МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «Белорусский государственный технологический университет»

Кафедра информационных технологий

**Практическое занятие №6**

**Тема «Криптографическая защита информации»**

Выполнила:

Студентка 2 курса, 7 группы

Курносенко Софья Андреевна

Проверил:

Барковский Евгений Валерьевич

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 от этого модуля | \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} |

\*

**Простое число** — натуральное число, имеющее ровно два различных натуральных делителя — единицу и самого себя. Другими словами, число x является простым, если оно больше 1 и при этом делится без остатка только на 1 и на x.

Ряд простых чисел от 1 до 15: 1, 2, 3, 5, 7, 11, 13.

\*\*

e:

▪ простое число

▪ < φ(n)

▪ взаимно простое с φ(n)

Два целых числа a и b называются **взаимно простыми**, если их наибольший общий делитель равен единице — то есть НОД (a, b) = 1.

\*\*\*

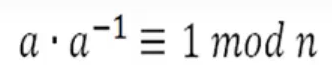
 d = e^{-1} \mod \varphi(n)

e-1 (mod φ(n)) – число обратное e по модулю φ(n).

**Что такое обратное число?**

Обратное число (обратное значение, обратная величина) к данному числу x — это число, умножение которого на x даёт единицу. Принятая запись:  или . Два числа, произведение которых равно единице, называются *взаимно обратными*.

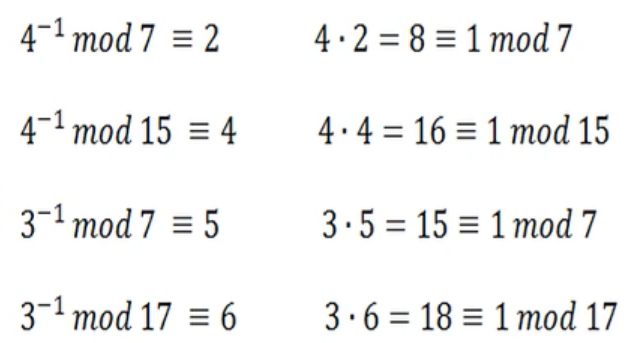
**Что такое обратное число по модулю?**



Число **a-1** называется обратным числу **a** по модулю **n**, если произведение **a-1 a** дает значение, деление которого на **n** вернет 1 в остатке.

Примеры обратных чисел:

Например, 2 является обратным числом к 4-ке по модулю 7.



**Как найти обратное число по модулю**

Обратное к числу **a** по модулю **n** можно найти тогда и только тогда, когда **a** и **n** взаимно простые, т.е. НОД(a, n) =1 (не имеют общих делителей, кроме 1).

Обратное по модулю число можно найти по **алгоритму Евклида**.

Если a > b,

то a можно представить в виде a = b ∙ q + r,

где 0 .

q – некое целое число

r – остаток

Т.е. мы делим a на b и в остатке получаем r.

**Рассмотрим нахождение обратного по модулю сразу на примере:**

***7****-1 mod* ***47*** *– ? (нужно найти число обратное 7-ке по модулю 47)*

1. Сначала ***47*** выразим по формуле a = b ∙ q + r через ***7***:

47 = 7 ∙ 6 + 5

Теперь 7 выразим через 5:

7 = 5 ∙ 1 + 2

Теперь 5 выразим через 2:

5 = 2 ∙ 2 + 1

Алгоритм Евклида заканчивает прямой ход, когда в остатке мы получаем 1.

1. Теперь выразим остатки (у нас это 5, 2, 1) из полученных выше равенств:

5 = 47 7 ∙ 6

2 = 7 5 ∙ 1

1 = 5 2 ∙ 2

1. Далее идет обратный ход алгоритма Евклида.

В обратном ходе алгоритма Евклида используем все равенства из прямого хода, двигаясь от последнего к первому.

Запишем выражение для остатка 1:

1 = 5 2 ∙ 2

В нем нам нужно на место 2 подставить выражение для остатка 2-ки:

1 = 5 2 ∙ (7 5 ∙ 1)

Уберем скобки (но перемножать ничего не нужно, мы разве что выносим общий множитель за скобки (как с 5-кой)):

5 2 ∙ 7 2 ∙ 5 = 5 2 ∙ 5 2 ∙ 7 = 5 (1 2) 2 ∙ 7 = 5 ∙ 3 2 ∙ 7

Теперь вместо 5 подставляем выражение остатка для 5-ки:

5 ∙ 3 2 ∙ 7 = (47 7 ∙ 6) ∙ 3 2 ∙ 7 = 47 ∙ 3 7 ∙ 6 ∙ 3 2 ∙ 7 47 ∙ 3 7 (6 ∙ 3 2) = 47 ∙ 3 7 ∙ 20

Полученное выражение представим в виде суммы:

47 ∙ 3 7 ∙ 20 = 47 ∙ 3 7 ∙ *20 ∙ (1)*

Число обратное к 7-ке стоит *в произведении с 7-кой*, таким образом,

***7****-1 mod* ***47 =***

# **► 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 < p.
3. Выбирается случайное целое число ~x такое, что 1< x < p.
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 = 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 Диффи-Хеллмана**

## **Генерация ключей**

Обмен ключами с помощью протокола Диффи-Хеллмана (DH) — это метод безопасного обмена криптографическими ключами по общедоступному каналу. 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. Публичный выбор двух чисел: p – большое простое число, g – целое число; g < p
2. Каждая сторона выбирает свой секретный ключ, например, первая сторона выбирает число «a», вторая – «b»
3. Вычисляются числа:

ga mod p = A – первая сторона получила такое значение, используя свой секретный ключ

gb mod p = B – вторая такое

Далее публичный обмен числами A и B.

1. Каждая сторона вычисляет общий секретный ключ:

Ba mod p = Ab mod p = k – общий секретный ключ

Ba = Ab = gba

**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.

**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.