

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder

Assignment 4 Corrected

Programming project: Simplified DES, part 1

30 points

In either Java ≥ 8 or Python ≥ 3.7 implement one round of encryption of the textbook's simplified DES scheme. Write a program called `SDESRound.java` or `sdesround.py` so that it contains:

- a method called `encryptRound(plaintext, subkey)` where the plaintext and the subkey are both integers. As specified in section 7.2 of the text, a plaintext contains 12 bits and, so is in the range 0 to 4095, and the subkey contains 8 bits, and so in the range 0 to 255. This method performs one round of the simplified DES scheme and returns the ciphertext after that round.
- a main method that takes a plaintext integer and a subkey integer as command line parameters, calls the encryption method, and prints the resulting ciphertext. I will run your code as follows:
 - `python sdesround.py 128 250`
 - `java SDESRound 128 250`

Here is an updated table with sample inputs and the expected output.

Plaintext Subkey Ciphertext

0	0	44
0	85	33
0	170	48
0	255	18
1365	0	1390
1365	85	1379
1365	170	1360
1365	255	1398
2730	0	2697
2730	85	2735
2730	170	2716
2730	255	2705
4095	0	4067
4095	85	4047
4095	170	4062

Submission instructions

Please make sure your name appears in comments at the top of the source file. Submit the .java or .py file (not zipped!) to the D2L submission folder provided for it.

Document last updated on February 4th, 2021.

Assignment Project Exam Help

<https://powcoder.com>

Add WeChat powcoder