Київський національний університет імені Тараса Шевченка

Факультет комп’ютерних наук та кібернетики

Кафедра інтелектуальних програмних систем

Математичні основи захисту інформації

Лабораторна робота №11

“Протокол обміну ключами Діффі-Хелмана і Шаміра. Побудова поля за допомогою незвідного многочлена”

Виконали студенти 3-го курсу

Групи ІПС-32

Роботу виконали:

Ольховатий Ігор

Ковальов Володимир

Тряско Софія

Цілинко Олександр

Бондар Юлія

Волик Артем

Київ 2023

Тема: побудувати скінченне поля порядку 3^4. У цьому полі знайти циклічну групу порядку 80. Запрограмувати протокол Діффі-Хелмана і протокол Шаміра

Побудова скінченного поля порядку $3^4 = 81$

Для цього скористаємось теоремою про розмір поля побудованного за допомогою незвідного многочлена. Розглянемо поле F_p – скінченне поле порядку p.

f – незвідний поліном степеня n над полем F_p. Тоді $|F_{f(x)}| = p^n$

Виберемо довільний незвідний многочлен

$f(x) = x^4 + x + 2$

Доведемо, що даний многочлен є незвідним.

Спосіб 1

Помітимо, що $x^{3^4} = x\ (mod\ f(x))$

Дільники 4: 2

1)

$GCD(f(x),\ x^{3^{4/2}} - x\ mod\ f(x)) = GCD(f(x),\ x^9 - x\ mod\ f(x)) = GCD(f(x), x^3 + x^2) = 1$

Отже многочлен незвідний

Спосіб 2

Припустимо, супротивне. По-перше, даний поліном не має коренів над F_3 – очевидно.

Отже, його не можливо розкласти як добуток многочленів 1 степенів і не можна розкласти як добуток многочлена 3 і 1 степені, бо тоді б він мав корінь, а він не має. Отже теоретично його можна розкласти як добуток многочленів 2 степенів.

$x^4 + x + 2 = (a_1x^2 + b_1x + c_1)(a_2x^2 + b_2x + c_2)$

Використаємо метод невизначених коефіцієнтів

$x^4: 1 = a_1a_2$

$x^3: 0 = a_1b_2 + a_2b_1$

$x^2: 0 = a_1c_2 + b_1b_2 + a_2c_1$

$x: 1 = b_1c_2 + c_1b_2$

$2 = c_1c_2$

З першого рівня перебором отримаємо, два розв'язки

$\{a_1 = 1\ a_2 = 1\}$ або $\{a_1 = 2\ a_2 = 2\}$ З останнього рівняння отримаємо, що

$\{c_1 = 1\ c_2 = 2\}$ або $\{c_1 = 2\ c_2 = 1\}$

Зробимо повний перебір

1) $a_1 = 1\ a_2 = 1\ c_1 = 1\ c_2 = 2$

$0 = b_2 + b_1$

$0 = 1 + b_1b_2 + 2 = b_1b_2$

$1 = 2b_1 + b_2$

З цих рівнянь отримаємо, що $b_1 = b_2 = 0$- з перший двох рівнянь, але тоді третя рівність не виконується

2) $a_1 = 2\, a_2 = 2\, c_1 = 1\, c_2 = 2$

$0 = 2b_2 + 2b_1$

$0 = 2 + b_1 b_2 + 4 = b_1 b_2$

$1 = 2b_1 + b_2$

З цих рівнянь отримаємо, що $b_1 = b_2 = 0$- з перший двох рівнянь, але тоді третя рівність не виконується

3) $a_1 = 1\, a_2 = 1\, c_1 = 2\, c_2 = 1$

$0 = b_2 + b_1$

$0 = 2 + b_1 b_2 + 1 = b_1 b_2$

$1 = 2b_1 + b_2$

З цих рівнянь отримаємо, що $b_1 = b_2 = 0$- з перший двох рівнянь, але тоді третя рівність не виконується

