Assignment 2

Problem Submission Rules:

1) **Detection of plagiarism will result in Failing grade. Students must do this assignment by themselves.**
2) **After completion, your work must be submitted to an assignment folder in D2L by a corresponding deadline.**
3) **Late assignments will be accepted up to 24 hours after the due date for 50% credit. Assignments submitted more than 24 hours late will not be accepted for credit.**
4) **It is much better to submit a partial/failed-attempt solution than none. Include the circumstances of the incompletion in your report.**

Problems:

The aim of this assignment is to implement a Feistel cipher round function which consists of the following steps:

1. **Implementing a Feistel Cipher – 70 points**

Step 1: The function takes as input 8 bits and the 4-bit key k.
Step 2: The binary is divided into two halves (L_0 and R_0).
Step 3: The function computes $L_1 = R_0$ and $R_1 = L0 \oplus F(R_0, k)$, where

$$F(R_0, k) = 2 \times R_0^k \; mod \; 2^4$$

Step 4: The function performs a swapping of L_1 and R_1, then outputs $R_1 || L_1$.

2. **Combining with Assignment 1 – 20 points**

Improve your implementation for 1 by using your Text Converter, so it can handle a string from a user and output a string.

3. **Make some test codes to show the correctness of your implementation – 10 points**

Note: It is recommended to exchange a ciphertext generated by the implementation with your friend and check the decryption algorithm successfully recovers the original plaintext (you can use the discussion section in D2L).

Complier requirement:

The text converter must be implemented using Python version 3.9.x or higher. Students must use Python official libraries that are accessible from the webpage (https://docs.python.org/3/library/index.html). All used libraries and their purpose should be described in the report.

Submission instructions:

Please submit your deliverables to the D2L Assignments folder:

(a) **"HW 2"**: create a txt file, copy and paste your entire Python code, save, and then submit with a written report explaining your implementation. The report should have some test inputs and screenshots of execution results, which verify the correctness of your implementation.

Once you submit, D2L will perform a similarity check for your submission and show you the result. Your similarity score must be lower than 50% unless valid reasons for a high score described in the report. Otherwise, (the score -50%) will be deducted.