- Konstantinos Filippou
- ics23044

Exercise 1

Προσδιορίστε την τάξη (order) όλων των στοιχείων των πολλαπλασιαστικών ομάδων:

- Z*5
- Z*13
- Z*17

Δημιουργήστε έναν πίνακα με δύο στήλες για κάθε ομάδα. Κάθε γραμμή να περιέχει στην πρώτη στήλη τα στοιχεία a∈Z*p και στη δεύτερη στήλη την τάξη **ord(a)**(υπόδειξη: προκειμένου να εξοικειωθείτε με τις κυκλικές ομάδες και τις ιδιότητές τους, υπολογίστε όλες τις τάξεις στο Z *5 "με το χέρι" και εν συνεχεία επαληθεύστε το αποτέλεσμα με κώδικα Sage).

Solution

Η ομάδα Z*5 είναι η ομάδα των μη μηδενικών στοιχείων του Z *5 με τη μορφή modulo 5

Δηλαδή Z*5 = {1,2,3,4}. Αρκεί να δείξουμε ότι a^k≡1(mod5) για κάθε στοιχείο a και k μικρότερος θετικός ακέραιος, για να βρούμε την τάξη του a.

Για το στοιχείο 1 η τάξη του είναι: 1^1 ≡ 1 mod 5. Άρα η τάξη του είναι 1.

Για το στοιχείο 2 η τάξη του είναι: 2^1 ≡ 2 (mod 5), 2^2 ≡ 4 (mod 5), 2^3 ≡ 3 (mod 5), 2^4 ≡ 1 (mod 5)

Για το στοιχείο 3 η τάξη του είναι: 3^1 ≡ 3 (mod 5), 3^2 ≡ 4 (mod 5). 3^3 ≡ 2 (mod 5), 3^4 ≡ 1 (mod 5)

Για το στοιχείο 4 η τάξη του είναι: 4^1 ≡ 4 (mod 5), 3^2 ≡ 1 (mod 5)

a	**ord(a)**
1	1
2	4
3	4
4	2

Για τις υπόλοιπες ομάδες (Z*13 και Z *17), τα στοιχεία τους {1...12} και {1..16}

Χρησιμοποιόντας sage για τις υπόλοιπες μέσω κώδικα προκύπτει ο πίνακας για Z*13:

a	**ord(a)**
1	1
2	12

a	ord(a)
3	3
4	6
5	4
6	12
7	12
8	4
9	3
10	6
11	12
12	2

Τέλος, προκύπτει ο πίνακας για Z*17:

a	ord(a)
1	1
2	8
3	16
4	4
5	16
6	16
7	16
8	8
9	8
10	16
11	16
12	16
13	4
14	16
15	8
16	2

Ο κώδικας που εφαρμόσαμε για επαλήθευση είναι:

```
p = 13
Zp = [a for a in range(1, p)]

print("a\tord(a)")
for a in Zp:
    order = Mod(a, p).multiplicative_order()
    print(f"{a}\t{order}")
```

```
a       ord(a)
1       1
2       12
3       3
4       6
5       4
6       12
7       12
8       4
9       3
10      6
11      12
12      2
```

```
p = 17
Zp = [a for a in range(1, p)]

print("a\tord(a)")
for a in Zp:
    order = Mod(a, p).multiplicative_order()
    print(f"{a}\t{order}")
```

```
a       ord(a)
1       1
2       8
3       16
4       4
5       16
6       16
7       16
8       8
9       8
10      16
11      16
12      16
13      4
14      16
15      8
16      2
```

Exercise 2

Υπολογίστε τα δύο δημόσια κλειδιά και το κλειδί συνεδρίας (session key) για το πρωτόκολλο DHKE με παραμέτρους **p = 467**, **g = 2**, και:

- **a = 3, b = 5**
- **a = 400 , b = 134**
- **a = 228, b = 57**

Σε όλες τις περιπτώσεις, εκτελέστε τον υπολογισμό του κλειδιού συνεδρίας τόσο στην πλευρά της Alice όσο και του Bob. Αυτός είναι ένας τρόπος να επαληθεύσετε την ορθότητα των υπολογισμών σας.