4) $a_1 = 2\, a_2 = 2\, c_1 = 2\, c_2 = 1$

$0 = 2b_2 + 2b_1$

$0 = 4 + b_1 b_2 + 2 = b_1 b_2$

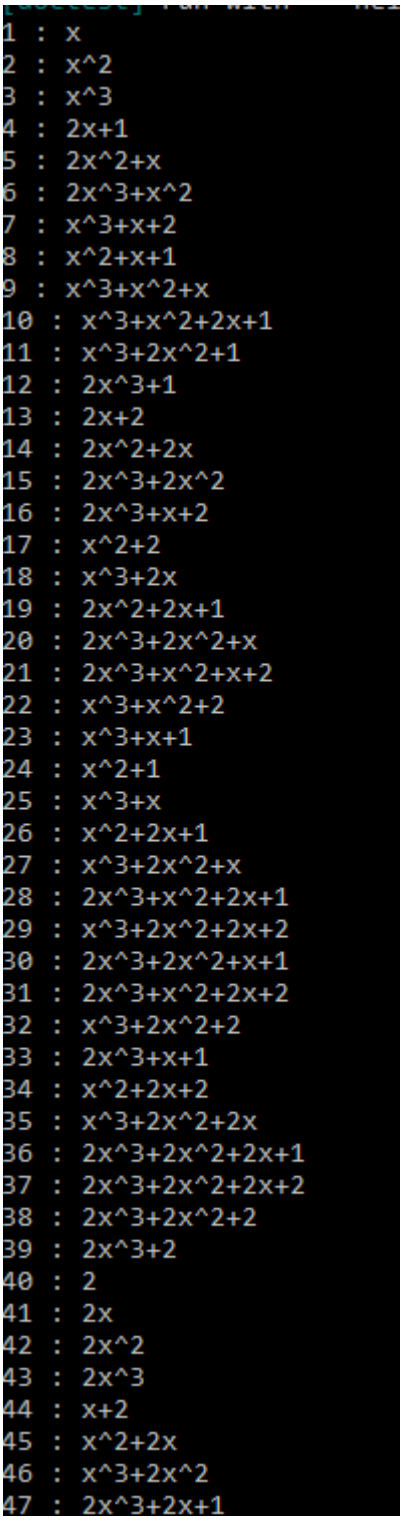
$1 = 1b_1 + 2b_2$

З цих рівнянь отримаємо, що $b_1 = b_2 = 0$- з перший двох рівнянь, але тоді третя рівність не виконується

Отже дійсно даний поліном є незвідним

Знайдемо елемент, який є генератором цієї групи.

Помітимо, що елемент x є генератором цієї групи



```
48 : 2x^2+2x+2
49 : 2x^3+2x^2+2x
50 : 2x^3+2x^2+x+2
51 : 2x^3+x^2+2
52 : x^3+2
53 : x+1
54 : x^2+x
55 : x^3+x^2
56 : x^3+2x+1
57 : 2x^2+1
58 : 2x^3+x
59 : x^2+x+2
60 : x^3+x^2+2x
61 : x^3+2x^2+2x+1
62 : 2x^3+2x^2+1
63 : 2x^3+2x+2
64 : 2x^2+2
65 : 2x^3+2x
66 : 2x^2+x+2
67 : 2x^3+x^2+2x
68 : x^3+2x^2+x+2
69 : 2x^3+x^2+x+1
70 : x^3+x^2+2x+2
71 : x^3+2x^2+x+1
72 : 2x^3+x^2+1
73 : x^3+2x+2
74 : 2x^2+x+1
75 : 2x^3+x^2+x
76 : x^3+x^2+x+2
77 : x^3+x^2+x+1
78 : x^3+x^2+1
79 : x^3+1
80 : 1
```

Отже ми знайшли генератор нашої групи

$g = x \mid < g > \mid = 80$

Цей елемент має номер 3

Протокол обміну ключами Діффі-Хелмана

Обом абонентам відомі числа g, p^n . Аліса випадковим чином генерує число a і обраховує $A = g^a \, mod \, p^n$ а Боб обраховує число $B = g^b \, mod \, p^n$. Потім за допомогою відкритого каналу вони обмінюються повідомленням і Аліса обраховує B^a , а Боб A^b ці числа рівні і це стає їх спільним ключем

Приклад

Беремо $p = 3, \; g = x$ (номер 3), $n = 4$

Аліса

$a = 73$

$A = g^a = x\text{^}3 + 2x + 2 = 35$ (цей поліном має 35 номер)

$B^a = x^2 + 2x + 1 = 16$ (цей поліном має номер 16)

Боб

$b = 42$

$B = g^b = 2x^2 = 18$ (цей поліном має номер 18)

$A^b = x^2 + 2x + 1 = 16$ (цей поліном має номер 16)

