Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Московский государственный технический университет
имени Н. Э. Баумана
(национальный исследовательский университет)»
(МГТУ им. Н. Э. Баумана)

ФАКУЛЬТЕТ «Информатика и системы управления»

КАФЕДРА «Программное обеспечение ЭВМ и информационные технологии»

РАСЧЕТНО-ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

К НАУЧНО-ИССЛЕДОВАТЕЛЬСКОЙ РАБОТЕ

НА ТЕМУ:

«Методы асимметричного шифрования данных»

Студент ИУ7-51Б (Группа) ______ (Подпись, дата) В. А. Гаврилюк (И. О. Фамилия)

Руководитель НИР ______ (Подпись, дата) А.С. Кострицкий (И. О. Фамилия)

2024 г.

СОДЕРЖАНИЕ

ОПРЕДЕЛЕНИЯ

В настоящей расчетно-пояснительной записке применяют следующие термины с соответствующими определениями.

Открытый текст (англ. «plaintext») — исходный текст сообщения [1].

Шифрование — процесс маскировки сообщения, скрывающий его содержание [1].

Шифротекст — зашифрованное сообщение [1].

Расшифровка — процесс преобразования шифротекста обратно в открытый текст [1].

ВВЕДЕНИЕ

В современном мире во многих сферах вопрос безопасности обмена данными через открытые сети является ключевым: банковское дело, оплата счетов, электронная коммерция, биржевые торги и т. д. Применение криптографии позволяет эффективно решить эту проблему. Одним из наиболее распространенных криптографических средств, обеспечивающих безопасность связи, является шифрование [2].

Цель работы — анализ методов асимметричного шифрования данных. Для достижения поставленной цели необходимо решить следующие задачи:

– проанализировать предметную область;

– обозначить основные этапы развития;

– формализовать задачу асимметричного шифрования данных;

– перечислить методы или группы методов решения;

– сформулировать критерии сравнения;

– сравнить перечисленные методы по сформулированным критериям.

1 Аналитический раздел

1.1 История развития асимметричных методов шифрования данных

Основные вехи развития асимметричного шифрования:

– зарождение концепции асимметричного шифрования в научной работе Уитфилда Диффи и Мартина Хеллмана в 1976 году [3];

– создание первой криптосистемы с открытым ключом (RSA) в 1977 году [3];

– открытие криптографии эллиптических кривых Нейлом Коблицем и Виктором Миллером в 1985 году [4].

1.2 Формализация задачи асимметричного шифрования данных

Криптографическая система состоит из следующих компонентов [2]:

– пространство исходных сообщений M — множество строк над некоторым алфавитом;

– пространство зашифрованных текстов C — множество возможных зашифрованных сообщений;

– пространство ключей шифрования K — множество возможных ключей шифрования;

– пространство ключей расшифровки K' – множество возможных ключей расшифровки;

– эффективный алгоритм генерации ключей $G : \mathbb{N} \mapsto K \times K'$;

– эффективный алгоритм шифрования $E : M \times K \mapsto C$;

– эффективный алгоритм расшифровки $D : C \times K' \mapsto M$.

Для целого числа 1^l результатом алгоритма $G(1^l)$ является пара ключей $(ke, kd) \in K \times K'$, имеющих длину l.

Операция шифрования обозначается как

$$c = E_{ke}(m), \tag{1.1}$$

где $ke \in K$ — ключ шифрования, $m \in M$ — исходное сообщение. Операция расшифровки обозначается как

$$m = D_{kd}(c), \tag{1.2}$$

где $kd \in K'$ — ключ расшифровки, c — зашифрованное сообщение. Необходимо, чтобы для всех сообщений $m \in M$ и всех ключей $ke \in K$ существовал ключ $kd \in K'$, удовлетворяющий условию

$$D_{kd}(E_{ke}(m)) = m. \tag{1.3}$$

В [1] данная последовательность действий показана с помощью схемы, продемонстрированной на рисунке 1.1.

