Презентация по лабораторной работе №7

Математические основы защиты информации и информационной безопасности

Быстров Г. А.

7 декабря 2024

Российский университет дружбы народов, Москва, Россия

Цели и задачи

- Получить понимание как делать дискретное логарифмирование в конечном поле.
- Реализовать алгоритм программно

Выполнение лабораторной работы

1. Реализация метода (рис. 1).

```python
def extended_euclid(a, b):
    if b == 0:
        return a, 1, 0
    gcd, x1, y1 = extended_euclid(b, a % b)
    x = y1
    y = x1 - (a // b) * y1
    return gcd, x, y

def modular_inverse(a, n):
    return extended_euclid(a, n)[1]

def process_xab(x, a, b, params):
    G, H, P, Q = params
    mod_case = x % 3
    if mod_case == 0:
        x = x * G % P
        a = (a + 1) % Q
    elif mod_case == 1:
        x = x * H % P
        b = (b + 1) % Q
    else:
        x = x * x % P
        a = (a * 2) % Q
        b = (b * 2) % Q
    return x, a, b

def pollard_algorithm(G, H, P):
    Q = (P - 1) // 2
    x = G * H
    a, b = 1, 1
    X, A, B = x, a, b
    for _ in range(1, P):
```

Рис. 1: Код

2. Реализация метода (рис. 2).

```
        x, a, b = process_xab(x, a, b, (G, H, P, Q))
        X, A, B = process_xab(X, A, B, (G, H, P, Q))
        X, A, B = process_xab(X, A, B, (G, H, P, Q))
        if x == X:
            break

    nominator = a - A
    denominator = B - b
    x_result = (modular_inverse(denominator, Q) * nominator) % Q

    return x_result if verify_result(G, H, P, x_result) else x_result + Q

def verify_result(g, h, p, x):
    return pow(g, x, p) == h

test_cases = [(10, 64, 107)]
for G, H, P in test_cases:
    result = pollard_algorithm(G, H, P)
    print(f"Для входных данных ({G}, {H}, {P}) результат: {result}")
    print(f"Проверка: {'успешно' if verify_result(G, H, P, result) else 'неуспешно'}")
```

```
Для входных данных (10, 64, 107) результат: 20
Проверка: успешно
```

Рис. 2: Код и вывод

Результаты

Успешно удалось получить понимание как делать дискретное логарифмирование в конечном поле. Реализовал на практике метод.