Ми дійсно переконались, що ключі співпадають

Код

```
# This is a sample Python script.

# Press Shift+F10 to execute it or replace it with your code.
# Press Double Shift to search everywhere for classes, files, tool
windows, actions, and settings.

import random
from sympy import isprime

def power(a:int, d:int,m:int):
    d_binary = bin(d)

    d_binary = d_binary[2:]
    y =1
    s = a

    for i in reversed(d_binary):
        if i == '1':
            y = (y*s)%m

        s = (s*s)%m

    return y
def generate_large_prime(bits):
    while True:
        candidate = random.getrandbits(bits)

        candidate |= (1 << bits - 1) | 1

        if isprime(candidate):
            return candidate

# Example: Generate a 1024-bit prime number
bits = 1024
prime_number = generate_large_prime(bits)

# Press the green button in the gutter to run the script.
if __name__ == '__main__':
    a = input()

    b = input()

    p = generate_large_prime(bits)
```

```
g = 64
A = power(g,a,p)
B = power(g,b,p)

if power(A,b,p) == power(B,a,p):
    print('secret key: ' + power(A,b,p))
```

Протокол обміну ключами Шаміра

За допомогою нього зашифруємо деяке повідомлення “`The extraction point is a nondescript alley behind the concert hall`”

Крок 0
Буква для шифрації: T
Аліса відправляє: 2974
Боб відправляє: 6743
Аліса отримує: 1573
Боб дещифрує: T
Крок 1
Буква для шифрації: H
Аліса відправляє: 1069
Боб відправляє: 5671
Аліса отримує: 3702
Боб дещифрує: H
Крок 2
Буква для шифрації: E
Аліса відправляє: 1211
Боб відправляє: 5657
Аліса отримує: 5163
Боб дещифрує: E
Крок 3
Буква для шифрації: E
Аліса відправляє: 446
Боб відправляє: 14
Аліса отримує: 3625
Боб дещифрує: E
Крок 4
Буква для шифрації: X
Аліса відправляє: 5207
Боб відправляє: 1186
Аліса отримує: 2407
Боб дещифрує: X
Крок 5

Буква для шифрації: T
Аліса відправляє: 4314
Боб відправляє: 5258
Аліса отримує: 6462
Боб дещифрує: T
Крок 6
Буква для шифрації: R
Аліса відправляє: 4586
Боб відправляє: 6388
Аліса отримує: 1815
Боб дещифрує: R
Крок 7
Буква для шифрації: A
Аліса відправляє: 1
Боб відправляє: 1
Аліса отримує: 1
Боб дещифрує: A
Крок 8
Буква для шифрації: C
Аліса відправляє: 6756
Боб відправляє: 4991
Аліса отримує: 3777
Боб дещифрує: C
Крок 9
Буква для шифрації: T
Аліса відправляє: 7021
Боб відправляє: 396
Аліса отримує: 3042
Боб дещифрує: T
Крок 10
Буква для шифрації: I
Аліса відправляє: 5686
Боб відправляє: 27
Аліса отримує: 2267
Боб дещифрує: I
Крок 11
Буква для шифрації: O
Аліса відправляє: 3975
Боб відправляє: 4646
Аліса отримує: 5212
Боб дещифрує: O
Крок 12
Буква для шифрації: N
Аліса відправляє: 5842
Боб відправляє: 2277
Аліса отримує: 581
Боб дещифрує: N
Крок 13

Буква для шифрації: P
Аліса відправляє: 5675
Боб відправляє: 7010
Аліса отримує: 4263
Боб дещифрує: P
Крок 14
Буква для шифрації: O
Аліса відправляє: 5022
Боб відправляє: 3532
Аліса отримує: 481
Боб дещифрує: O
Крок 15
Буква для шифрації: I
Аліса відправляє: 5770
Боб відправляє: 5941
Аліса отримує: 4390
Боб дещифрує: I
Крок 16
Буква для шифрації: N
Аліса відправляє: 6251
Боб відправляє: 1389
Аліса отримує: 2907
Боб дещифрує: N
Крок 17
Буква для шифрації: T
Аліса відправляє: 6459
Боб відправляє: 1852
Аліса отримує: 6972
Боб дещифрує: T
Крок 18
Буква для шифрації: I
Аліса відправляє: 411
Боб відправляє: 4535
Аліса отримує: 5417
Боб дещифрує: I
Крок 19
Буква для шифрації: S
Аліса відправляє: 1908
Боб відправляє: 1451
Аліса отримує: 7103
Боб дещифрує: S
Крок 20
Буква для шифрації: A
Аліса відправляє: 1
Боб відправляє: 1
Аліса отримує: 1
Боб дещифрує: A
Крок 21

