Учреждение образования “Белорусский государственный технологический yниверситет”

Практическая работа №6 «Криптографическая защита информации»

Выполнила:

студентка 2 курса, 7 группы

Колядко Яна Дмитриевна

Проверил:

Барковский Евгений Валерьевич

ПроТТеоре

Цель: овладение основными криптографическими алгоритмами асимметричного шифрования.

Теоретические сведения

# Реализация элементов криптосистемы RSA.

RSA — 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.

|  |  |  |
| --- | --- | --- |
| Этап | Описание операции | Результат операции |
| Генерация ключей | Выбрать два простых различных числа | p = 3557, q = 2579 |
| Вычислить модуль (произведение) | n = p \* q = 3557 \* 2579 = 9713503 |
| Вычислить функцию Эйлера | φ(n) = (p - 1)(q - 1) = 9167368 |
| Выбрать открытую экспоненту | e = 3 |
| Вычислить секретную экспоненту | d = e-1 mod φ(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 | c = E(m) = me mod n = 1111113 mod 9173503 = 4051753 |
| Расшифрование | Вычислить исходное сообщение | m = D(c) = cd mod n = 40517536111579 mod 9173503 = 111111 |

# 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 = gx mod p.
5. Открытым ключом является тройка (p, g, y), 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 = gk mod p и b = yk M mod p.
3. Пара чисел (a, b) 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).

## **Расшифрование**

Зная закрытый ключ x, исходное сообщение можно вычислить из шифротекста (a, b) по формуле: M = b(ax)-1 mod p.

# Реализация элементов схемы шифрования Дифи-Хеллмана.

## **Генерация ключей**

Алгоритм Диффи‑Хеллмана не предназначен для шифрования данных. Он был ориентирован на передачу секретных ключей DES, ARS или других подобных алгоритмов через небезопасную среду.

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. Никакое третье лицо, контролирующее обмен, не сможет вычислить ключ сессии, не зная один из секретных ключей.

Алгоритм Диффи‑Хеллмана применяется для обработки небольших сообщений от отправителя получателю. Но в этом маленьком сообщении передается секретный ключ для расшифровки большого сообщения.

**Задание №1**

Рассказать процесс работы алгоритма RSA.

**Задание №2**

Рассказать процесс работы алгоритма Диффи-Хеллмана.

**Задание №3**

Рассказать процесс работы алгоритма Эль-Гамаля.

**Задание №4\***

Используя существующие криптографические библиотеки, создать приложение и проанализировать работу вышеперечисленных алгоритмов.

**Изображение выглядит как текст

Автоматически созданное описание**

Вывод: в данной лабораторной работе овладели основными криптографическими алгоритмами асимметричного шифрования.