Тут типа титульник

Содержание

[Список основных понятий и сокращений 3](#_Toc514247965)

[Введение 4](#_Toc514247966)

[Постановка задачи 5](#_Toc514247967)

[1. Общая информация о криптосистеме Эль-Гамаля 6](#_Toc514247968)

# Список основных понятий и сокращений

Абелева (или коммутативная) группа — группа, в которой групповая операция является коммутативной; иначе говоря, группа (G, \*) абелева, если a\*b = b\*a для любых a, b, принадлежащих G.

Говорят, что числа a и b сравнимы по модулю m, если a и b при делении на m дают одинаковые остатки.

Множество всех чисел, сравнимых с a по модулю m, называется классом вычетов a по модулю m. Если определить для класса вычетов операции сложения и умножения, то такое множество будет называться кольцом вычетов a по модулю m.

Мультипликативной группой называют такую группу, в которой групповой бинарной операцией является умножение.

# 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”.

# 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 , то вычислить относительно просто

• Если известно , то для вычисления 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.