ОГЛАВЛЕНИЕ

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 Гамаля [1 – 3]. К сожалению, подавляющее большинство из них содержат задания и примеры реализации схемы Эль Гамаля 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 Гамаля. Предлагаемый вариант лабораторной работы позволяет, на мой взгляд, преодолеть указанные недостатки.

ПОСТАНОВКА ЗАДАЧИ

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

1. ОБЩАЯ ИНФОРМАЦИЯ О КРИПТОСИСТЕМЕ ЭЛЬ-ГАМАЛЯ

Схема Эль-Гамаля (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-Гамаля 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-Гамаля 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-Гамаля 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-Гамаля 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-Гамаля 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 $y = g^x \ mod \ p$.
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: $a = g^k \ mod \ p$, и $b = y^k M \ mod \ p$.

Алгоритм для расшифрования:

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

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-Гамаля:

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

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