Буква для шифрації: N
Аліса відправляє: 5903
Боб відправляє: 1846
Аліса отримує: 7045
Боб дещифрує: N
Крок 22
Буква для шифрації: O
Аліса відправляє: 3814
Боб відправляє: 6821
Аліса отримує: 1214
Боб дещифрує: O
Крок 23
Буква для шифрації: N
Аліса відправляє: 5800
Боб відправляє: 4087
Аліса отримує: 6599
Боб дещифрує: N
Крок 24
Буква для шифрації: D
Аліса відправляє: 7014
Боб відправляє: 6135
Аліса отримує: 799
Боб дещифрує: D
Крок 25
Буква для шифрації: E
Аліса відправляє: 184
Боб відправляє: 3345
Аліса отримує: 5613
Боб дещифрує: E
Крок 26
Буква для шифрації: S
Аліса відправляє: 1340
Боб відправляє: 3722
Аліса отримує: 2503
Боб дещифрує: S
Крок 27
Буква для шифрації: C
Аліса відправляє: 2344
Боб відправляє: 2167
Аліса отримує: 5854
Боб дещифрує: C
Крок 28
Буква для шифрації: R
Аліса відправляє: 3456
Боб відправляє: 3907
Аліса отримує: 271
Боб дещифрує: R
Крок 29

Буква для шифрації: I
Аліса відправляє: 2796
Боб відправляє: 3671
Аліса отримує: 5323
Боб дещифрує: I
Крок 30
Буква для шифрації: P
Аліса відправляє: 4722
Боб відправляє: 2245
Аліса отримує: 6418
Боб дещифрує: P
Крок 31
Буква для шифрації: T
Аліса відправляє: 6453
Боб відправляє: 4682
Аліса отримує: 335
Боб дещифрує: T
Крок 32
Буква для шифрації: A
Аліса відправляє: 1
Боб відправляє: 1
Аліса отримує: 1
Боб дещифрує: A
Крок 33
Буква для шифрації: L
Аліса відправляє: 2436
Боб відправляє: 7015
Аліса отримує: 2900
Боб дещифрує: L
Крок 34
Буква для шифрації: L
Аліса відправляє: 1664
Боб відправляє: 1497
Аліса отримує: 227
Боб дещифрує: L
Крок 35
Буква для шифрації: E
Аліса відправляє: 4988
Боб відправляє: 4527
Аліса отримує: 6200
Боб дещифрує: E
Крок 36
Буква для шифрації: Y
Аліса відправляє: 3237
Боб відправляє: 4638
Аліса отримує: 5204
Боб дещифрує: Y
Крок 37

Буква для шифрації: B
Аліса відправляє: 3882
Боб відправляє: 2908
Аліса отримує: 1179
Боб дещифрує: B
Крок 38
Буква для шифрації: E
Аліса відправляє: 2589
Боб відправляє: 2142
Аліса отримує: 4829
Боб дещифрує: E
Крок 39
Буква для шифрації: H
Аліса відправляє: 2374
Боб відправляє: 5454
Аліса отримує: 4233
Боб дещифрує: H
Крок 40
Буква для шифрації: I
Аліса відправляє: 2304
Боб відправляє: 3708
Аліса отримує: 3329
Боб дещифрує: I
Крок 41
Буква для шифрації: N
Аліса відправляє: 2153
Боб відправляє: 1037
Аліса отримує: 1456
Боб дещифрує: N
Крок 42
Буква для шифрації: D
Аліса відправляє: 1187
Боб відправляє: 4316
Аліса отримує: 3788
Боб дещифрує: D
Крок 43
Буква для шифрації: T
Аліса відправляє: 5267
Боб відправляє: 5147
Аліса отримує: 6496
Боб дещифрує: T
Крок 44
Буква для шифрації: H
Аліса відправляє: 3771
Боб відправляє: 3109
Аліса отримує: 1608
Боб дещифрує: H
Крок 45

