Cairo University
Faculty of Computers and
Information

Information Technology Department
IT423 - Information and Computers Networks Security
Spring 2015

Lab Assignment (4)

Assignment deadline: - Wednesday 30 November 2022

"I'm very pleased that the authors have succeeded in creating a highly valuable introduction to the subject of applied cryptography. I hope that it can serve as a guide for practitioners to build more secure systems based on cryptography, and as a stepping stone for future researchers to explore the exciting world of cryptography and its applications"

Implement AES Algorithm encryption and decryption:-

Input: -

1- Plain text → given plain text with any size to be divided into blocks of 16 characters
2- Key → 32 Hexa-decimals (i.e. 128 bits)

Output1 from encryption: - Cipher as Characters

Special Cases:-

Input Handling:-

- Your code must handle that plaintext size is of any size not only 16 characters. If the plain text size is less than 16 characters your code should handle that by adding special characters and if the plain text size is more than 16 characters your code should also handle that by dividing plain text to blocks of size 16.
- Your code must handle that key size must be 16 hexa-decimals by displaying error message and request another key from user.

Grading Criteria: - (You should display each step below to get its mark)

Total mark: - 25 marks (20 for encryption part and 5 for Decryption part)

Input handling: - 3 marks
Plain text size < 16 → 0.5 mark
Plain text size >16 → 2 mark
Key handling→ 0.5 mark

Key Generation 5 marks divided as follows:-
1- Word Rotation---> 1mark
2- Word Substitution --> 1mark
3- XOR with round constant ---> 1mark
4- XOR to generate 4 word sub-key per round---> 1 mark
5- 11 sub-keys---> 1 mark

Encryption 12 marks divided as follows:-

1- Initial key addition ---> 0.5 mark
2- 10 rounds----------> 2 marks
3- Each round (7.5 marks) divided as follows:-
   3.1. Byte Substitution ---> 1 mark
   3.2. Shift Rows ---> 1 mark
   3.3. Mix columns (5 marks) divided as follows:-
      3.3.1. Individual element calculation (3.5 mark) divided as:-
         - Elements multiplication---> 1 mark
         - Elements XOR---> 1 mark
         - Element reduction---> 1.5 mark
      3.3.2. Complete final matrix ---> 1.5 mark
   3.4. Key addition -----> 0.5 mark
4- Last Round no mix columns -----> 1 mark
5- Display output in hexa-decimal -----> 0.5 mark
6- Display output in characters -----> 0.5 mark

Decryption 5 marks