МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Отчет по лабораторной работе №10**

**″Исследование асимметричных шифров RSA и Эль-Гамаля″**

Выполнила студентка 3 курса 5 группы Максимчикова Ю. С.

Проверила: Блинова Е. А.

Минск 2020

**Цель**: изучение и приобретение практических навыков разработки и использования приложений для реализации асимметричных шифров RSA и Эль-Гамаля.

**Задачи**:

* Закрепить теоретические знания по алгебраическому описанию, алгоритмам реализации операций зашифрования/расшифрования и оценке криптостойкости асимметричных шифров RSA и Эль-Гамаля.
* Разработать приложение для реализации асимметричного зашифрования/расшифрования на основе алгоритмов RSA и Эль-Гамаля.
* Выполнить анализ криптостойкости асимметричных шифров RSA и Эль-Гамаля.
* Оценить скорость зашифрования/расшифрования реализованных шифров.
* Результаты выполнения лабораторной работы оформить в виде описания разработанного приложения, методики выполнения экспериментов с использованием приложения и результатов эксперимента.

**Теория.** Как отмечалось выше, асимметричная криптография основана на сложности решения некоторых математических задач. Эти задачи объединяет то, что они используют операцию получения остатка от целочисленного деления. В силу этого практически все системы асимметричного зашифрования/расшифрования основаны либо на проблеме факторизации (среди них – RSA), либо на проблеме дискретного логарифмирования (среди них – Эль-Гамаля).

**Алгоритм RSA.** Рассматриваемый алгоритм появился (1977 г.) после алгоритма рюкзака Меркла. Он стал первым полноценный алгоритмом с открытым ключом, который впоследствии стал одним из основных для шифрования и для электронных цифровых подписей. Из всех предложенных алгоритмов с открытыми ключами RSA проще всего понять и реализовать. Названный в честь трех его создателей: Рона Ривеста (RonRivest), Ади Шамира (Adi Shamir) и Леонарда Эдлемана (Leonard Adleman). Как было отмечено, безопасность RSA основана на трудности разложения на множители больших чисел. Открытый и закрытый ключи являются функциями двух больших простых чисел. Предполагается, что восстановление открытого текста по шифртексту и открытому ключу эквивалентно разложению на множители двух больших чисел. Для зашифрования/расшифрования используется ключ получателя: отправитель шифрует сообщение открытым ключом, а получатель расшифровывает шифртекст своим тайным ключом.

**Алгоритм Эль-Гамаля.** Предложен Эль-Гамалем (T. El-Gamal) в 1985 г. Он может быть использован для решения трех основных криптографических задач: для зашифрования/расшифрования данных, для формирования цифровой подписи и для согласования общего ключа. Кроме того, возможны модификации алгоритма для схем проверки пароля, доказательства идентичности сообщения и другие варианты. Как подчеркивалось выше, безопасность алгоритма Эль-Гамаля, как и безопасность алгоритма Диффи-Хеллмана, основана на трудности вычисления дискретных логарифмов. Алгоритм Эль-Гамаля фактически использует схему Диффи-Хеллмана, чтобы сформировать общий секретный ключ для абонентов, передающих друг другу сообщение, и затем сообщение шифруется путем умножения его на этот ключ. И в случае шифрования, и в случае формирования цифровой подписи каждому пользователю необходимо сгенерировать пару ключей. Рассматриваемый алгоритм отличается от алгоритма RSA несколькими параметрами и особенностями: 1) генерацией ключевой информации и числом компонент, составляющих ключ; 2) каждому блоку (символу) открытого сообщения в шифртексте на основе алгоритма Эль-Гамаля соответствуют 2 блока (в RSA – один-один); 3) в алгоритме Эль-Гамаля при зашифровании используется число (обозначим его k), которое практически никак не связано с ключевой информацией получателя и которое принимает (по определению) различные значения при зашифровании различных блоков сообщения.

**Задание.** В данной лабораторной работе необходимо было разработать авторское приложение в соответствии с целью лабораторной работы. Разработанное приложение реализует алгоритмы RSA и Эль-Гамаля.

**RSA.** Для генерации двух ключей: тайного и открытого(а по сути – двух взаимосвязанных частей одного ключа, т. е. ключа, принадлежащего одному физическому лицу (или группе лиц), либо одному юридическому лицу) используются два больших случайных простых числа, p и q. Для максимальной большей криптостойкости нужно выбирать p и q равной длины. Рассчитывается произведение: n = pq. Этой есть один из трех компонент ключа, состоящего из чисел n, e, d. Затем случайным образом выбирается второй компонент ключа(открытый ключ или ключ зашифрования, e, такой что e и (p-1)(q-1) являются взаимно простыми числами; вспомним, что (p-1)(q-1) = φ(n) – функция Эйлера. Б. Шнайер [4] рекомендует число е выбирать из ряда: 3, 17, 216 + 1. Наконец расширенный алгоритм Евклида используется для вычисления третьего компонента ключа: ключа расшифрования, d, такого, что выполняется условие: ed = 1 (mod φ(n)). Другими словами: d-1 = e (mod φ(n)). Таким образом, сформирован ключ, состоящий из трех чисел, которые, в свою очередь, образуют две вышеупомянутые взаимосвязанные части: открытый (публичный) ключ, (e, n), и тайный ключ, (d, n; на самом деле, как видим, тайным здесь является лишь первое из пары чисел).