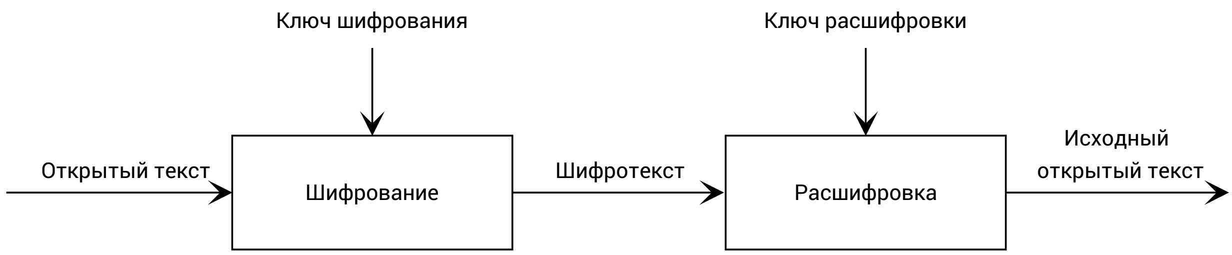

Рисунок 1.1 – Шифрование и расшифровка с двумя разными ключами

Эффективным называется детерминированный или рандомизированный алгоритм, время выполнения которого полиномиально зависит от размера исходных данных [2]. Требование эффективности, предъявляемое к алгоритмам G, E и D, позволяет отнести их к классу полиномиальных алгоритмов.

В алгоритмах с открытым ключом, также называемых асимметричными алгоритмами [1], шифрование и расшифровка используют разные ключи: для каждого ключа $ke \in K$ существует ключ $kd \in K'$, причем они отличаются друг от друга и взаимосвязаны [2]. Более того, ключ расшифровки не может быть (по крайней мере, в течение разумного интервала времени) вычислен по ключу шифрования [1]. Данное требование формально описывается формулой (1.4):

$$\forall A : \mathrm{Prob}[A(ke) = kd] \leq \varepsilon(t), \tag{1.4}$$

где:

- A — любой алгоритм, не имеющий доступа к kd, доступный атакующему,
- $ke \in K$ — ключ шифрования (открытый ключ),
- $kd \in K'$ — ключ расшифровки (закрытый ключ),
- $\varepsilon(t)$ — пренебрежительно малая функция от времени t, стремящаяся к нулю быстрее, чем $\frac{1}{p(t)}$, где $p(t)$ — произвольный полином [2].

Следующее требование, предъявляемое к алгоритмам асимметричного шифрования, касается устойчивости алгоритма к атакам, направленным на восстановление исходного сообщения из шифротекста без использования закрытого ключа. Формальная запись данного условия продемонстрирована формулой (1.5).

$$\forall A : \mathrm{Prob}[A(c, ke) = m] \leq \varepsilon(t) \tag{1.5}$$

С учётом всех перечисленных требований задача асимметричного шифрования данных записывается в виде системы

$$\begin{cases} c = E_{ke}(m), \\ m = D_{kd}(c), \\ D_{kd}(E_{ke}(m)) = m, & ke \neq kd \\ \forall A : \mathrm{Prob}[A(ke) = kd] \leq \varepsilon(t), \\ \forall A : \mathrm{Prob}[A(c, ke) = m] \leq \varepsilon(t). \end{cases} \tag{1.6}$$

1.3 Методы асимметричного шифрования данных

Идея криптографии с открытым ключом тесно связана с идеей односторонних функций. По заданному аргументу x легко вычислить значение функции $f(x)$, тогда как определение x из $f(x)$ трудновычислимо [5]. Здесь «трудновычислимость» понимается в смысле теории сложности, а под $f(x)$ также допускаются и недетерминированные алгоритмы [5].

Функцию $f_t(x) : D \mapsto R$ называют однонаправленной функцией с секретом (англ. «one-way trapdoor function»), если её легко вычислить для всех $x \in D$, но определение x из $f_t(x)$ трудновычислимо для почти всех значений из R. Однако, если используется секретная информация t, то для всех значений $y \in R$ легко вычислить величину $x \in D$, удовлетворяющую условию $y = f_t(x)$ [2].

Основными методами асимметричного шифрования данных считаются алгоритм RSA, криптосистема Рабина и криптосистема Эль-Гамаля [3]. Каждый из данных алгоритмов основан на односторонних функциях с секретом, которые, в свою очередь, опираются на некоторые трудновычислимые задачи.

