Министерство образования Республики Беларусь

Учреждение образование

«Белорусский государственный технологический университет»

Кафедра информационных систем и технологий

**Отчет к лабораторной работе**:

«Исследование ассиметричных шифров»

Выполнил:

студент III курса 8 группы

специальности ПОИБМС

Астровская Д.А.

Проверил:

Берников Владислав Олегович

Минск 2022**1. Теоретические сведения**

**1.1 Основные свойства ассиметричных криптосистем**

*Потоковый шифр* (иногда говорят «поточный») – симметричный шифр, преобразующий каждый символ *mi* открытого текста в символ шифрованного, *ci*, зависящий от ключа и расположения символа в тексте.

Две известные нам проблемы, связанные с практическим использованием симметричных криптосистем, стали важными побудительными мотивами для разработки принципиально нового класса методов шифрования: криптографии с *открытым* ключом или *асимметричной криптографии*.

Концепция нового подхода предложена Уитфилдом Диффи (Whitfield Diffie) и Мартином Хеллманом (Martin Hellman), и, независимо, Ральфом Мерклом (Ralph Merkle).

В основу асимметричной криптографии положена идея использовать ключи парами: один – для зашифрования (открытый или публичный ключ), другой – для рас-шифрования (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. Определение 1. *Односторонней функцией* (one-way function) называется математическая функция, которую относительно легко вычислить, но трудно найти по значению функции соответствующее значение аргумента, т. е., зная *х*, легко вычислить *f*(*x*), но по известному *f*(*x*) трудно найти подходящее значение *x*.

Практически первой реализацией идеи Диффи-Хеллмана стал алгоритм согласования по открытому каналу тайного ключа между абонентами *А* и В.

Алгоритмы шифрования с открытым ключом можно использовать для решения следующих задач: зашифрования/расшифрования передаваемых и хранимых данных в целях их защиты от несанкционированного доступа, формирования цифровой подписи под электронными документами, распределения секретных ключей, используемых далее при шифровании документов симметричными методами.

**1.2 Общая характеристика алгоритма**

Алгоритм разработан Р. Мерклом и М. Хеллманом. Стал первым алгоритмом шифрования с открытым ключом широкого назначения.

*Определение* 2. *Ранцевый* (*рюкзачный*) *вектор* ***S*** = (*s*1, . . ., *s*z) – это упоря-доченный набор из *z*, *z* ≥ 3, различных натуральных чисел *s*i. 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, s*2, …, *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 zэлементов: d*1, *d2,…, dz*: ***d*** = {*di*}, *i* = 1,…, *z*.

*Определение* 3. *Сверхвозрастающей* называется последовательность, в ко-торой 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.

**1.3 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.

*Пример 2*. Пусть полный вес ранца равен 270, а последовательность весов предметов равна: {2, 3, 6, 13, 27, 52, 105, 210} (*d*1 =2, *d*2 =3, *d*3 =6 и т.д.).

Шаг 1. *S*=270. Самый большой вес предмета (*dz* = *d*8)– 210. Он меньше 270, поэтому предмет весом 210 кладут в ранец (1): вычитают 210 из 270 и получают 60: *S* = *S* – *d*8 = 270 – 210 = 60.

Шаг 2. Следующий наибольший вес последовательности равен 105. Он больше 60, поэтому предмет весом 105 в ранец не кладут (0): *S* = *S* – 0 = 60.

Шаг 3. Следующий самый тяжелый предмет имеет вес 52. Он меньше 60, поэтому предмет весом 52 также кладут в рюкзак (1): *S* = *S* – 52 = 8.

На 4-м и на 5-м шагах рюкзак не пополняется. Текущий вес его остается неизменным.

На 6-м шаге в ранец кладут предмет весом 6 и на 8-м шаге – весом 2.

В результате полный вес уменьшится до 0, т. е. получили текущее значение *S* = 0.

Если бы этот ранец был бы использован для расшифрования, то открытый текст, полученный из значения шифртекста 270, был бы равен 10100101.

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.

*Пример 3*. Сумма элементов последовательности {2, 3, 6, 13, 27, 52, 105, 210} равна 418: 2+3+6+13+27+52+105+210=418. Элементы *di* этой последовательности являются элементами ключа ***d***: ***d*** = {*di*}. Примем, что *n* = 420 и а=31.

