300128 Information Security - Assignment

Submission Due Monday, 12/10/2020 at 11:59pm
Demonstration during week 13 tut classes

Please note the submission date on LG is Oct 16. It has been brought forward for 4 days to accommodate the demonstration. The assignment will be published in week 5. The student will have about 7 weeks' time. Such change should not affect any student

Task One: 10%
Write a program to implement the S-DES system with the functions defined in the lecture note.

Requirement:

1. Your S-DES system must allow manual input for both encryption and decryption so your program can be properly tested.
2. The inputs for encryption are 8-bit plaintext and 10-bit key both in binary form. The output is 8-bit ciphertext.
3. The inputs for decryption are 8-bit ciphertext and 10-bit key both in binary form. The output is 8-bit plaintext.

Sample test data:

10 bits key: 1000100011, P=00100100, K1=10100010, K2=00011011, C=00001010

10 bits key: 1010101010, P=10101010, K1=11100100, K2=01010011, C=01101011

10 bits key: 0010010011, P=10010010, K1=00100111, K2=01101010, C=01111100

Task Two: 10%
Write a program to implement the RSA encryption algorithm.

Requirement:

1. Your program must allow manual input.
2. Both input (p, q, e, m) and output (c) are decimal numbers.
3. The input will be arbitrary integers. You need to write functions to test if the arbitrary input values of p,q,e,m are legitimate. All modular calculations are required to use the square and multiple algorithm.

Sample test data:

p=11, q=3, e=7, m=5, c=14

p=17, q=11, e=7, m=88, c=11

What to submit:

1. Your source code with proper comments.
2. A document which describes your solution, test plan, test results, a simple manual stating how to test your program and the limitations if your program does not run as required.
3. Please use your student ID as part of your file name.

How to submit:

1. The assignment submission is under the assignment folder via Turnitin assignment submission.

2. Your program MUST be tested at the School laboratory before submission

3. Your submission will be checked by Turnitin for plagiarism.

4. Limited by the format Turnitin takes, your submission needs to convert to pdf for uploading.

5. The submission system will be closed automatically by 11:59pm on Friday 16/10/2020. Please submit on time. Penalty applies for late submission.

Assignment demonstration:

You are required to present in tutorial class in week 13 to demonstrate your assignment.