1.3.1 Трудновычислимые задачи

Для оценки сложности алгоритмов, решающих определённую трудновычислимую задачу, будет использоваться функция

$$L_N(\alpha, \beta) = exp((\beta + o(1))(lnN)^a(lnlnN)^{1-\alpha}). \tag{1.7}$$

Если алгоритм имеет сложность $O(L_N(0, \beta))$, то ему требуется полиномиальное время на работу, если $O(L_N(1, \beta))$ — экспоненциальное время. Т. к. скорость роста функции $L_N(\alpha, \beta)$ при $0 < \alpha < 1$ лежит между полиномиальной и экспоненциальной, алгоритм со сложностью $O(L_N(\alpha, \beta))$ при $0 < \alpha < 1$ будет требовать суб-экспоненциального времени [3].

Задача называется трудновычислимой, если нет алгоритма для решения данной задачи с полиномиальным временем работы. Если же такой алгоритм существует, то задача называется вычислимой. Легковычислимыми будут называться задачи, имеющие алгоритмы со временем работы, представимым в виде полинома низкой степени относительно входного размера задачи [5].

Большинство трудновычислимых задач основано на факторизации чисел, дискретном логарифмировании и эллиптических кривых [3]. Среди задач, связанных с факторизацией, выделяют четыре основные задачи [3]:

– факторизация: найти делители p и q числа $N = p \cdot q$, где p и q — простые;

– задача RSA: даны числа c и E, последнее из которых удовлетворяет соотношению

$$\text{НОД}(E,(p-1)(q-1))=1; \tag{1.8}$$

требуется найти такое число $m \in \mathbb{Z}_N^*$, что

$$m^E = c(\text{mod}N), c \in \mathbb{Z}_N^*; \tag{1.9}$$

– тест на квадратичный вычет: определить, является ли данное число A полным квадратом по модулю N;

– извлечение квадратных корней: дано такое число A, что

$$A = x^2(\text{mod}N); \tag{1.10}$$

необходимо вычислить x.

С проблемой дискретного логарифмирования связано несколько близких задач. Пусть $(G,\cdot)$ — конечная абелева группа.

– ПДЛ — задача дискретного логарифмирования: определить целое число x, которое при данных $A, B \in G$ удовлетворяет соотношению $A^x = B$;

– ЗДХ — задача Диффи-Хеллмана: для данных $A \in G$, $B = A^x$ и $C = A^y$ требуется вычислить $D = A^{xy}$;

– ПВДХ — проблема выбора Диффи-Хеллмана: для данных

$$A \in G,\ B = A^x,\ C = A^y,\ D = A^z \tag{1.11}$$

требуется определить, является ли z произведением $z = x \cdot y$.

В мультипликативной группе конечного поля алгоритмом с наименьшей сложностью, решающим проблему дискретного логарифмирования, является метод квадратичного решета в числовом поле. Сложность вычислений оценивается как $L_N(1/2, c)$, где c — некоторая константа, зависящая от типа поля [3].

Среди алгоритмов вычисления дискретных логарифмов над общей эллиптической кривой над полем $\mathbb{F}_q$ наименьшей сложностью обладает p - метод

Полларда. Его сложность — $L_N(1, 1/2)$ (экспоненциальная). Задача дискретного логарифмирования для эллиптических кривых является более сложной, чем аналогичная задача для мультипликативной группы конечного поля. Это позволяет использовать группы с меньшим порядком и, как следствие, ключи меньшей длины [3].

1.3.2 Алгоритм RSA

Алгоритм RSA, основанный на одноимённой трудновычислимой задаче, может использоваться как для шифрования данных, так и для цифровых подписей [1].

Числа e и N образуют открытый ключ, где

- $N = p \cdot q$ — произведение двух простых чисел p и q, при этом $|p| \approx |q|$;
- e является числом, взаимно простым с числом $(p-1)(q-1)$:

$$\text{НОД}(e, (p-1)(q-1)) = 1. \tag{1.12}$$

Закрытый ключ d вычисляется по формуле

$$d = e^{-1} \text{mod}((p-1)(q-1)). \tag{1.13}$$

Шифрование и расшифровка для некоторого сообщения $m < N$ в алгоритме RSA выполняются с помощью формул (1.14) и (1.15) соответственно.

$$c = m^e (\text{mod} N) \tag{1.14}$$

$$m = c^d (\text{mod} N) \tag{1.15}$$

1.3.3 Криптосистема Рабина

Криптосистема, разработанная Рабином, основана на сложности вычисления квадратного корня по модулю составного числа [2].