Реализация функции для генерации открытого и закрытого ключа представлена на рисунке 1.

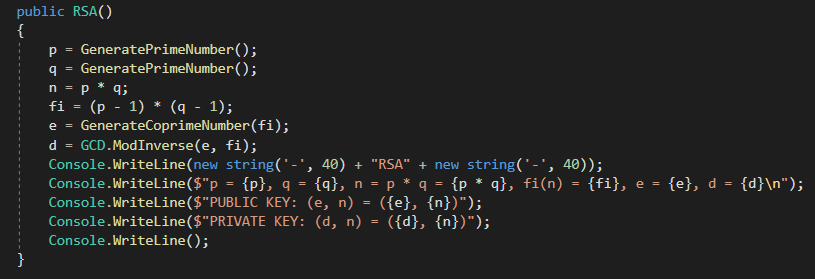


Рис. 1 – Генерация открытого и закрытого ключа

Если шифруется сообщение М, состоящее из r блоков: m1, m2 , …, mi,…,mr, то шифртекст С будет состоять из такого же числа (r) блоков, представляемых числами: ci = (mi)e mod n.

Реализация функции шифрования представлена на рисунке 2.

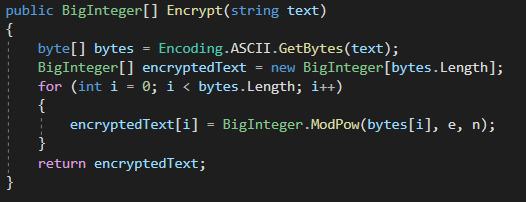


Рис. 2 – Функция шифрования RSA

Для расшифрования каждого зашифрованного блока производится вычисление вида: mi = (ci)d mod n.

Реализация функции расшифрования представлена на рисунке 3.

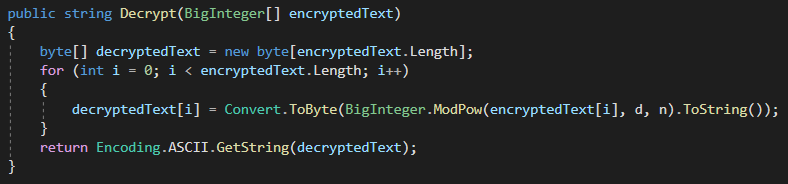


Рис. 3 – Функция расшифрования RSA

**Эль-Гамаль.** Генерация ключевой информации. Выбирается простое число, р. Выбирается число (g, g < p), являющееся первообразным корнем числа р – очень важный элемент с точки зрения безопасности алгоритма. Далее выбирается число х (х < p) и вычисляется последний компонент ключевой информации: y =gх mod р. Владельцу сформированной ключевой информации, состоящей из 4 чисел, может посылаться некоторый шифртекст, созданный с использованием открытого ключа получателя: p, g, y. Расшифрование шифртекста получатель производит своим тайным ключом: p, g, х.

Реализация функции для генерации открытого и закрытого ключа представлена на рисунке 4.

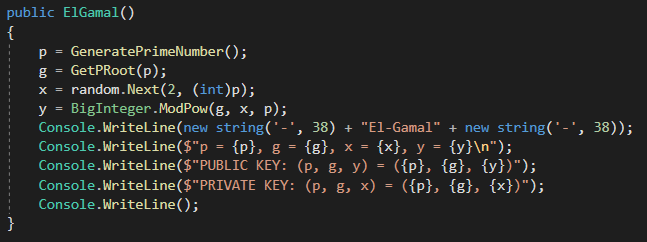


Рис. 4 – Генерация открытого и закрытого ключа

Зашифрование сообщения. Как ранее, предположим, что сообщение М = {mi}, где – mi – i-й блок сообщения. Зашифрование отправителем (каждого отдельного блокаmi исходного сообщения) предусматривает использование, как это особо подчеркивалось выше, некоторого случайного числа k (1 < k <p – 1). В силу использования случайной величины k шифр Эль-Гамаля называют также шифром многозначной замены, а также схемой вероятностного шифрования. Вероятностный характер шифрования является преимуществом для схемы Эль-Гамаля по сравнению, например, с алгоритмом RSA. Блок шифртекста (ci) состоит из двух чисел: аi и bi: ai = gk mod p, bi = (yk \*mi) mod p. Здесь стал очевидный упомянутый недостатком алгоритма шифрования Эль-Гамаля: удвоение (реально – примерно в 1,5 раза) длины зашифрованного текста по сравнению с начальным текстом. Случайное число k должно сразу после вычисления уничтожаться.

