

ОГЛАВЛЕНИЕ

Введение 3

Постановка задачи 4

1. Общая информация о криптосистеме Эль-Гамала 5

 1.1 Алгоритм создания открытого и закрытого ключей 6

 1.2 Шифрование и расшифрование 6

 1.3 Дешифрование 7

2. Алгоритмы решения задачи дискретного логарифмирования 8

Список используемых источников 9

ВВЕДЕНИЕ

В настоящее время в вузах Российской Федерации базовые стандарты обучения для ряда специальностей включают в себя разделы, связанные с изучением методов и средств защиты информации. Для успешного освоения данных тем необходимо понимание принципов и знание основных элементов криптографического преобразования информации.

В Интернете можно найти десятки описаний лабораторных работ, посвященных криптографической системе Эль Гамала [1 – 3]. К сожалению, подавляющее большинство из них содержат задания и примеры реализации схемы Эль Гамала без учета особенностей длинной арифметики, не требуя обоснований алгоритмов и использования обучающих программ, не затрагивая вопросы криптоанализа. Известно несколько компьютерных обучающих программ, позволяющих быстро и достаточно полно ознакомиться с алгоритмами шифрования и расшифрования данных, используемыми в традиционных симметричных и современных асимметричных криптосистемах. К сожалению, эти программы, представленные в сети Интернет, не сопровождаются исходными текстами, ограничиваются краткой справочной информацией и содержат большое число ошибок и недочетов. В связи с этим и было принято решение: разработать алгоритм и реализовать свою электронную обучающую программу для изучения криптосистемы Эль Гамала. Предлагаемый вариант лабораторной работы позволяет, на мой взгляд, преодолеть указанные недостатки.

ПОСТАНОВКА ЗАДАЧИ

1. Провести анализ криптографического алгоритма Эль Гамала.
2. Разработать сценарий выполнения лабораторной работы по изучению алгоритма Эль Гамала.
3. Разработать и реализовать обучающую компьютерную программу "El-Gamal_Tutor".

1. ОБЩАЯ ИНФОРМАЦИЯ О КРИПТОСИСТЕМЕ ЭЛЬ-ГАМАЛЯ

Схема Эль-Гамала (Elgamal) — криптосистема с открытым ключом, основанная на трудности вычисления дискретных логарифмов в конечном поле. Криптосистема включает в себя алгоритм шифрования и алгоритм цифровой подписи. Схема Эль-Гамала лежит в основе бывших стандартов электронной цифровой подписи в США (DSA) и России (ГОСТ Р 34.10-94, ГОСТ Р 34.10-2001). Схема была предложена Тахером Эль-Гамалем в 1985 году. Эль-Гамаль разработал один из вариантов алгоритма Диффи-Хеллмана. Он усовершенствовал систему Диффи-Хеллмана и получил два алгоритма, которые использовались для шифрования и для обеспечения аутентификации. В отличие от RSA алгоритм Эль-Гамала не был запатентован и, поэтому, стал более дешевой альтернативой, так как не требовалась оплата взносов за лицензию. Считается, что алгоритм попадает под действие патента Диффи-Хеллмана. Криптографические системы с открытым ключом используют так называемые односторонние функции, которые обладают следующим свойством:

- Если известно x , то $f(x)$ вычислить относительно просто
- Если известно $y = f(x)$, то для вычисления x нет простого (эффективного) пути.

Под односторонностью понимается не теоретическая однонаправленность, а практическая невозможность вычислить обратное значение, используя современные вычислительные средства, за обозримый интервал времени. В основу криптографической системы Эль-Гамала положена сложность задачи дискретного логарифмирования в конечном поле. Для шифрования используется операция возведения в степень по модулю большого числа. Для дешифрования за разумное время необходимо уметь вычислять дискретный логарифм в конечном поле по простому модулю, что является вычислительно трудной задачей. В криптографической системе с открытым ключом каждый участник располагает как открытым ключом (англ. public key), так и закрытым ключом (англ. private key). В криптографической

системе Эль-Гамала открытый ключ состоит из тройки чисел, а закрытый ключ состоит из одного числа. Каждый участник создаёт свой открытый и закрытый ключ самостоятельно. Закрытый ключ каждый из них держит в секрете, а открытые ключи можно сообщать кому угодно или даже публиковать их.

1.1 Алгоритм создания открытого и закрытого ключей

Ключи в схеме Эль-Гамала генерируются следующим образом:

1. Генерируется случайное простое число p .
2. Выбирается целое число g — первообразный корень p .
3. Выбирается случайное целое число x , такое, что $1 < x < p$.
4. Вычисляется $y = g^x \bmod p$.
5. Открытым ключом является тройка (p, g, y) , закрытым ключом — число x .

1.2 Шифрование и расшифрование

Предположим, пользователь А хочет послать пользователю Б сообщение. Сообщениями являются целые числа в интервале от 0 до $p - 1$. Алгоритм для шифрования:

1. Взять открытый ключ пользователя Б
2. Взять открытый текст M
3. Выбрать сессионный ключ — случайное целое число k такое, что $1 < k < p - 1$
4. Зашифровать сообщение с использованием открытого ключа пользователя Б, то есть вычислить числа: $a = g^k \bmod p$, и $b = y^k M \bmod p$.