Открытым ключом в криптосистеме Рабина может являться любое число $N = p \cdot q$, где p и q — два случайных простых числа и при этом $|p| \approx |q|$. Однако на практике в качестве открытого ключа N используются целые числа Блюма (англ. «Blum integer»), т. е. $N = p \cdot q$, где $p \equiv q \equiv 3(\mathrm{mod} 4)$ [2]. Данное условие позволяет упростить вычисления при расшифровке сообщения, используя китайскую теорему об остатках.

Для шифрования сообщения $M < N$ необходимо вычислить

$$c = M^2 \mathrm{mod} N. \tag{1.16}$$

Расшифровка сообщения выполняется в три этапа [1]:

– вычисление промежуточных значений m_1, m_2, m_3 и m_4, с учетом, что $p \equiv q \equiv 3(\mathrm{mod} 4)$:
$$\begin{aligned} m_1 &= C^{\frac{p+1}{4}} \mathrm{mod}\ p, \\ m_2 &= (p - C^{\frac{p+1}{4}}) \mathrm{mod}\ p, \\ m_3 &= C^{\frac{q+1}{4}} \mathrm{mod}\ q, \\ m_4 &= (q - C^{\frac{q+1}{4}}) \mathrm{mod}\ q. \end{aligned} \tag{1.17}$$

– вычисление целых чисел $a = q(q^{-1} \mathrm{mod}\ p)$ и $b = p(p^{-1} \mathrm{mod}\ q)$;

– вычисление значений M_1, M_2, M_3 и M_4, одно из которых равно M:

$$\begin{aligned} M_1 &= (am_1 + bm_3) \mathrm{mod} N, \\ M_2 &= (am_1 + bm_4) \mathrm{mod} N, \\ M_3 &= (am_2 + bm_3) \mathrm{mod} N, \\ M_4 &= (am_2 + bm_4) \mathrm{mod} N. \end{aligned} \tag{1.18}$$

Определить, какое значение M_j при $j = \overline{1,4}$ является исходным, возможно, если сообщение M является осмысленным текстом (например, на английском языке). Однако не существует способа определить, какое значение M_j является исходным, если сообщение M является потоком случайных битов. Одним из способов решить эту проблему служит добавление к сообщению известного заголовка перед шифрованием [1].

1.3.4 Криптосистема Эль-Гамаля

Эль-Гамаль разработал криптосистему, основанную на дискретном логарифмировании, которая использует однонаправленную функцию Диффи-Хеллмана с секретом [2]. Существует два варианта криптосистемы: первый вариант использует конечные поля, второй вариант — эллиптические кривые [3].

Криптосистему Эль-Гамаля можно использовать как для цифровых подписей, так и для шифрования данных [1].

Система на основе конечных полей

Открытым ключом в криптосистеме Эль-Гамаля является тройка (p, g, y), где

– p является случайным простым числом;

– g — случайный мультипликативный порождающий элемент $g \in \mathbb{F}_p^*$ $(g < p)$;

– $y = g^x \text{mod } p$.

Закрытым ключом является случайное целое число $x < p$.

Шифротекст (c_1, c_2) для сообщения $m < p$ вычисляется по формуле:

$$\begin{cases} c_1 = g^k (\text{mod } p), \\ c_2 = y^k (\text{mod } p), \end{cases} \tag{1.19}$$

где целое число $k < p$ выбирается случайным образом, k взаимно простое с $(p - 1)$ [1]. Шифротекст, полученный в результате шифрования методом Эль-Гамаля, в 2 раза длиннее открытого текста [1].

Для расшифровки (c_1, c_2) используется формула (1.20) [2].

$$m = \frac{c_2}{c_1^x} (\text{mod } p) \tag{1.20}$$

Система на основе эллиптических кривых

Открытым ключом в криптосистеме Эль-Гамаля на основе эллиптических кривых является $(\mathcal{E}, P, A)$, где

– $\mathcal{E}$ — эллиптическая кривая;

– P — точка высокого порядка из группы точек $\mathcal{E}\mathcal{F}$, N — порядок этой точки;

– $A = k \cdot P$.

