ЛАБОРАТОРНАЯ РАБОТА №7

Дискретное логарифмирование в конечном поле

Кузнецов Юрий Владимирович

Введение

В данном отчёте будет представлена реализация дискретного логарифмирования в конечном поле

Основное содержание

Основной метод

- p-метод Полларда для задач дискретного логарифмирования

Кодовая реализация

Метод Полларда

```
function find_gamma(a_diff, b_diff, prime_modulus)
  for gamma in 1:prime_modulus
    if (b_diff * gamma) % prime_modulus == a_diff
      return gamma
    end
  end
end

function update_xab(x, a, b, prime_modulus, alpha, beta)
  if x % 3 == 0
    return mod(x^2, prime_modulus), mod(a * 2, prime_modulus - 1), mod(b * 2, pri
  elseif x % 3 == 1
    return mod(x * alpha, prime_modulus), mod(a + 1, prime_modulus - 1), b
  else
    return mod(x * beta, prime_modulus), a, mod(b + 1, prime_modulus - 1)
  end
end

function pollard_rho_log(prime_modulus, alpha, beta)
```

```
  if prime_modulus % 2 == 0
    return "Invalid"
  end
```

Метод Полларда

```
 a1, b1, x1 = 0, 0, 1
  a2, b2, x2 = 0, 0, 1
  iteration_limit = 1000


  trace1 = zeros(Int64, 3, iteration_limit)
  trace2 = zeros(Int64, 3, iteration_limit)

  for iteration in 1:iteration_limit

    x1, a1, b1 = update_xab(x1, a1, b1, prime_modulus, alpha, beta)
    trace1[:, iteration] = [x1, a1, b1]


    x2, a2, b2 = update_xab(x2, a2, b2, prime_modulus, alpha, beta)
    x2, a2, b2 = update_xab(x2, a2, b2, prime_modulus, alpha, beta)
    trace2[:, iteration] = [x2, a2, b2]

    if x1 == x2
      display(trace1[:, 1:iteration])
      display(trace2[:, 1:iteration])
```

```
      diff_b = b2 - b1
      if diff_b == 0
        return "Not found"
      else
        return find_gamma(a1 - a2, diff_b, prime_modulus)
      end
    end
  end
```

Метод Полларда

```
  return "Invalid"
end

prime1 = 2341
alpha1 = 4
beta1 = 86
println(pollard_rho_log(prime1, alpha1, beta1))

prime2 = 1234
alpha2 = 3
beta2 = 4
println(pollard_rho_log(prime2, alpha2, beta2))
```

Заключение

В данной лабораторной работе представлена реализация дискретного логарифмирования в конечном поле