Solution

- A = g^a mod p = 2^3 mod 467 = 8

  B = g^b mod p = 2^5 mod 467 = 32

  KAB = A^b mod p = 8^5 mod 467 = 32768 mod 467 = 78 = B^a mod 467 = 32^3 mod 467 = 78

- A = 2^400 mod 467 = 137

  B = 2^134 mod 467 = 84

  KAB= 137^134 mod 467 = 90 = 84^400 mod 467 = 90
- A = 2^228 mod 467 = 394

  B = 2^57 mod 467 = 313

  KAB = 394^57 mod 467 = 206 = 313^228 mod 467 = 206

Exercise 3

Ολοκληρώστε και εκτελέστε τα 4 βήματα της δραστηριότητας Diffie-Hellman και παραθέστε το στιγμιότυπο της εκτέλεσής σας.

Solution

[64]:
```
def generate_parameters(bits):
    p=1
    while not is_prime(p):
        q = next_prime(ZZ.random_element(2^bits))
        p = 2*q + 1
    F = GF(p)
    while True:
        g = F.random_element()
        if g != 1 and g^2 != 1 and g^q != 1:
            break
    return (p,q,g,F)
```

[65]:
```
def public_private_pair(p,q,g,F):
    x = F(randint(2,p-2))
    X = g^x
    return(X,x)
```

[66]:
```
def generate_secret(X,y):
    Y = X^y
    return(Y)
```

[70]:
```
p, q, g, F = generate_parameters(100)
print(p, q)
print(g, F)

# Alice computes secret and public value
A, a = public_private_pair(p,q,g,F)
# Bob computes secret and public value
B, b = public_private_pair(p,q,g,F)
# Alice generates shared secret
generate_secret(A,b)
# Bob generates shared secret
generate_secret(B,a)
```

Exercise 4

Κρυπτογραφήστε τα ακόλουθα μηνύματα με το κρυπτοσύστημα Elgamal με παραμέτρους **p = 467** και **g = 2** . Στη συνέχεια αποκρυπτογραφήστε κάθε κρυπτοκείμενο δείχνοντας όλα τα βήματα.

- $k_{pr} = d = 105, i = 213, m = 33$
- $k_{pr} = d = 105, i = 123, m = 33$
- $k_{pr} = d = 300, i = 45, m = 248$
- $k_{pr} = d = 300, i = 47, m = 248$

Solution

- Κρυπτογράφηση:

  B = g^d mod p = 2^105 mod 467 = 444

  ks = B^i mod p = 444^213 mod 467 = 292

  c = ks * m mod p = 292 * 33 mod 467 = 296

  Αποκρυπτογράφηση:

  m = ks^-1 * c mod p = 292^-1 * 296 mod 467, βρίσκω τον αντίστροφο:

  467=292x1+175

  292 = 175 x1 + 117

  175 = 117 x1 + 58

  117 = 58x2 + 1

  58 = 1x58 + 0 υπόλοιπο 1 άρα υπάρχει αντίστροφος:

  Από το 4ο βήμα:

  1=117−58x2

  Αλλά 58= 175-117x1 οπότε:

  1=117−(175−117)x2=117−2x175+2x117=3x117−2x175

  Και 117 = 292 - 175 οπότε:

  1=3x(292−175)−2x175=3x292−3x175−2x175=3x292−5x175

  Και 175 = 467 - 292 οπότε:

  1=3x292−5x(467−292)=3x292−5x467+5x292=8x292−5x467

  Επομένως: 292^−1 ≡8 (mod467)

  Άρα: m = 8x296 mod 467 = 2368 mod 467 = 33

- Κρυπτογράφηση:

  B = g^d mod p = 2^105 mod 467 = 444

  ks = B^i mod p = 444^123 mod 467 = 278

  c = ks * m mod p = 278 * 33 mod 467 = 301

  Αποκρυπτογράφηση:

  m = ks^-1 * c mod p = 278^-1 * 301 mod 467, βρίσκω τον αντίστροφο:

  467=278x1+189

  278 = 189x1 + 89

  189 = 89x2 + 11

89 = 11x8 + 1

11 = 1x11 + 0 υπόλοιπο 1 άρα υπάρχει αντίστροφος:

Από το 4ο βήμα:

1=89−11x8

Αλλά 11 = 189 - 89 x 2, άρα:

1=89−(189−89x2)x8=89−189x8+89x16=89x17−189x8

Και 89 = 278 - 189, άρα:

1 = 17 x (278 - 189) - 8 x 189 = 17 x 278 - 17 x 189 - 8 x 189 = 17 x 278 - 25 x 189

Και 189 = 467 - 278 οπότε:

1 = 17 x 278 - 25 x (467 - 278) = 17 x 278 - 25 x 467 + 25 x 278 = 42 x 278 - 25 x 467

Επομένως: 278^-1 ≡ 42 (mod 467)

