Група ІПС-42, Геворгян Артем Арсенович
Тема: Системи обміну ключами **Варіант 23**
Вхідні дані
p = 5927
g = 53
повідомлення: delegates attending the conference must register
Завдання
1. ***Діффі-Хелман.*** Окремо зі своїм абонентом вибрати одному $a > 100$, другому $b > 100$, обчислити окремо ключі k і переконатись, що ці ключі співпадають.
2. ***Шамір.*** Перетворити текстове повідомлення у число, закодувавши кожен символ двозначними десятковим числом. Надіслати зашифроване повідомлення своєму абоненту і одержати від нього розшифроване повідомлення.
3. ***Ель-Гамаль.*** Обмінятися ключами.

Описати хід виконання завдання.

Розв'язок

Студент А - Геворгян Артем.
Студент Б - Пилипець Гліб.

1. Мета алгоритму в тому, щоб обмінятися ключем, не використовуючи відкриті канали зв'язку.

Для роботи алгоритму необхідно вибрати значення p, g. Нехай ми вибрали значення із варіанту абонента А, тобто $p = 7523$, $g = 66$.

Абонент А має порахувати свій публічний ключ, передати його абоненту Б. У свою чергу, абонент Б може розраховувати на те, що абонент А самостійно порахує свій публічний ключ та передасть його абоненту Б. Таким чином, абонент А має отримати публічний ключ від абонента Б та порахувати свій публічний ключ. Маючи ці ключі, абонент А порахує значення k. Абонент Б, у свою чергу, порахує значення k для себе. Якщо все виконано правильно, то отримані значення k для обох абонентів співпадають.

Псевдокод:

Алгоритм роботи абонента А
1. Задані p = 7523, g = 66.
2. Отримуємо від абонента Б його публічний ключ 4334:
    a. Для цього спочатку визначимо приватний ключ, нехай це буде 2319.
    b. Тепер порахуємо публічний ключ: $(66^{2319})\ mod\ 7523 = 4334$.
3. Обрахуємо власний приватний ключ $pk = random(0,\ p)$, випадкове ціле число з вказаного проміжку. Нехай маємо $pk = 2057$.
4. Відправляємо абоненту Б наш публічний ключ $(g^{pk})\ mod\ p = 6616$.
5. Рахуємо спільне число $k = (4334^{2057})\ mod\ p = 3269$.
6. Абонент А рахує своє значення $k = (6616^{2319})\ mod\ p = 3269$.

2. Повідомлення: "delegates attending the conference must register". Нехай потрібно передати наступне повідомлення. Спочатку абоненти мають домовитися про число $p = 4679$. Абонент А вибирає 2 числа a_A, b_A: $(a_A * b_A)\ mod\ p$. Таким чином обирає два своїх числа і

абонент Б. Тепер абонент А передає повідомлення m^{a_A}, абонент Б отримує це число і підносить його до степені, щоб у результаті отримати наступне число: $m^{a_A a_B}$. Нехай це проміжне значення названо f. Тоді абонент Б відправляє f абоненту А. Абонента А рахує значення f^{b_A}, після чого відправляє це значення абоненту Б. Абонент Б нарешті рахує $f^{b_A b_B}$. За властивостями такої процедури, це число дорівнює m. Таким чином, у 4 кроки ми передали повідомлення.

Нехай у даній задачі абонент А передає повідомлення абоненту Б. Для цього, нам необхідно закодувати повідомлення m. Зрозуміло, що ми не можемо представити весь текст у вигляді одного числа. Тому розіб'ємо його на символи, кожен символ співставимо із певним числом із інтервалу $[10, 37]$. Тепер робимо наступне: чотири кроки, які були описані раніше, виконуємо із кожним символом водночас. Таким чином, усього за три кроки ми отримаємо повідомлення на стороні абонента Б.

