Introduction to Cryptography, Spring 2024

Homework 3

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 $b(x) = a^{-1}(y) \bmod (y^4 + 1)$, 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 5 lines: the first three lines (Hex) are from (I), the last two lines are the used key (ASCII) and decrypted message (ASCII) from (II)

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. There is no input to your code.
   D. Output: print 5 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

Part A

2.(a)

$$\begin{array}{rrr} 8 & 3 & 12 \\ 10 & 5 & 3 \\ \hline 18 & 8 & 15 \end{array}$$

$\Rightarrow (8x^2+3x+12)+(10x^2+5x+3)$
$\equiv 18x^2+8x+15$
$\equiv 5x^2+8x+2$ over $\mathbb{Z}_{13}$

2.(b)

$$\begin{array}{rrrrrr} & & & 1 & 3 & 9 \\ & & 5 & 11 & 0 & 7 \\ \hline & & & 7 & 21 & 63 \\ & 11 & 33 & 99 & & \\ 5 & 15 & 45 & & & \\ \hline 5 & 26 & 78 & 106 & 21 & 63 \end{array}$$

$(x^2+3x+9)(5x^3+11x^2+7)$
$\equiv 5x^5+26x^4+78x^3+106x^2+21x+63$
$\equiv 5x^5+2x^2+8x+11$ over $\mathbb{Z}_{13}$

3.(b) $x^4+x^3+x+1=(x+1)(x^3+1)$
$\Rightarrow x^4+x^3+x+1$ is reducible over $\mathbb{Z}_2$

(a) Claim: x^4+x+1 : irreducible over $\mathbb{Z}_2$

pf Case 1: $x^4+x+1\equiv(ax+b)(cx^3+dx^2+ex+f)$ over $\mathbb{Z}_2$

WLOH, $a,b,c,d,e,f=0$ or 1

$$\Rightarrow \begin{cases} x^4: ac\equiv 1 & \Rightarrow a=c=1 \\ x^3: bc+ad\equiv 0 \\ x^2: bd+ae\equiv 0 \\ x: be+af\equiv 1 \\ x^0: bf\equiv 1 & \Rightarrow b=f=1 \end{cases}$$

$$\Rightarrow \begin{cases} x^3: 1+d\equiv 0 \\ x^2: d+e\equiv 0 \\ x: e+1\equiv 1 \end{cases} \Rightarrow \begin{cases} d=1 \\ e=1 \end{cases} \Rightarrow 2\equiv 1 \ ※$$

代入

$\Rightarrow$ case 1 failed.

Case 2: $(x^4+x+1) \equiv (ax^2+bx+c)(dx^2+ex+f)$ over $\mathbb{Z}_2$

WLOH, $a,b,c,d,e,f = 0$ or 1

$$\Rightarrow \begin{cases} x^4: ab \equiv 1 \\ x^3: ae+bd \equiv 0 \\ x^2: af+be+cd \equiv 0 \\ x: ce+bf \equiv 1 \\ x^0: cf \equiv 1 \end{cases} \Rightarrow \begin{cases} a=1 \\ b=1 \\ c=1 \\ f=1 \end{cases}$$

$$\Rightarrow \begin{cases} x^3: e+d \equiv 0 \\ x^2: 1+e+d \equiv 0 \\ x: e+1 \equiv 1 \end{cases} \Rightarrow 1+2(e+d) \equiv 0$$

$\Rightarrow 1 \equiv 0$ ※

$\Rightarrow$ case 2 failed

$\Rightarrow x^4+x+1$ is irreducible over $\mathbb{Z}_2$ $\square$

4. Step 1. Find $a(x)f(x)+b(x)m(x) \equiv \gcd(f(x), m(x))$

Step 2. Use property: $f^{-1}(x) \equiv a(x) \mod m(x)$

$(\because a(x)f(x)+b(x)m(x) \equiv a(x)f(x)\gcd^{-1}(f,m) \mod m(x))$

$\begin{cases} 1^{-1} \equiv 1 \\ 2^{-1} \equiv 2 \end{cases}$ over $\mathbb{Z}_3$

Let $f(x) = x^2+x+2$, $m(x) = x^3+2x^2+1$

Step 1.

