МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Отчет по лабораторной работе №9**

**″Исследование асимметричных шифров″**

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.

**Задачи**:

* Закрепить теоретические знания по алгебраическому описанию, алгоритмам реализации операций зашифрования/расшифрования и оценке криптостойкости асимметричных шифров.
* Разработать приложение для реализации указанных преподавателем методов генерации ключевой информации и ее использования для асимметричного зашифрования/расшифрования.
* Выполнить анализ криптостойкости асимметричных шифров.
* Оценить скорость зашифрования/расшифрования реализованных шифров.
* Оценить скорость зашифрования/расшифрования реализованных способов шифров.
* Результаты выполнения лабораторной работы оформить в виде описания разработанного приложения, методики выполнения экспериментов с использованием приложения и результатов эксперимента.

**Теория.** В основу асимметричной криптографии положена идея использовать ключи парами: один – для зашифрования (открытый или публичный ключ), другой – для расшифрования (тайный ключ). Отметим, что указанная пара ключей принадлежит получателю зашифрованного сообщения. Все алгоритмы шифрования с открытым ключом основаны на использовании односторонних функций, к числу которых, как известно, относится вычисление дискретного логарифма.

**Криптоалгоритм на основе задачи об укладке ранца**. Алгоритм разработан Р. Мерклом и М. Хеллманом. Ранцевый (рюкзачный) вектор S = (s1, . . ., sz) – это упорядоченный набор из z, z ≥ 3, различных натуральных чисел si. Входом задачи о

ранце (рюкзаке) называем пару (S, S), где S – рюкзачный вектор, а S – натуральное число. Решением для входа (S, S) будет такое подмножество из S, сумма элементов которого равняется S. В наиболее известном варианте задачи о ранце требуется выяснить, обладает или нет данный вход (S, S) решением. В варианте, используемом в криптографии, нужно для данного входа (S, S) построить решение, зная, что такое решение существует. Оба эти варианта являются NP-полными. Имеются также варианты этой задачи, которые не лежат даже в классе NP. Как видим, проблема укладки ранца формулируется просто. Дано множество предметов общим числом z различного веса. Спрашивается, можно ли положить некоторые из этих предметов в ранец так, чтобы его вес стал равен определенному значению S? Более формально задача формулируется так: дан набор значений s1, s2, …, sz и суммарное значение S. Требуется вычислить значения si такие, что S = b1s1 + b2s2+... + bzsz. (7.1) Здесь bi может быть либо нулем, либо единицей. Значение bi = 1 означает, что предмет mi кладут в рюкзак, а bi = 0 – не кладут. Суть метода для шифрования состоит в том, что существуют две различные задачи укладки ранца: одна из них решается легко и характеризуется линейным ростом трудоемкости, а другая решается трудно. Легкий для укладки ранец можно трансформировать в трудный. Трудный для укладки ранец применяется в качестве открытого ключа е, который легко использовать для зашифрования, но невозможно – для расшифрования. В качестве закрытого ключа d применяется легкий для укладки ранец, который предоставляет простой способ расшифрования сообщения. В качестве закрытого ключа d (легкого для укладки ранца) используется сверхвозрастающая последовательность, состоящая из z элементов: d1, d2,…, dz: d = {di}, i = 1,…, z. Определение 3. Сверхвозрастающей называется последовательность, в которой каждый последующий член больше суммы всех предыдущих. Пример 1. Последовательность {2, 3, 6, 13, 27, 52, 105, 210} (z = 8) является сверхвозрастающей, а {1, 3, 4, 9, 15, 25, 48, 76} – нет.

**Алгоритм укладки ранца на основе сверхвозрастающей последовательности.** Необходимо по очереди анализировать некоторый «текущий вес» S предметов, составляющих сверхвозрастающую последовательность; в результате анализа нужно упаковать (доупаковать) ранец. 1. В качестве текущего выбирается число S, которое сравнивается с «весом» самого тяжелого предмета (dz); если текущий вес меньше веса данного предмета, то его в ранец не кладут (0), в противном случае его укладывают (bz = 1) в ранец и переходят к анализу очередного (в общем случае – i-го предмета). 2. Если на предыдущем (i-м шаге) предмет пополнил ранец, то текущий вес уменьшают на вес положенного предмета (S = S – di); переходят к следующему по весу предмету в последовательности: di-1. Шаги повторяются до тех пор, пока процесс не закончится. Если текущий вес уменьшится до нуля (S = 0), то решение найдено. В противном случае – нет.

