Introduction to Cryptography, Fall 2021

Homework 2

Due: 5pm, 10/19/2021 (Wed)

Part 1: Written Problems

For this part, submit your answer to E3 with filename: “youid”.pdf

1. For polynomial arithmetic with specified coefficient fields, perform the following calculation:
   a. $(x^2 + 7x + 9)(2x^3 + 9x^2 + 5)$ over GF(11)
   b. $(2x^5 + 3x + 2) \bmod (5x^3 + 4)$ over GF(7)
   c. $\gcd(x^4 + 8x^3 + 7x + 8, 2x^3 + 9x^2 + 10x + 1)$ over GF(11)
   d. $(x^3+x+1)^{-1} \bmod x^4+x+1$ over GF(2)
2. Determine which of the following polynomials are reducible over GF(2).
   a. $x^3 + x + 1$
   b. $x^4 + x^2 + x + 1$
3. In the discussion of MixColumns and InvMixColumns in AES, it is stated that $b(y) = a^{-1}(y) \bmod (y^4 + 1)$, where $a(y) = \{03\}y^3 + \{01\}y^2 + \{01\}y + \{02\}$ and $b(y) = \{0B\}y^3 + \{0D\}y^2 + \{09\}y + \{0E\}$. Show that this is true.

Part 2: DES Programming

This part is to implement DES core function, which encrypts a 64-bit plaintext to a 64-bit block ciphertext with a 64-bit key (with parity bits).

1. Input format: the input is an ordered pair of keys and plaintexts in ASCII characters, such as, ‘a’ = 01100001 (Bit) = 61 (Hex)
2. Output format: 16 hex characters, such as AE184796707E59FB.
3. You can use the following key-plaintext-ciphertext tuple as a test sample for correctness: “security”, “Hi Mary!” and “303B1E1CBA103695”.
4. Use C or C++ to write your code.
5. Submission to E3 with two files.
   a. The source code file with name: des.cpp or des.c.
   b. The output file “des-out.txt” that contains 5 lines of plaintexts (in ASCII) for the ordered pairs of key and ciphertext (one pair per line) from the file “DES-Key-Ciphertext.txt”.

Part 3: Use Crypto++ for AES

This part is to use the crypto library "Crypto++" to encode messages in various encryption and padding modes. The purpose is to get familiar with AES function calls and parameter setting. Please find the related library and programming environment (e.g. Visual Studio) information on the Internet.

I. Encrypt the following 36-byte message (in ASCII, quotes are not included.)

`"AES is the US block cipher standard."`

by the key "keyis84932731830" (ASCII) and the following specifications.

Mode	Initial Vector (IV)	Output form	Padding method
CFB (block size = 4 bytes)	0000 0000 0000 0000 (ASCII)	Hex	no padding
CBC	0000 0000 0000 0000 (ASCII)	Hex	Zeros Padding
CBC	9999 9999 9999 9999 (ASCII)	Hex	PKCS#7
ECB	-	Hex	PKCS#7

II. Test data: Plaintext = "Hello World!" (ASCII) and key="1234567890ABCDEF" (ASCII) .

A. CFB, IV=0000 0000 0000 0000, block size=4 bytes → 36 db 74 5b 3b 6d a6 9a bf 5f eb 23

B. CBC, IV=0000 0000 0000 0000, Zeros Padding
→ 4c 85 5d 63 17 60 8f 8d d3 94 61 e5 bc c9 40 b8

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

III. Submission: you need to upload two files to E3.

A. aes.cpp or aes.c: the program of generating the answers.

B. aes-out.txt: 4 lines of ciphertexts (in Hex).

On-site test (detail to be announced)

- Test time: 10/20, 10/21
- Test venue: to be announced.
- For DES, TA will ask you to modify your DES program and test it on the given data on the spot.
- For AES, TA will announce the test data and check the results on the spot.

Grading

- If you fail the on-site test, you fail the programming parts of this homework.
- TA will run a plagiarism checker on your programs. So, write your own code, do not copy from others or anywhere.