i	r_i	q_i	x_i	y_i
-1	x^2+x+2		1	0
0	x^3+2x^2+1		0	1
1	x^2+x+2	0	1	0
2	2	$x+1$	$-(x+1)$	1

$$\begin{array}{r} x+1 \\ x^2+x+2 \overline{\big) x^3+2x^2+0x+1} \\ x^3+x^2+2x \\ \hline x^2+x+1 \\ x^2+x+2 \\ \hline 2 \end{array}$$

$\Rightarrow -(x+1)(x^2+x+2)+(x^3+2x^2+1) \equiv 2$

$\Rightarrow -2(x+1)(x^2+x+2)+2(x^3+2x^2+1) \equiv 2 \cdot 2$ (multiply $2^{-1}=2$)

$\Rightarrow \boxed{-2(x+1)}(x^2+x+2) \equiv 1 \pmod{x^3+2x^2+1}$

$\Rightarrow (x^2+x+2)^{-1} \equiv -2(x+1)$

$\equiv x+1 \mod (x^3+2x^2+1)$ $\square$

5. check $a(y)b(x) \equiv 1 \pmod{y^4+1}$

$$\Leftrightarrow (0B\,y^3 + 0D\,y^2 + 09\,y + 0E)(03x^3 + 01x^2 + 01x + 02)_H \equiv 1_H \pmod{y^4+1}$$

$$\Leftrightarrow (11y^3 + 13y^2 + 9y + 14)(3y^3 + y^2 + y + 2)_{10} \equiv 1_{10} \pmod{y^4+1}$$

$$\Leftrightarrow 33y^6 + 50y^5 + 51y^4 + 86y^3 + 49y^2 + 32y + 28 \equiv 1 \pmod{y^4+1}$$

$$\Leftrightarrow y^6 + y^4 + y^2 \equiv 1 \pmod{y^4+1} \quad (\because \text{over } \mathbb{Z}_2)$$

$$\Leftrightarrow y^2(y^4+1) \equiv y^4+1 \pmod{y^4+1} \quad (\because -y^4 \equiv y^4 \text{ over } \mathbb{Z}_2)$$

$$\Leftrightarrow 0 \equiv 0 \pmod{y^4+1} \quad (\because \bmod y^4+1) \quad \square$$

1. We need to find all

$a \in \mathbb{Z}_{11}^*$ s.t. $\{a^k\}_{k=1}^{k=11} = \mathbb{Z}_{11}^*$

$\Rightarrow$ All $a = \{2, 6, 7, 8\}$

test.py - /Users/origamyee/Desktop/test.py (3.12.

```python
Z_11_star = [i for i in range(11) if i > 0]
candidate_points = Z_11_star
ans = []

for t in candidate_points:
    tempGroup = [t]
    for j in range(10):
        tempGroup.append((tempGroup[-1] * t) % 11)
    print(tempGroup)
    flag = True
    for e in Z_11_star:
        smallFlag = False
        for te in tempGroup:
            if e == te:
                smallFlag = True
        if smallFlag == False:
            flag = False
    if flag == True:
        ans.append(t)

print(ans)
```

IDLE Shell 3

```
Python 3.12.0 (v3.12.0:0fb18b02c8, Oct  2
300.0.29.30)] on darwin
Type "help", "copyright", "credits" or "l
>>>
==================== RESTART: /Users/origa
[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1]
[2, 4, 8, 5, 10, 9, 7, 3, 6, 1, 2]
[3, 9, 5, 4, 1, 3, 9, 5, 4, 1, 3]
[4, 5, 9, 3, 1, 4, 5, 9, 3, 1, 4]
[5, 3, 4, 9, 1, 5, 3, 4, 9, 1, 5]
[6, 3, 7, 9, 10, 5, 8, 4, 2, 1, 6]
[7, 5, 2, 3, 10, 4, 6, 9, 8, 1, 7]
[8, 9, 6, 4, 10, 3, 2, 5, 7, 1, 8]
[9, 4, 3, 5, 1, 9, 4, 3, 5, 1, 9]
[10, 1, 10, 1, 10, 1, 10, 1, 10, 1, 10]
[2, 6, 7, 8]
>>>
```