**Задание**. В данной лабораторной работе необходимо было разработать авторское приложение в соответствии с целью лабораторной работы. Данное приложение генерирует сверхвозрастающую последовательность, вычисляет нормальную последовательность, шифрует и расшифрует сообщение, а также выполняет оценку времени выполнения операций зашифрования и расшифрования

Функция для генерации сверхвозрастающей последовательности представлена на рисунке 1.

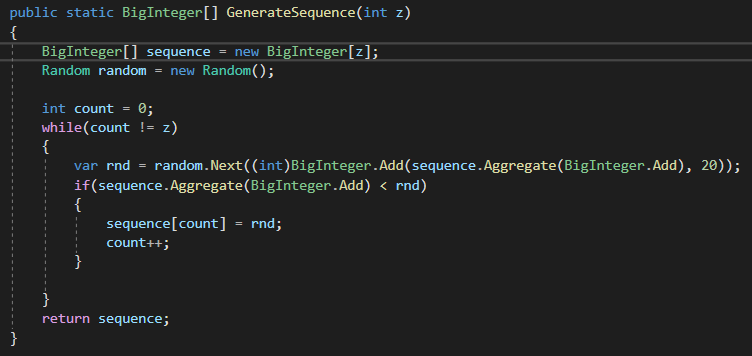


Рис. 1 – Генерация сверхвозрастающей последовательности

Сверхвозрастающей называется последовательность, в которой каждый последующий член больше суммы всех предыдущих.

В качестве закрытого ключа d (легкого для укладки ранца) используется сверхвозрастающая последовательность, состоящая из z элементов: d1, d2, …, dz: d = {di}, i = 1, …, z.

Реализация функции генерации закрытого ключа представлена на рисунке 2.

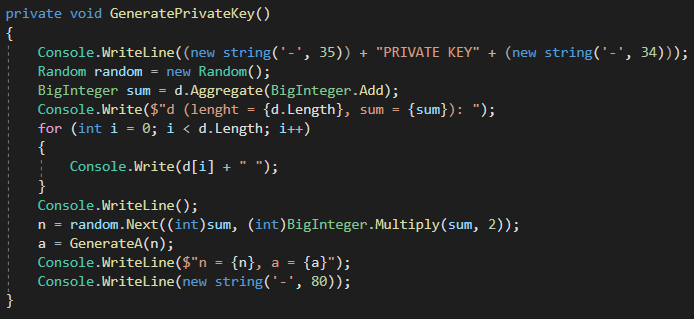


Рис. 2 – Функция генерации закрытого ключа

Открытый ключ e представляет собой нормальную (не сверхвозрастающую) последовательность. Он формируется на основе закрытого ключа и не позволяет легко решить задачу об укладке ранца. Для получения открытого ключа e (e = {ei}, i = 1, …, z) все значения закрытого ключа умножаются на некоторое число a по модулю n: ei = di a (mod n).

Значение модуля n должно быть больше суммы всех чисел последовательности; кроме того, НОД (а, n) = 1.

Реализация функции генерации публичного ключа представлена на рисунке 3.

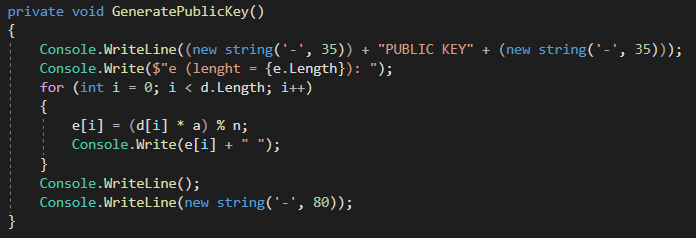


Рис. 3 – Функция генерации публичного ключа

Для зашифрования сообщения (М) оно сначала разбивается на блоки, по размерам равные числу (z) элементов последовательности в ранце. Затем, считая, что 1 указывает на присутствие элемента последовательности в ранце, а 0 – на его отсутствие, вычисляются полные веса рюкзаков (Si, i = 1, . . ., z): по одному ранцу для каждого блока сообщения с использованием открытого ключа получателя, e.

Реализация функции зашифрования представлена на рисунке 4.

