**Лабораторная работа: Метод ассиметричного шифрования ElGamal.**

**Краткое описание:**

Метод асимметричного шифрования ElGamal, разработанный в 1985 году, представляет собой криптографический алгоритм, основанный на сложности дискретного логарифмирования. Он использует пару ключей: открытый и закрытый, что позволяет безопасно обмениваться данными и создавать цифровые подписи.

В отличие от симметричного шифрования, где один ключ используется для шифрования и дешифрования, в ElGamal открытый ключ используется для шифрования, а закрытый — для расшифровки.

Этот алгоритм обеспечивает высокий уровень безопасности благодаря своей зависимости от математических задач, сложность которых затрудняет взлом. ElGamal находит широкое применение в области электронной коммерции, защиты данных и обеспечения анонимности в сетевых коммуникациях.

**Шаги алгоритма ElGamal:**

1. **Генерация ключей:**
   * **Входные данные:** простое число p и примитивный корень α для p
   * **Секретный ключ** — случайное целое число a (секретное значение отправителя).
   * **Публичный ключ:** вычисляется β=α^a mod  p
   * **Параметры:** p, α, и β — публичные; a — секретный ключ.
2. **Шифрование (или подпись):**
   * **Входные данные:** сообщение x, хэш сообщения H(x), и случайное k (секретное).
   * Вычисляем параметры шифра (или подписи):
     + γ=α^k mod  p
     + δ=(H(x)−a⋅γ)⋅k^−1mod  (p−1)
   * **Результат:** шифротекст или подпись представляется как пара (γ,δ)
3. **Расшифрование:**
   * **Входные данные:** γ, δ, публичные параметры p, α, β, и a.
   * **Действие:** Восстанавливаем x с помощью формулы x=δ⋅(γa)^−1mod  p
4. **Проверка подписи:**
   * **Входные данные:** x, γ, δ, и публичные параметры p, α, β
   * Проверяем равенство β^γ⋅γ^δ mod  p =α^x mod  p. Если равенство верно, подпись считается подлинной.

**Generarea cheilor:**

Допустим простое число p = 71.

primitive root of(Alpha = Af) 71 = 7 (wolfram alpha)

P=Zp\*, A=Zp\*xZp-1, K={(p,**)}. logαβ mod(p)=a.**

Beta(Bt) = Af^a mod p = 7^6 mod 71 = 2

a = 6

Значения p, Af,,Bt – публичные, a – секретное.

**Criptare /( подпись)**

Беру сообщение х = M –ASCII > 77. HASH(77) = Adler32(77) = 2084060710.

H(x) = 20840607

H(x) = x

⁻¹(mod (p – 1)). ⁻¹(mod p - 1). 34537760⁻¹(mod p - 1).

𝜸 = 717 mod 71 **= 62.**

**=** (H(x)−aγ)k−1mod(p−1)

Подставим известные значения:

H(x)=20840607

a=6

γ=62

Таким образом, у нас есть:

δ=(20840607−6⋅62)k−1mod  70 = (20840607−372)k−1mod70 = (20840235⋅33)mod70 = 687227005 mod 70 = 45

**Итоговые результаты шифрования**

Теперь мы можем представить зашифрованное сообщение (или подпись) в виде пары (γ,δ)

**Подпись: (γ,δ)=(62,45)**

**Дешифрование**

𝜸,δ определяется: dK(𝜸,δ) = δ \* (𝜸**ᵅ**)ˉ¹ mod p --- формула для шифрования

y = 62, δ = 45, p = 71, a = 6.

dK(𝜸,δ) = 22 \*(445)ˉ¹ mod 71 = 77 –ASCII ---> M

**Подпись:**

= 717 mod 71 = **62**

⁻¹(mod p - 1) = (20840607−6⋅62)⋅17^−1 mod 70 = (20840235)⋅17^−1 mod 70 = **45**

**Проверка подписи:**

Для проверки подписи, проведем некоторые вычисления:

verK(x,) = T <=>  **mod ⬄**  mod p = (262 \* 6245) mod 71 =

= αᵡ mod p = 766 mod 71 **⬄** 14 = 14

Так как обе части равны, значит подпись валидна.

### Заключение

Согласно алгоритму ElGamal, после расшифрования мы получили исходное сообщение в открытом тексте. Подпись, созданная на основе алгоритма ElGamal с использованием ключей, сгенерированных для шифрования, является действительной.