Introduction of Information Security

HW2

Before That

Q&A

- The key of “Rail Fence” is a number of rows or columns?
  - I made a mistake… It is row.
- In “Playfair”, if a pair a repeated letter, we need to insert filler like ‘X’. But what if the duplicate letter is ‘X’?
  - The case will not be in test cases.
- If the key is English letters, it will be upper or lower?
  - Lower, in case you can handle both.
- Can I use the lib which is not used for encryption?
  - No, otherwise my test environment is hard to set up. BTW, all standard lib is ok.
- How are the scores calculated?
  - Report 10 points, the other 90 points are divided between each test case. The number of test case is unsure. Other violations are additionally deductions.

Back to HW2

Assignments

- Two people in a group, one encrypts and the other decrypts
- DES implementation
  - Block size: 64 bits
  - Key size: 64 bits
- Report
  - Simple description how you implement

Notes

- C/Cpp/Python
- Can NOT use external lib (std lib is ok)
- I/O format
  - encrypt.o/decrypt.o –i [input] –k [key]
  - python3 encrypt.py/decrypt.py –i [input] –k [key]
    - Ex: *encrypt.o –i 0x456 –k 0x123*
    - *Ex: python3 encrypt.py –i 0x456 –k 0x123*
  - All input is “Hex”, the leading of the input/key has “0x”, and similarly, the leading of your output must have “0x”. If there are English character in the hex number, please output upper case.
- Report format
  - File name: Report.pdf
  - Submit on Moodle, each term submits one report. Please write down your student ID and who finished encryption, who finished decryption.

Additions

- Using “argv/argc” instead of “input/scanf/cin”.
- If the input size of block/key is less than 64 bits, please make up zero leading automatically, the same with output.
  - 0x123 -> 0x0000000000000123
  - Out of 64 bits will not in test case.
- Output to STDOUT(print/printf/cout). Please do not have unnecessary characters before and after the answer, and don’t use the function what will affect the automatic judge, such as system(“pause”).
- The runtime environment is Linux, you can test in yourself in case there is a compilation error.
- No public test case.
- Make sure your GitHub account and repo name are correct, penalty if TA contacts you for the assignment.

Info

- Deadline: 2022/4/5 23:55
- Contact: M11015028@mail.ntust.edu.tw

GitHub repo

110-Information-Security
|
----HW1
|
----HW2
|
----HW3
...