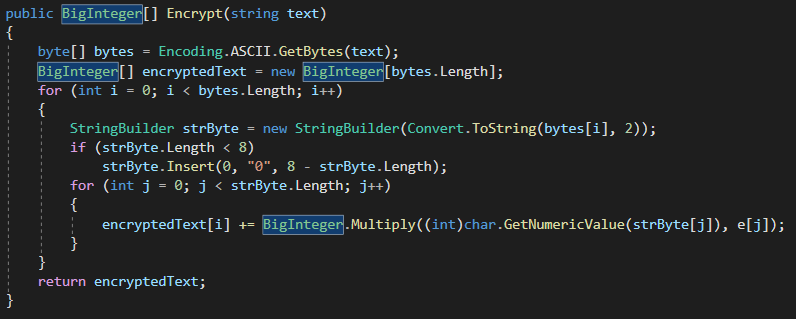


Рис. 4 – Функция зашифрования

Для расшифрования сообщения получатель (использует свой тайный ключ, d: сверхвозрастающую последовательность) должен сначала определить обратное к а число: а-1, такое что а \* а-1(mod n) = 1.

Для вычисления обратных чисел по модулю можно использовать известный нам расширенный алгоритм Евклида. После определения обратного числа каждое значение шифрограммы (ci) преобразуется в соответствии со следующим соотношением: Si = ci а-1 mod n.

Полученное на основании последней формулы для каждого блока число далее рассматривается как заданный вес ранца, который следует упаковать по изложенному выше алгоритму, используя сверхвозрастающую последовательность (тайный ключ получателя).

Реализация функции расшифрования представлена на рисунке 5.

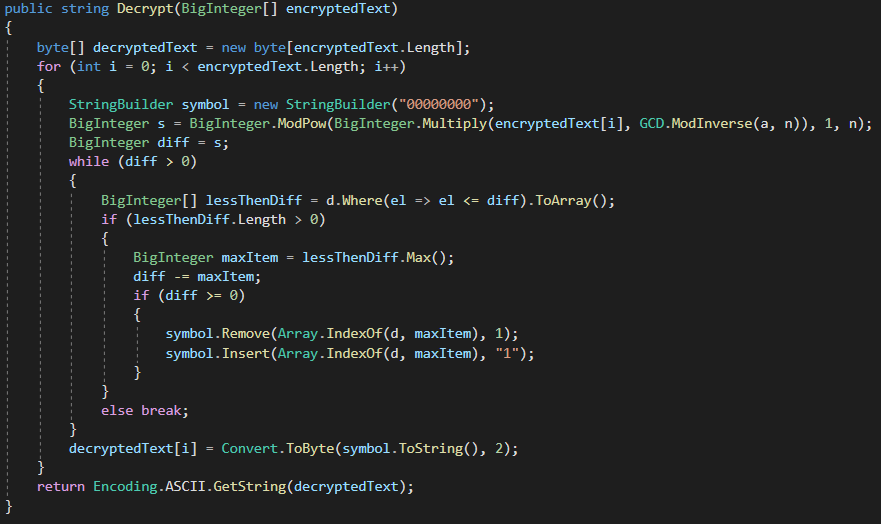


Рис. 5 – Функция расшифрования

Результат работы алгоритма и замеры времени выполнения операция шифрования и расшифрования сообщения Maximchikova Yuliya Sergeevna представлены на рисунке 6.

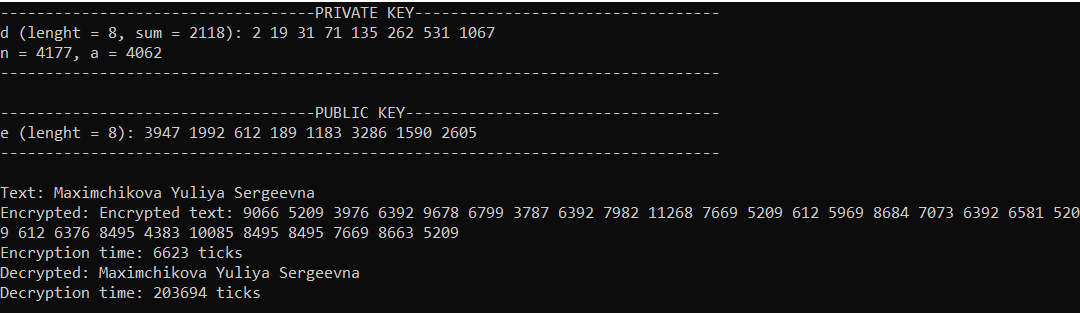


Рис.6 – Результат работы приложения

Вывод: в результате данной лабораторной работы было разработано приложение для реализации криптоалгоритма на основе задачи об укладке ранца. Также был проведен анализ его криптостойкости и замеры времени работы операций шифрования и расшифрования с помощью этого алгоритма.