**Практическое задание №4.2**

**Тема «Криптографическая защита информации»**

Цель: Овладение основными криптографическими алгоритмами асимметричного шифрования .

**Теоретические сведения**

# Реализация элементов криптосистемы RSA

RSA (аббревиатура от фамилий Rivest, Shamir и Adleman) — криптографический алгоритм с открытым ключом, основывающийся на вычислительной сложности задачи факторизации больших целых чисел.

Криптосистема RSA стала первой системой, пригодной и для шифрования, и для цифровой подписи. Алгоритм используется в большом числе криптографических приложений, включая PGP, S/MIME, TLS/SSL, IPSEC/IKE и других.

Весь алгоритм расписан в таблице:

|  |  |  |
| --- | --- | --- |
| Этап | Описание операции | Результат операции |
| Генерация ключей | Выбрать два простых различных числа | p=3557,  q=2579 |
| Вычислить модуль (произведение) | n = p \cdot q = 3557 \cdot 2579 = 9173503 |
| Вычислить функцию Эйлера | \varphi(n) = (p-1) (q-1) = 9167368 |
| Выбрать открытую экспоненту | e = 3 |
| Вычислить секретную экспоненту | d = e^{-1} \mod \varphi(n)  d = 6111579 |
| Опубликовать открытый ключ | \{e, n\} = \{3,9173503 \} |
| Сохранить закрытый ключ | \{d, n\} = \{6111579, 9173503 \} |
| Шифрование | Выбрать текст для зашифровки | m = 111111 |
| Вычислить шифротекст | \begin{align} c &= E(m) \\  &= m^e \mod n \\  &= 111111^3   \mod 9173503 \\  &= 4051753 \end{align} |
| Расшифрование | Вычислить исходное сообщение | \begin{align} m &= D(c) = \\   &= c^d \mod n \\   &= 4051753^{6111579} \mod 9173503 \\   &= 111111 \end{align} |

# Реализация элементов схемы шифрования Эль-Гамаля

## **Генерация ключей**

1. Генерируется случайное простое число ~p длины ~n [битов](https://ru.wikipedia.org/wiki/%D0%91%D0%B8%D1%82).
2. Выбирается случайный примитивный элемент ~g.
3. Выбирается случайное целое число ~x такое, что ~1 < x < p-1.
4. Вычисляется ~y = g^x\,\bmod\,p.
5. Открытым ключом является тройка \left( p,g,y \right), закрытым ключом — число ~x.

## **Шифрование**

Сообщение ~M шифруется следующим образом:

1. Выбирается сессионный [ключ](https://ru.wikipedia.org/wiki/%D0%9A%D0%BB%D1%8E%D1%87_(%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F)) — случайное целое число ~k такое, что ~1 < k < p - 1
2. Вычисляются числа a = g^k\,\bmod\,p и b = y^k M\,\bmod\,p.
3. Пара чисел \left( a, b \right) является [шифротекстом](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80%D0%BE%D1%82%D0%B5%D0%BA%D1%81%D1%82" \o "Шифротекст).

Нетрудно видеть, что длина шифротекста в схеме Эль-Гамаля длиннее исходного сообщения M вдвое.

## **Расшифрование**

Зная закрытый ключ ~x, исходное сообщение можно вычислить из шифротекста \left( a, b \right) по формуле:

M = b(a^x)^{-1}\,\bmod\,p.

При этом нетрудно проверить, что

~(a^x)^{-1}\equiv g^{-kx}\pmod{p}

и поэтому

~b(a^x)^{-1}\equiv (y^kM)g^{-xk}\equiv (g^{xk}M) g^{-xk}\equiv M \pmod{p}.

Для практических вычислений больше подходит следующая формула:

M = b(a^x)^{-1}\,\bmod\,p = b \cdot a^{(p-1-x)}\,\bmod\,p 

## **Пример**

**Шифрование**

Допустим, что нужно зашифровать сообщение ~M=5.

Произведем генерацию ключей :

пусть ~p=11, g=2. Выберем ~x=8 - случайное целое число ~x такое, что ~1 < x < p.

Вычислим ~y= g^x\bmod{p}=2^8\bmod{11}=3.

Итак, открытым является тройка ~(p,g,y)=(11,2,3), а закрытым ключом является число ~x=8.

Выбираем случайное целое число ~k такое, что 1 < k < (p − 1). Пусть ~k=9.

Вычисляем число ~a=g^k\bmod{p}=2^9 \bmod{11}=512 \bmod{11}=6.

Вычисляем число ~b=y^k M\bmod{p}=3^9 5 \bmod{11}=19683 \cdot 5 \bmod{11}=9.

