Introduction to Cryptography, Spring 2024

Homework 3: On-site Test

Time: 5:30-9:00pm, 4/1/2024 (Monday)

Problem:

We intercept a ciphertext C and try to decrypt it. By the help of the intelligence agency, we find the following information about the ciphertext:

a. C is encrypted from an intelligible message with characters from English characters, digits, space, ‘,’ and ‘.’.
b. The key is of form “Our key is: XXXX” (ASCII), where XXXX are 4 Hex symbols, such as F79F
c. The mode is CFB (2-byte feedback), CFB (4-byte feedback), or CFB (8-byte feedback)
d. The IV is “0000000000000000” (ASCII)
e. There is no padding.

Submission:

A. Input: a line of ciphertext in Hex from stdin, such as “3FD975AB…”
B. Output: a line of message (ASCII) to stdout