Реализация функции шифрования представлена на рисунке 5.

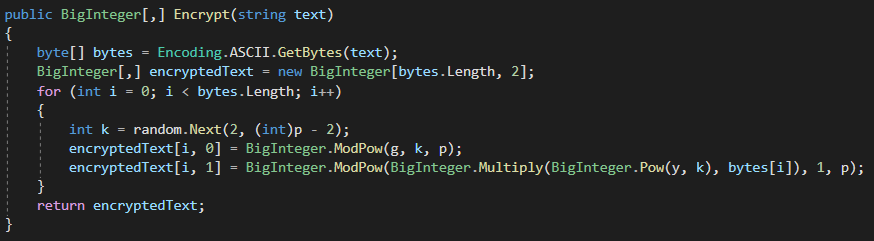


Рис. 5 – Функция шифрования Эль-Гамалем

Расшифрование ci выполняется по следующей формуле: mi = (bi \*(ai)x)-1) mod p или mi = (bi \*(ai)р-x-1) mod, где (ax)-1 – обратное значение числа ax по модулю p.

Реализация функции расшифрования представлена на рисунке 6.

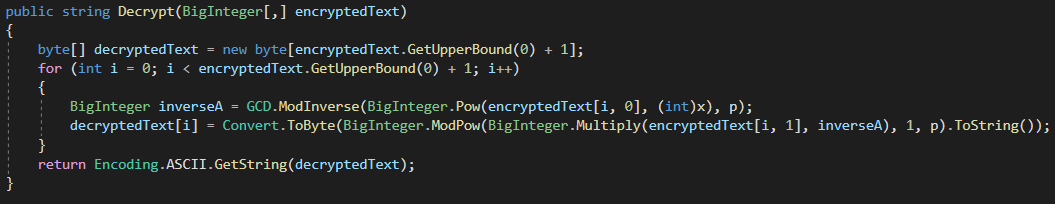


Рис. 6 – Функция расшифрования Эль-Гамалем

Результат работы алгоритмов и замеры времени выполнения операция шифрования и расшифрования сообщения Maximchikova Yuliya представлены на рисунке 7.

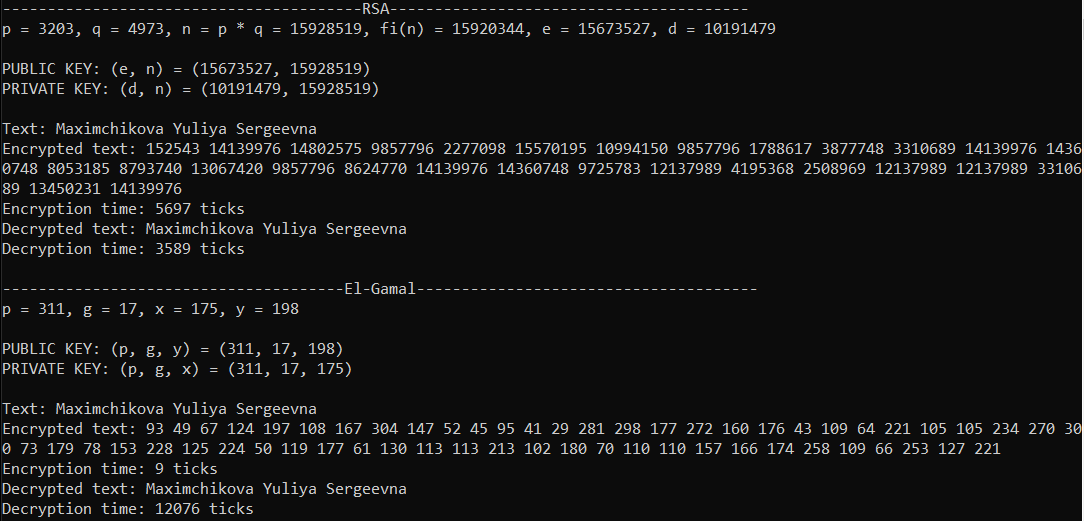


Рис. 7 – Результат работы приложения

Вывод: в результате данной лабораторной работы было разработано приложение, реализующее шифрование и расшифрование сообщения с помощью алгоритмов RSA и Эль-Гамаля. Также был проведен анализ его криптостойкости и замеры времени работы операций шифрования и расшифрования с помощью этих алгоритмов.