Introduction to Cryptography, Spring 2024

Homework 3 (updated)

Due: 3/29/2024 (Friday)

Notes:

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

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

Part A: Written Problems

1. Compute all generators of the multiplicative group Z_{11}^*

2. Compute the following with coefficients over Z_{13},
   a. $(8x^2 + 3x + 12) + (10x^2 + 5x + 3)$
   b. $(x^2 + 3x + 9)(5x^3 + 11x^2 + 7)$

3. Determine which of the following polynomials are irreducible over Z_2:
   a. $x^4 + x + 1$
   b. $x^4 + x^3 + x + 1$

4. Compute $(x^2 + x + 2)^{-1} \bmod x^3 + 2x^2 + 1$, where the coefficients are over Z_3.

5. In the discussion of MixColumns and InvMixColumns in AES, it was stated that b(x) = a^{-1}(y) mod (y^4 + 1), where a(y) = 03y^3 + 01y^2 + 01y + 02 and b(y) = 0By^3 + 0Dy^2 + 09y +0E. Show that this is true.

Part B: Programming Problem

This programming problem is to get familiar with the crypto library "Crypto++" for encoding and decoding messages in various encryption and padding modes.

I. Encrypt the following message (in ASCII, quotes are not included):
"AES is the US block cipher standard."
by key= "2357111317192329" (ASCII) and the following specifications:

Mode	Initial Vector (IV)	Padding method (see Wiki Padding for details)
ECB	-	PKCS padding
CBC	"1234567812345678" (ASCII)	One and Zeros Padding
CFB (feedback =2 bytes)	"9999999999999999" (ASCII)	No need

The output is in Hex format, such as "327E9ADE37…"

II. We intercept ciphertext blocks
"104839DE2B34D9BA96F6E054F79F865890B827381D22FC3388690794F0D08EB3" (Hex). By espionage, we know that it was encrypted from an intelligible message, which consists of English characters, digits and space, using a key from the key space of form "00000000000" (ASCII) concatenated with 5 ASCII digits, such as, "0000000000010007" (ASCII), in ECB mode and PKCS padding. Write a key searching code to find out the used key (ASCII) and encrypted message (ASCII). You need to handle execution exceptions when a wrong key is used for decryption during brute-force search.

III. The output of your program consists of **10** lines.

(1) the first three lines (Hex) are from (I);

(2) the next two lines are the **found** key (ASCII) and decrypted message (ASCII) from (II);

(3) **the last 5 lines are similar to the first 5 lines with the same parameters and settings except reading message (ASCII) for (I) and intercepted ciphertext (Hex) for (II) from stdin.**

IV. Test data: plaintext = "Hello World!" (ASCII) and key is "1234567890ABCDEF" (ASCII)

A. ECB, PKCS padding → d5 23 32 6c 27 ee 0f 21 65 c7 69 6b 36 f2 68 8e

B. CBC, IV="0000000000000000" (ASCII), Zeros Padding
→ 4c 85 5d 63 17 60 8f 8d d3 94 61 e5 bc c9 40 b8

C. CFB, IV="0000000000000000" (ASCII), block size=4 bytes → 36 db 74 5b 3b 6d a6 9a bf 5f eb 23

V. Submission:

A. Submit before 12:01pm, 3/29 (Friday). The submission system will close on time.

B. Submit a file AES.cpp to Formosa OJ with your own account.

C. Read in two lines from stdin: one is the message (ASCII) for (I) and the other is the intercepted ciphertext (Hex) for (II)

D. Output: print **10** lines as specified above.

E. Formosa OJ will compile your code and judge the result.

VI. On-site test

A. Test time: 5:30-9:00pm, 4/1 (Monday).

B. Test site: Computer rooms (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 code by the given specification and submit it to Formosa OJ for judging.

VII. Grade evaluation

A. 50%: the submitted programs and test results

B. 50%: correctness of the on-site test