Алгоритм для расшифрования:

1. принять зашифрованное сообщение (a, b) от пользователя А
2. Взять свой закрытый ключ M
3. Применить закрытый ключ для расшифрования сообщения: $M = b(a^x)^{-1} \bmod p$
4. При этом нетрудно проверить, что $(a^x)^{-1} \equiv g^{-kx} \pmod{p}$, и поэтому $b(a^x)^{-1} \equiv (y^k M)g^{-xk} \equiv (g^{xk} M)g^{-xk} \equiv M \pmod{p}$.

1.3 Дешифрование

Дешифрование - получение открытых данных по зашифрованным в условиях, когда алгоритм расшифрования и его секретные параметры не являются полностью известными и расшифрование не может быть выполнено обычным путем. Алгоритм для дешифрования криптосистемы Эль-Гамала:

1. Перехватить зашифрованное сообщение (a, b) .
2. Взять открытый ключ p, g, y
3. Решить относительно x уравнение $y \equiv g^x \pmod{p}$
4. Расшифровать сообщение по формуле $M = b(a^x)^{-1} \bmod p$

Собственно, самый главный вопрос из этого алгоритма – как по данным (p, g, y) найти x . Эта задача называется задачей дискретного логарифмирования [2].

2. АЛГОРИТМЫ РЕШЕНИЯ ЗАДАЧИ ДИСКРЕТНОГО ЛОГАРИФМИРОВАНИЯ



Рис. 1: Ну это типа Хеллман короч

Литература

1. **Гилбарг, Д.** Эллиптические дифференциальные уравнения с частными производными второго порядка / Д. Гилбарг, П. Трудингер. — М. : Наука, 1989. — 464 с.
2. **Ильин, В. А.** О рядах Фурье по фундаментальным системам функций оператора Бельтрами/В. А. Ильин // Дифференц. уравнения. — 1969. — Т. 5, № 11. — С. 1940–1978.
3. **Ильин, В. А.** Некоторые свойства регулярного решения уравнения Гельмгольца в плоской области / В. А. Ильин // Мат. заметки. — 1974. — Т. 15, № 6. — С. 885–890.
4. **Ильин, В. А.** Об одном обобщении формулы среднего значения для регулярного решения уравнения Шредингера / В. А. Ильин, Е. И. Моисеев // ИПМ АН СССР, 1977. — С. 157–166.
5. **Ильин, В. А.** Формула среднего значения для присоединенных функций оператора Лапласа / В. А. Ильин, Е. И. Моисеев // Дифференц. уравнения. — 1981. — Т. 17, № 10. — С. 1908–1910.
6. **Моисеев, Е. И.** Формула среднего для собственных функций эллиптического самосопряженного оператора второго порядка / Е. И. Моисеев // Докл. АН СССР. — 1971. — Т. 197, № 3. — С. 524–525.
7. **Моисеев, Е. И.** Асимптотическая формула среднего значения для регулярного решения дифференциального уравнения / Е. И. Моисеев // Дифференц. уравнения. — 1980. — Т. 16, № 5. — С. 827–844.

8. **Хелгасон, С.** Дифференциальная геометрия и симметрические пространства / С. Хелгасон. — М. : Мир, 1964. — 534 с.
9. **Иванов, Л. А.** О некоторых свойствах оператора Бельтрами в римановой метрике / Л. А. Иванов, И. П. Половинкин // Докл. РАН. — 1999. — Т. 365, № 3. — С. 306–309.
10. **Йон, Ф.** Плоские волны и сферические средние / Ф. Йон. — М. : Иностр. лит., 1958. — 158 с.
11. **Бицадзе, А. В.** К теории уравнений смешанного типа в многомерных областях / А. В. Бицадзе, А. М. Нахушев // Дифференц. уравнения. — 1974. — Т. 10, № 12. — С. 2184–2191.
12. **Гельфанд, И. М.** Обобщенные функции и действия над ними / И. М. Гельфанд, Г. Е. Шиллов. — М. : Физматлит, 1958. — 440 с.
13. **Хермандер, Л.** Анализ линейных дифференциальных операторов с частными производными. Т. 1 / Л. Хермандер. — М. : Мир, 1986. — 464 с.
14. **Мешков, В. З.** К свойствам решений линейных уравнений в частных производных / В. З. Мешков, И. П. Половинкин // Черноземный альманах научных исследований. — Сер. Фундамент. математика. — 2007. — Вып. 1(5). — С. 3–11.
15. **Мешков, В. З.** Разностная формула среднего значения для двумерного линейного гиперболического уравнения третьего порядка / В. З. Мешков, И. П. Половинкин, М. В. Половинкина, Ю. Д. Ермакова, С. А. Рабеева // ВЕСТНИК ВГУ. СЕРИЯ: ФИЗИКА. МАТЕМАТИКА. — 2015. — № 3
16. **Половинкин, И.П.** К свойствам решений линейных уравнений в частных производных / Половинкин И.П. // Вестник Челябинского государственного университета. Математика. Механика. Информатика. Выпуск 12. — 2010. — № 23(204) — С. 59–66.

17. **Половинкин, И.П.** О получении новых формул среднего значения для линейных дифференциальных уравнений с постоянными коэффициентами / Половинкин И.П., Мешков В.З. // Дифференциальные уравнения. — 2011 — - Т. 47, № 12 — С. 1724–1791.
18. **Половинкин, И.П.** Дополнения к свойствам средних значений решений линейных дифференциальных уравнений с постоянными коэффициентами / Половинкин И.П., Мешков В.З. // Дифференциальные уравнения. — 2011 — Т. 47, № 11 — С. 1669 – 1671.