Introduction to Cryptography, Spring 2024

Homework 2

Due: 3/19/2024 (Tuesday)

Notes:

(1) For Part A, submit a “hardcopy” right after the class on the due day.

(2) For any question about the online judge system Formosa OJ, consult TA’s.

(3) TAs will run plagiarism check on your submitted programs. Write your own code and do not copy from others or anywhere.

Part A: Written exercises

1. Decrypt the following ciphertext that is generated by the Vigenere autokey cipher with keyword=apple:

   `cgnaxqcmvr wd wtrmjmfmmek`

2. Consider the one-time pad cipher with a skewed key distribution. Assume that the plaintext M is 2-bit long with distribution Pr[M=00]=0.2, Pr[M=01]=0.25, Pr[M=10]=0.4 and Pr[M=11]=0.15 and the key is picked with distribution Pr[K=00]=0.2, Pr[K=01]=0.35, Pr[K=10]=0.15 and Pr[K=11]=0.3.
   a) What is the distribution of the ciphertext $C=M\oplus K$?
   b) What is the deduced plaintext distribution after a ciphertext C=10 is observed? That is, to compute $\Pr[M=b_1b_2|C=10]$ for $b_1, b_2\in\{0,1\}$
   c) If you intercept a ciphertext C=11, what would you guess about the plaintext M? Explain the reason.

Part B: Programming

1. This homework is to implement DES, which encrypts a 64-bit plaintext block to a 64-bit ciphertext block with a key of 64 bits (with parity bits). Do not call crypto library directly since you need to modify the code during the on-site test.
   a. Input format: an ordered pair of key and plaintext in characters, such as “12345678 Pachinko”. Each character is interpreted as its 8 bit-ASCII code, e.g., ‘A’ = 41 (Hex)
   b. Output format: 16 hex characters, such as “C45077C10E08B3D0” which is the ciphertext of the above key and plaintext.
   c. Use C++ programming language in order to use the Formosa Online Judge system.
2. Submission:
   a. Submit before 9:00am, 3/19 (Tuesday). The submission system will close on time.

    b. Submit a file DES.cpp to Formosa OJ (https://formosa.oj.cs.nycu.edu.tw/) with your own account.
    c. Your code needs to read the input from **stdin**, which contains 5 ordered pairs of key and plaintext, one in each line, such as, “12345678 Pachinko”.
    d. Output: print 5 lines of ciphertexts (in Hex) for the test data that are read from stdin.
    e. Formosa OJ will compile your code and judge it on the test data from stdin.
3. On-site test
    a. Test time: 5:30-9:00pm, 3/22 (Friday).
    b. Test site: Computer rooms (EC315、EC316、EC324)
    c. It is your responsibility to reserve sufficient time for completing the test. The system will close at 9 pm on time.
    d. You will be asked to modify your DES implementation, which is your submitted C++ file on Formosa OJ, according to the given specification.
    e. Your code needs to read the input from **stdin,** which has the same format as the submitted version. The output format is the same also.
4. Grade evaluation
    a. 50%: the submitted programs and test results
    b. 50%: correctness of the on-site test

Appendix: Join the course group on Formosa OJ

1. Please find the course "515611 密碼學概論" in the group list (https://formosa.oj.cs.nycu.edu.tw/groups/), and press the "Join" button.
2. **Important**: Login Formosa OJ by NYCU Oauth2. If you don't login by NYCU Oauth2, your username will not be the student ID and you won’t have any grade on this homework.