Άρα m = 42*301 mod 467 = 33

- Κρυπτογράφηση:

  B = g^d mod p = 2^300 mod 467 = 317

  ks = B^i mod p = 317^45 mod 467 = 12

  c = ks * m mod p = 12 * 248 mod 467 = 174

  Αποκρυπτογράφηση:

  m = ks^-1 * c mod p = 12^-1 * 174 mod 467, βρίσκω τον αντίστροφο:

  467 = 12x38 + 11

  12 = 11x1 + 1

  11 = 11x1 + 0 υπόλοιπο 1 άρα υπάρχει αντίστροφος:

  Από 2ο βήμα: 1 = 12-11x1

  Αλλά 11 = 467-12x38, άρα:

  1=12−(467−12x38)x1=12−467+12x38=39x12−467

  Επομένως:12^-1 ≡ 39 mod 467

  Άρα m = 39 * 174 mod 467 = 248

- Κρυπτογράφηση:

  B = g^d mod p = 2^300 mod 467 = 317

  ks = B^i mod p = 317^47 mod 467 = 74

  c = ks * m mod p = 74 * 248 mod 467 = 139

  Αποκρυπτογράφηση:

  m = ks^-1 * c mod p = 74^-1 * 139 mod 467, βρίσκω τον αντίστροφο:

  467=74x6+23

  74 = 23 x 3 + 5

  23 = 5 x 4 + 3

  5 = 3 x 1 + 2

  3 = 2 x 1 + 1

2 = 1 x 2 + 0 υπόλοιπο 1 άρα υπάρχει αντίστροφος:

Από το 5ο βήμα: 1=3-2x1

Αλλά 2 = 5-3x1, άρα:

1=3−(5−3x1)x1=3−5+3=2x3−5=2x3−5

Και 3 = 23-5x4, άρα:

1=2x(23−5x4)−5=2x23−8x5−5=2x23−9x5

Και 5 = 74 - 23x3, άρα:

1=2x23−9x(74−23x3)=2x23−9x74+27x23=(2+27)x23−9x74=29x23−9x74

Και 23 = 467 - 74x6, άρα:

1=29x(467−74x6)−9x74=29x467−174x74−9x74=29x467−183x74

Επομένως 74^-1 ≡ −183 mod 467, 467-183 = 284

Άρα m = 284*139 mod 467 = 248

Exercise 5

Υποθέστε ότι ο Bob στέλνει ένα κρυπτογραφημένο μήνυμα στην Alice χρησιμοποιώντας το κρυπτοσύστημα Elgamal. Εσφαλμένα, ο Bob χρησιμοποιεί την ίδια παράμετρο για όλα τα μηνύματα. Επιπλέον, γνωρίζουμε ότι όλες οι διαβιβάσεις του Bob ξεκινούν με πρώτο αρχικό κείμενο (plaintext) το **m1 = 7** (αποτελεί το ID του Bob). Αν οι παράμετροι Elgamal είναι **p = 83**,**g = 2**,**A = 57** και έχουμε λάβει τα παρακάτω κρυπτοκείμενα, προσδιορίστε το δεύτερο αρχικό κείμενο (plaintext) **m2**:

- $(k_{e,1} = 82, c_1 = 76)$
- $(k_{e,2} = 82, c_2 = 60)$

Solution

Ξέρουμε ότι c = m * ks (mod p), άρα για m1:

76 = 7 * ks1 (mod 83)

Βρίσκουμε τον αντίστροφο του 7 στο 83:

83 = 7x11 + 6, 7 = 6x1 + 1, 6=6x1 + 0 , υπάρχει αντίστροφο αφού υπόλοιπο 1

και από βήμα 2, 7 = 6x1 + 1, αλλά 6 = 83-7x11, άρα 1=7-83+7x11 = 12x7-83, Άρα 1=12x7 - 1x83

12x7≡1 (mod 83)

Άρα 7^-1 ≡ 12 (mod 83)

ks1 = 76x12 (mod 83) = 912 ≡ 82 (mod 83)

Άρα ks1 = 82 ≡ -1 (mod 83)

Εφόσον ke1=ke2 τότε ks1=ks2 και για m2:

60 = m2 * 82 (mod 83)

m2 = 60 * (82)^-1 (mod 83)

Επειδή ks2 = 82 ≡ -1 , το αντίστροφο είναι 82^-1 ≡ 82 (mod 83)

τότε m2 = 60x82 (mod 83) = 4920 (mod 83) = 23

Άρα m2 = 23