Опустивши деталі імплементації, наведемо роботу алгоритму:

```
--------------------------- SHAMIR ALGO ---------------------------
Message:  delegates attending the conference must register
Message to number:  13142114161029142836102929142313182316362917143612242315142714231214362230282936271416182829142 7
Splitted message number:  [1314, 2114, 1610, 2914, 2836, 1029, 2914, 2313, 1823, 1636, 2917, 1436, 1224, 2315, 1427, 1423, 1214, 3622, 3028, 2936, 2714, 1618, 2829, 1427]
Ciphered by A:  [3114, 2720, 1138, 3521, 4086, 408, 1613, 917, 3960, 282, 3739, 4630, 2058, 1816, 4076, 2079, 1963, 4511, 901, 3809, 56, 640, 2572, 2615]
Ciphered by B:  [2799, 364, 115, 3540, 3006, 3900, 3232, 3474, 4377, 803, 2709, 4586, 955, 1885, 1807, 498, 85, 2924, 70, 3946, 2365, 3197, 200, 2045]
Deciphered by A:  [3103, 2374, 2454, 520, 4654, 650, 4668, 226, 3831, 4253, 396, 3870, 1880, 1909, 2552, 339, 788, 2987, 2400, 4076, 4464, 2125, 2415, 2576]
Deciphered by B:  [1314, 2114, 1610, 2914, 2836, 1029, 2914, 2313, 1823, 1636, 2917, 1436, 1224, 2315, 1427, 1423, 1214, 3622, 3028, 2936, 2714, 1618, 2829, 1427]
Array to number:  13142114161029142836102929142313182316362917143612242315142714231214362230282936271416182829142 7
Answer message:  delegates attending the conference must register
```

Наведемо код для вибору чисел a_A, a_B, b_A, b_B:

```
def get_d(self, c):
    return (gcd_global(c, self.p - 1)[1] + (self.p - 1)) % (self.p - 1)

def get_random_c(self):
    c, d = 0, 0
    while not self.check_cd(c, d):
        c = random.randint(2, self.p - 2)
        if gcd(c, self.p - 1) == 1:
            d = self.get_d(c)
        else:
            c = 0
    return c
```

Ми обираємо випадкове c, потім вибираємо d, використовуючи розширений алгоритм Евкліда.

3. Нехай абонент А відправляє абоненту Б повідомлення "delegates attending the conference must register". Для цього як у попередньому випадку, кодуємо повідомлення двозначними десятковими числами. Змінений лише алгоритм передачі самого повідомлення m.

Для абонентів A, B, C вибирається велике просте число p і число g (число g вибирається так як в протоколі Діффі-Хелмана). Числа p і g висилаються всім абонентам. Після отримання цих чисел кожен абонент вибирає приватне число c_i, $1 < c_i < p-1$, і обчислює число $d_i = g^{c_i} \ mod \ p$. Результати обчислень наведені в таблиці:

Абонент	Ключ приватний	Ключ відкритий
A	c_A	d_A
B	c_B	d_B
C	c_C	d_C

Покажемо як абонент A передає повідомлення m абоненту B. Припустимо, що $m < p$ (якщо $m < p$, то повідомлення передається зразу, а коли $m > p$, то m ділиться на частини $m = m_1, m_2, \ldots, m_k$, де $m_i < p$ – прості числа $(i = 1, 2, \ldots, k)$ і висилається кожна з частин з власними c_i і d_i). Реалізація такого способу виконується наступним чином:

крок 1. Абонент A вибирає довільним чином число k, $1 \leq k < p-2$, обчислює числа $r = g^k \ (mod \ p)$, $e = m \cdot d_B^k \ (mod \ p)$ і пересилає пару (r, e) абоненту B.

крок 2. Абонент B, отримавши пару (r, e), обчислює число $m' = e \cdot r^{p-1-c_B} \ (mod \ p)$.

У цьому випадку $p = 7523$, $g = 66$, як у варіанті абоненту А.
Продемонструємо роботу алгоритму:

```
Message:  delegates attending the conference must register
Ciphered:  [(5616, 4913), (4548, 5456), (2694, 4117), (5472, 364),
(2542, 4326), (64, 1503), (4511, 3814), (4834, 2087), (1157, 382),
(5404, 2638), (1437, 1065), (1577, 4633), (967, 2820), (2481, 5592),
(3208, 592), (847, 756), (24, 2337), (5522, 4918), (1226, 4349),
(1737, 4169), (3160, 2023), (904, 4858), (4083, 3355), (5606, 877)]
Deciphered message:  delegates attending the conference must register
```