|  |  |
| --- | --- |
| Cairo University  Faculty of Computers and artificial intelligence Information Technology Department  Information and Computers Networks Security |  |

**Lab Assignment (2)**

**Assignment deadline: -** week start 3 December 2023

“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 DES Algorithm encryption and decryption: -

**Input: -**

1-Plain text 🡪 given plain text with any size

2- Key 🡪 8 Characters

**Output1 from encryption: -** Cipher as ASCII characters or Hexa or Decimal

**Special Cases:-**

**Input Handling:-**

* Your code must handle that plaintext size is of any size not only 8 characters. If the plain text size is less than 8 characters your code should handle that by adding special characters and if the plain text size is more than 8 characters your code should also handle that by dividing plain text to blocks of size 8.
* Your code must handle that key size must be 8 characters by displaying error message and request another key from user.

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

|  |
| --- |
| **Total mark: -** 20 marks  **Input handling: - 3 marks**  Plain text size < 8 🡪 0.5 mark  Plain text size >8 🡪 2 mark  Key handling🡪 0.5 mark  **Key Generation 4 marks divided as follows:-** 1- Permutated choice1---> 1mark 2- Left shift --> 1mark 3- Permutated choice-2 ---> 1mark 4- Repeat step 2 and 3 to generate the 16 keys---> 1 mark  **Encryption 8 marks divided as follows:-**   1. Initial permutation ---> 0.5 mark   2- 16 rounds-----------> 2 marks  Each round (4.5 marks) divided as follows: -   Expansion ---> 0.5 mark  Xor (key, result of expansion) ---> 0.5 mark  SBoxes ----> 2 marks  Permutation -----> 0.5 mark  Xor (result of permutation and left) -----> 0.5 mark  Left and Right swap ---> 0.5 mark   1. 32 bit swap------> 0.5 mark 2. Inverse initial permutation-----> 0.5 mark   **Decryption 5 marks** |