your own words). You must include references to all resources that you have consulted for your answers (e.g., books, articles, tutorials, videos, etc.).
3. **You are not allowed to discuss your solution with other students during the examination. If it is found that a student has discussed his/ her solution with other students, the case will be referred to disciplinary committee for further actions.**
4. This is a Turnitin assignment and the plagiarism will be checked based on Turnitin database. It will be used to check whether a text is copied from Internet, any other source or peer students.
5. You should submit the solution of this assignment on your Moodle page at the TERMINAL ASSIGNMENT Link.
6. You can also draw a diagram/ figure on a piece of paper, take a picture with your mobile phone camera then you submit the photo on Moodle. Please ensure that you write below your drawing the question number the drawing corresponds to.
7. Use a single column layout document.

8. Font size for the body of the text should be 12 point Times New Roman/ Arial.
9. Include student name, student ID and course name (e.g. MSCCYB, PGDCYBE) at the top of the first page.
10. The question number being addressed must be clearly indicated in the document.
11. **You must submit the PDF (or DOC) file by the end of your TABA deadline. Late submissions are not allowed.**
12. **Attempt all questions.**

Question 1:

Use the following steps to determine the value of N:

a. Choose the last two digits of your NCI student id. Let's assume the digits are AB. For example, if your student ID number is x12345867, then A is 6 and B is 7.
b. Calculate S by adding A and B i.e., S = A + B.
c. Select a random number between 10 and 30. Let R be the number.
d. Add R and S to calculate N, i.e., N = R + S.

(5 marks)

Question 2:

Follow the steps below to encrypt and decrypt a random text:

a. Select a random plaintext of N characters and split the plaintext into at least three blocks.
(8 marks)
b. Encrypt the blocks generated in step a) with ECB and find the associated ciphertexts.
(8 marks)
c. Decrypt the ciphertexts generated in step b) with ECB and find their corresponding plaintexts.
(8 marks)
d. Apply CBC encryption to the blocks from step a) and find the associated ciphertexts.
(12 marks)
e. Decrypt the ciphertexts generated in step d) with CBC and find the corresponding plaintexts.
(12 marks)
f. Compare the ECB and CBC modes using the calculations performed on the above plaintext.
(12 marks)

You are free to choose any parameter of the block cipher such as block size, type of block cipher, and initialization vector. For simplicity, you may use the additive cipher as a block cipher.

(8+8+8+12+12+12=60 marks)

(Maximum words: 600 for each)

Question 3:

a. Suppose that a sender needs to send plaintext equal to number N to a destination. Explain how you will use public-key cryptography to meet confidentiality, authentication, integrity, and nonrepudiation security requirements (all together) for plaintext equal to number N.

(12 marks)

(Maximum words: 400 words)

b. Select the RSA public-key cryptography algorithm and use the method given in question a) to meet all security requirements. Note that the plaintext is the number N in this question. There is no word limit for this question. You are free to choose any parameter of the RSA algorithm.

(13 marks)
(No word Limit)

(12+13=25 marks)

Question 4:

Why is the double DES less secure than a single 112-bit DES? Consider an appropriate example to support your answer.

(10 marks)
(Max 400 words)

Marking Scheme:

Q1: If N is calculated correctly, the full five marks will be awarded. The marks could, however, be reduced if the calculation is incorrect.
Q2: The maximum marks for each part are given with the question. However, if part of the answer is correct, a portion of the marks are awarded.
Q3: Equal marks to each correct method and result will be awarded for each correct confidentiality, integrity, and non-repudiation method.
Q4: Only 5 marks will be awarded if the answer is not justified with an appropriate example. A full mark is awarded otherwise.