Закрытым ключом является случайное число $k \in \mathbb{Z}_N^*$.

Получение зашифрованного сообщения $C = (C_1, C_2)$ выполняется по формулам

$$\begin{aligned} C_1 &= r \cdot P \\ C_2 &= M + r \cdot A, \end{aligned} \tag{1.21}$$

где сообщение m представляется как точка $M \in \mathcal{E}$, а $r \in \mathbb{Z}_N^*$ — некоторое случайное число (рандомизатор).

Расшифровка выполняется по формуле (1.22).

$$M = ((N-1) \cdot k \cdot r) \cdot P + C_2 \tag{1.22}$$

1.4 Сравнительный анализ рассмотренных методов

В качестве критериев сравнения методов асимметричного шифрования данных выбраны следующие параметры:

– класс трудновычислимой задачи;

– длина ключей для 128-битной безопасности [6] (уровень криптографической стойкости, при котором для успешной атаки на алгоритм потребуется вычислительная мощность, эквивалентная перебору 2^{128} вариантов);

– отношение длины зашифрованного текста к длине открытого текста;

– поддержка работы с входными данными, состоящими из случайных битов;

– скорость генерации ключей (для 128-битной безопасности) [6];

– скорость шифрования (для 128-битной безопасности) [6];

– скорость расшифровки (для 128-битной безопасности) [6].

В таблице 1.1 представлены результаты сравнения рассмотренных методов.

Таблица 1.1 – Сравнение основных методов асимметричного шифрования данных

Критерий	RSA	Rabin	ElGamal	EC ElGamal
Класс трудно-вычислимой задачи	Факторизация	Факторизация	Дискретные логарифмы	Эллиптические кривые
Длина ключей для 128-битной безопасности, биты	3072	3072	3072	256
Отношение длины шифротекста к длине открытого текста	1:1	1:1	2:1	2:1
Поддержка работы со случайными данными	Есть	Нет	Есть	Есть
Скорость генерации ключей, с	42.600	–	893.400	0.066
Скорость шифрования, с	0.623	–	13.000	0.532
Скорость расшифровки, с	5.900	–	181.800	0.467

В сравнении отсутствуют данные о скорости работы криптосистемы Рабина, т. к. авторы исследования [6] не включали данный метод в рассмотрение.

ЗАКЛЮЧЕНИЕ

В ходе выполнения научно-исследовательской работы были выполнены следующие задачи:

– проанализирована предметная область;
– выделены основные вехи развития асимметричного шифрования данных;
– формализована задача асимметричного шифрования данных;
– перечислены методы асимметричного шифрования данных;
– сформулированы критерии сравнения;
– проведено сравнение перечисленных методов по сформулированным критериям.

Все поставленные задачи выполнены, цель научно-исследовательской работы, которая заключалась в проведении сравнительного анализа методов асимметричного шифрования данных, достигнута.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. *Шнайер Б.* Прикладная криптография: протоколы, алгоритмы и исходных код на C. — 2-е юбилейное. — Санкт-Петербург : ООО "Диалектика", 2019. — Перевод с английского.
2. *Мао В.* Современная криптография: теория и практика. — Москва : Издательский дом "Вильямс", 2005. — Перевод с английского.
3. *Смарт Н.* Криптография. — Москва : Техносфера, 2005.
4. Алгоритмические основы эллиптической криптографии / А. Болотов [и др.]. — Москва : Изд-во РГСУ, 2004.
5. *Саломаа А.* Криптография с открытым ключом: Пер. с англ. — Москва : Мир, 1995. — ил.
6. *Singh S. R.*, *Khan A. K.*, *Singh S. R.* Performance evaluation of RSA and Elliptic Curve Cryptography // 2016 2nd International Conference on Contemporary Computing and Informatics (IC3I). — Bangalore, India : IEEE, 2016. — С. 302—306.

ПРИЛОЖЕНИЕ А

Презентация к научно-исследовательской работе состоит из 3 слайдов.