Полученная пара ~(a,b)=(6,9) является шифротекстом.

**Расшифрование**

Необходимо получить сообщение ~M=5 по известному шифротексту ~(a,b)=(6,9) и закрытому ключу ~x=8.

Вычисляем M по формуле : ~M=b(a^x)^{-1}\bmod{p}=9(6^8)^{-1}\mod{11}=5

Получили исходное сообщение ~M=5.

# Реализация элементов схемы шифрования Дифи-Хеллмана

## **Генерация ключей**

В 1976 году после публичной критики алгоритма DES и указания на сложность обработки секретных ключей Уитфилд Диффи (Whitfield Diffie) и Мартин Хеллман (Martin Hellman) опубликовали свой алгоритм обмена ключами. Это была первая публикация на тему криптографии с открытым ключом и, возможно, самый большой шаг вперед в области криптографии, сделанный когда‑либо.

Из‑за невысокого быстродействия, свойственного асимметричным алгоритмам, алгоритм Диффи‑Хеллмана не предназначен для шифрования данных. Он был ориентирован на передачу секретных ключей DES, ARS или других подобных алгоритмов через небезопасную среду. В большинстве случаев алгоритм Диффи‑Хеллмана не используется для шифрования сообщений, потому что он, в зависимости от реализации, от 10 до 1000 раз медленнее алгоритма DES.

До алгоритма Диффи‑Хеллмана было сложно совместно использовать зашифрованные данные из‑за проблем хранения ключей и передачи информации. В большинстве случаев передача информации по каналам связи небезопасна, потому что сообщение может пройти десятки систем, прежде чем оно достигнет потенциального адресата, и нет никаких гарантий, что по пути никто не сможет взломать секретный ключ. Уитфилд Диффи и Мартин Хеллман предложили зашифровывать секретный ключ DES по алгоритму Диффи‑Хеллмана на передающей стороне и пересылать его вместе с сообщением, зашифрованным с использованием DES. Тогда на другом конце его сможет расшифровать только получатель сообщения.

На практике **обмен ключами** по алгоритму Диффи‑Хеллмана происходит по следующей схеме.

1. Два участника обмена договариваются о двух числах. Один выбирает большое простое число, а другой – целое число, меньшее числа первого участника. Переговоры они могут вести открыто, и это никак не отразится на безопасности.
2. Каждый из двух участников, независимо друг от друга, генерирует другое число, которое они будут хранить в тайне. Эти числа выполняют роль секретного ключа. Далее в вычислениях используются секретный ключ и два предыдущих целых числа. Результат вычислений посылается участнику обмена, и он играет роль открытого ключа.
3. Участники обмена обмениваются открытыми ключами. Далее они, используя собственный секретный ключ и открытый ключ партнера, конфиденциально вычисляют ключ сессии. Каждый партер вычисляет один и тот же ключ сессии.
4. Ключ сессии может использоваться как секретный ключ для другого алгоритма шифрования, например DES. Никакое третье лицо, контролирующее обмен, не сможет вычислить ключ сессии, не зная один из секретных ключей.

**Самое сложное в алгоритме** Диффи‑Хеллмана обмена ключами – это понять, что в нем фактически два различных независимых цикла шифрования. Алгоритм Диффи‑Хеллмана применяется для обработки небольших сообщений от отправителя получателю. Но в этом маленьком сообщении передается секретный ключ для расшифровки большого сообщения.

**Сильная сторона алгоритма** - никто не сможет скомпрометировать секретное сообщение, зная один или даже два открытых ключа получателя и отправителя. В качестве секретных и открытых ключей используются очень большие целые числа. Алгоритм Диффи‑Хеллмана основан на полезных для криптографии свойствах дискретных логарифмов.

## **Пример**

Ева — криптоаналитик. Она читает пересылку Боба и Алисы, но не изменяет содержимого их сообщений.

* s = секретный ключ. s = 2
* g = простое число меньшее p. g = 5
* p = открытое простое число. p = 23
* a = секретный ключ Алисы. a = 6
* A = открытый ключ Алисы. A = ga mod p = 8
* b = секретный ключ Боба. b = 15
* B = открытый ключ Боба. B = gb mod p = 19



**Задание №1**

Рассказать процесс работы алгоритма RSA.

RSA (аббревиатура от фамилий Rivest, Shamir и Adleman) — криптографический алгоритм с открытым ключом, основывающийся на вычислительной сложности задачи факторизации больших целых чисел.