Буква для шифрації: E
Аліса відправляє: 4809
Боб відправляє: 4968
Аліса отримує: 2969
Боб дещифрує: E
Крок 46
Буква для шифрації: C
Аліса відправляє: 6348
Боб відправляє: 1071
Аліса отримує: 4746
Боб дещифрує: C
Крок 47
Буква для шифрації: O
Аліса відправляє: 2818
Боб відправляє: 94
Аліса отримує: 4418
Боб дещифрує: O
Крок 48
Буква для шифрації: N
Аліса відправляє: 5520
Боб відправляє: 6541
Аліса отримує: 1790
Боб дещифрує: N
Крок 49
Буква для шифрації: C
Аліса відправляє: 3289
Боб відправляє: 5096
Аліса отримує: 1024
Боб дещифрує: C
Крок 50
Буква для шифрації: E
Аліса відправляє: 1741
Боб відправляє: 6412
Аліса отримує: 1603
Боб дещифрує: E
Крок 51
Буква для шифрації: R
Аліса відправляє: 2644
Боб відправляє: 475
Аліса отримує: 6153
Боб дещифрує: R
Крок 52
Буква для шифрації: T
Аліса відправляє: 1586
Боб відправляє: 6233
Аліса отримує: 1736
Боб дещифрує: T
Крок 53

Буква для шифрації: H
Аліса відправляє: 186
Боб відправляє: 3963
Аліса отримує: 2491
Боб дещифрує: H
Крок 54
Буква для шифрації: A
Аліса відправляє: 1
Боб відправляє: 1
Аліса отримує: 1
Боб дещифрує: A
Крок 55
Буква для шифрації: L
Аліса відправляє: 950
Боб відправляє: 6443
Аліса отримує: 2505
Боб дещифрує: L
Крок 56
Буква для шифрації: L
Аліса відправляє: 2936
Боб відправляє: 3468
Аліса отримує: 2370
Боб дещифрує: L

Process finished with exit code 0

Бачимо, що Боб розшифрував усі букви коректно, отже алгоритм є вірним

```
# This is a sample Python script.

# Press Shift+F10 to execute it or replace it with your code.
# Press Double Shift to search everywhere for classes, files, tool
windows, actions, and settings.
alphabet_dict = {
    'A': 1, 'B': 2, 'C': 3, 'D': 4, 'E': 5,
    'F': 6, 'G': 7, 'H': 8, 'I': 9, 'J': 10,
    'K': 11, 'L': 12, 'M': 13, 'N': 14, 'O': 15,
    'P': 16, 'Q': 17, 'R': 18, 'S': 19, 'T': 20,
    'U': 21, 'V': 22, 'W': 23, 'X': 24, 'Y': 25,
    'Z': 26
}
import random
def inverse(a , p):
    for i in range(p):
        if (a*i)%(p-1) ==1:
            return i
def search(d : dict, target):
    for key in d.keys():
        if d[key] == target:
```

```
            return key
def power(a:int, d:int,m:int):
    d_binary = bin(d)

    d_binary = d_binary[2:]
    y =1
    s = a

    for i in reversed(d_binary):
        if i == '1':
            y = (y*s)%m

        s = (s*s)%m

    return y
def gcd(a,b):
    for i in range(1,min(a,b)):
        if a % i ==0 and b % i ==0 and i!=1:
            return False

    return True
def encrypt(M : int):
    p = 7187
    cA = random.randint(1, p)
    cB =  random.randint(1, p)
    while not (gcd(cA,p-1)):
        cA= random.randint(1, p)
    while not (gcd(cB,p-1)):
        cB= random.randint(1, p)

    dA = inverse(cA,p)
    dB = inverse(cB,p)

    x1 = power(M,cA,p)
    x2 = power(x1,cB,p)
    x3 = power(x2, dA, p)
    x4 = power(x3, dB, p)
    print('Аліса відправляє: ' + str(x1))
    print('Боб відправляє: ' + str(x2))
    print('Аліса отримує: ' + str(x3))
    print('Боб дещифрує: ' + str(search(alphabet_dict,x4)))



# Press the green button in the gutter to run the script.
if __name__ == '__main__':
  s = "THEEXTRACTIONPOINTISANONDESCRIPTALLEYBEHINDTHECONCERTHALL"
  for i in range(len(s)):
```

```
        print("Крок " + str(i))
        print('Буква для шифрації: ' + s[i])
        encrypt(alphabet_dict[s[i]])
```

Література

- Лекції з предмету “Математичні основи захисту інформації”
- https://ru.wikipedia.org/wiki/%D0%A2%D1%80%D1%91%D1%85%D1%8D%D1%82%D0%B0%D0%BF%D0%BD%D1%8B%D0%B9_%D0%BF%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D0%A8%D0%B0%D0%BC%D0%B8%D1%80%D0%B0
- https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D0%94%D0%B8%D1%84%D1%84%D0%B8_%E2%80%94_%D0%A5%D0%B5%D0%BB%D0%BB%D0%BC%D0%B0%D0%BD%D0%B0