1. Генерация ключей:
   * Шаг 1: Выбор двух больших простых чисел p и q. Эти числа должны быть достаточно велики, чтобы обеспечить безопасность алгоритма.
   * Шаг 2: Вычисление произведения n = p \* q. Число n будет использоваться в качестве модуля для шифрования и расшифрования.
   * Шаг 3: Вычисление функции Эйлера φ(n) = (p - 1) \* (q - 1), где φ(n) - это количество целых чисел, меньших n и взаимно простых с n.
   * Шаг 4: Выбор целого числа e, такого что 1 < e < φ(n) и e взаимно просто с φ(n). Число e будет использоваться в качестве открытого ключа.
   * Шаг 5: Вычисление числа d, обратного по модулю e и φ(n), то есть d \* e ≡ 1 (mod φ(n)). Число d будет использоваться в качестве закрытого ключа.
2. Шифрование сообщения:
   * Шаг 1: Преобразование сообщения в числовое представление, где каждый символ или блок символов кодируется числом, меньшим, чем n.
   * Шаг 2: Шифрование числового представления сообщения с использованием открытого ключа (n, e) по формуле: C = M^e (mod n), где C - зашифрованное сообщение, а M - числовое представление исходного сообщения.
3. Расшифрование зашифрованного сообщения:
   * Шаг 1: Использование закрытого ключа (n, d) для расшифровки зашифрованного сообщения C по формуле: M = C^d (mod n), где M - числовое представление исходного сообщения.

**Задание №2**

Рассказать процесс работы алгоритма Диффи-Хеллмана.

Алгоритм Диффи-Хеллмана - это протокол обмена ключами, который позволяет двум сторонам, находящимся в открытом канале связи, согласовать общий секретный ключ без необходимости предварительного обмена секретными ключами. Процесс работы алгоритма Диффи-Хеллмана выглядит следующим образом:

1. Настройка параметров:
   * Шаг 1: Выбор большого простого числа p и примитивного элемента g, который является первообразным корнем по модулю p. Эти параметры должны быть известны обеим сторонам.
2. Генерация общего секретного ключа:
   * Шаг 1: Каждая сторона выбирает свое секретное число. Пусть это числа будут a и b для первой и второй стороны соответственно.
   * Шаг 2: Первая сторона вычисляет A = g^a (mod p) и отправляет полученное значение второй стороне.
   * Шаг 3: Вторая сторона вычисляет B = g^b (mod p) и отправляет полученное значение первой стороне.
   * Шаг 4: Первая сторона вычисляет общий секретный ключ K = B^a (mod p).
   * Шаг 5: Вторая сторона вычисляет общий секретный ключ K = A^b (mod p).
   * После выполнения этих шагов обе стороны имеют одинаковое значение общего секретного ключа K, которое может быть использовано для шифрования и расшифрования сообщений.

**Задание №3**

Рассказать процесс работы алгоритма Эль-Гамаля.

Алгоритм Эль-Гамаля - это криптографический алгоритм с открытым ключом, который используется для шифрования и подписи сообщений. Он основан на трудности вычисления дискретного логарифма в конечных полях. Процесс работы алгоритма Эль-Гамаля следующий:

1. Генерация ключей:
   * Шаг 1: Выбор простого числа p, которое является большим и сложно факторизуемым.
   * Шаг 2: Выбор числа g, которое является первообразным корнем по модулю p. Это число должно быть известно всем участникам.
   * Шаг 3: Каждая сторона (отправитель и получатель) генерирует свой закрытый ключ, который представляет собой случайное число x, такое что 1 ≤ x ≤ p-2.
   * Шаг 4: Каждая сторона вычисляет свой открытый ключ, который представляет собой число y = g^x (mod p).
   * Открытый ключ (p, g, y) передается другим сторонам, а закрытый ключ x хранится в тайне.
2. Шифрование сообщения:
   * Шаг 1: Отправитель преобразует сообщение M в числовое представление, которое обычно называется m.
   * Шаг 2: Отправитель выбирает случайное число k, такое что 1 ≤ k ≤ p-1 и k и p-1 взаимно просты.
   * Шаг 3: Отправитель вычисляет первую часть шифртекста a = g^k (mod p).
   * Шаг 4: Отправитель вычисляет вторую часть шифртекста b = (y^k \* m) (mod p).
   * Шифртекст (a, b) является результатом шифрования и передается получателю.
3. Расшифрование зашифрованного сообщения:
   * Шаг 1: Получатель вычисляет общий секретный ключ K = a^x (mod p).
   * Шаг 2: Получатель вычисляет обратное значение K^(-1) (mod p).
   * Шаг 3: Получатель восстанавливает исходное сообщение m = (b \* K^(-1)) (mod p).