В соответствии с этими при использовании (7.2) результат построения нормальной последовательности (открытого ключа, ***е***) будет представлен следующим множеством: {62, 93, 186, 403, 417, 352, 315, 210}: *е*1 = 62, *е*2 = 93 и т. д.

**2. Практическая часть**

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

**Задачи:**

1. Закрепить теоретические знания по алгебраическому описанию, алгоритмам реализации операций зашифрования/расшифрования и оценке крипто-стойкости асимметричных шифров.

2. Разработать приложение для реализации указанных преподавателем методов генерации ключевой информации и ее использования для асимметричного зашифрования/расшифрования.

3. Выполнить анализ криптостойкости асимметричных шифров.

4. Оценить скорость зашифрования/расшифрования реализованных шифров.

5. Результаты выполнения лабораторной работы оформить в виде описания разработанного приложения, методики выполнения экспериментов с использованием приложения и результатов эксперимента.

**Ход работы**

В данной лабораторной работе мы работали с шифром на основе укладки рюкзака. Это асимметричный шифр. 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.

Меркль и Хеллман предложили использовать задачу об укладке ранца (рюкзака) для асимметричного шифрования . Она относится к классу NP-полных задач и формулируется следующим образом. Дано множество предметов различного веса. Спрашивается, можно ли положить некоторые из этих предметов в ранец так, чтобы его вес стал равен определенному значению? Более формально задача формулируется так: дан набор значений M1, M2, ..., Мn и суммарное значение S; требуется вычислить значения bi такие что:

S = b1М1 + b2М2 + ... + bnМn,

где n - количество предметов;

bi - бинарный множитель. Значение bi = 1 означает, что предмет i кладут в рюкзак, bi = 0 - не кладут.

В основе алгоритма, предложенного Мерклом и Хеллманом, лежит идея шифрования сообщения на основе решения серии задач укладки ранца. Предметы из кучи выбираются с помощью блока открытого текста, длина которого (в битах) равна количеству предметов в куче. При этом биты открытого текста соответствуют значениям b, a текст является полученным суммарным весом. Пример шифрограммы, полученной с помощью задачи об укладке ранца, показан в следующей таблице.

Суть использования данного подхода для шифрования состоит в том, что на самом деле существуют две различные задачи укладки ранца - одна из них решается легко и характеризуется линейным ростом трудоемкости, а другая, как принято считать, нет. Легкий для укладки ранец можно превратить в трудный. Раз так, то можно применить в качестве открытого ключа трудный для укладки ранец, который легко использовать для шифрования, но невозможно - для дешифрования. А в качестве закрытого ключа применить легкий для укладки ранец, который предоставляет простой способ дешифрования сообщения.

В качестве закрытого ключа (легкого для укладки ранца) используется сверхвозрастающая последовательность. Сверхвозрастающей называется последовательность, в которой каждый последующий член больше суммы всех предыдущих.

В данной лабораторной работе необходимо было разработать приложение, которое реализует алгоритм генерации Шифрования на основе укладки ранца. Основная реализация шифрования представлена на рисунке (Рисунок 2.1):

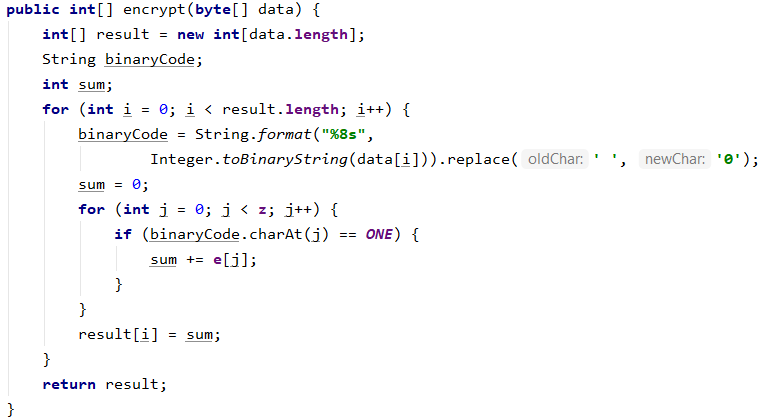


Рисунок 2.1 – Шифрование на основе укладки ранца

Дешифрование приведено на рисунке (Рисунок 2.2)

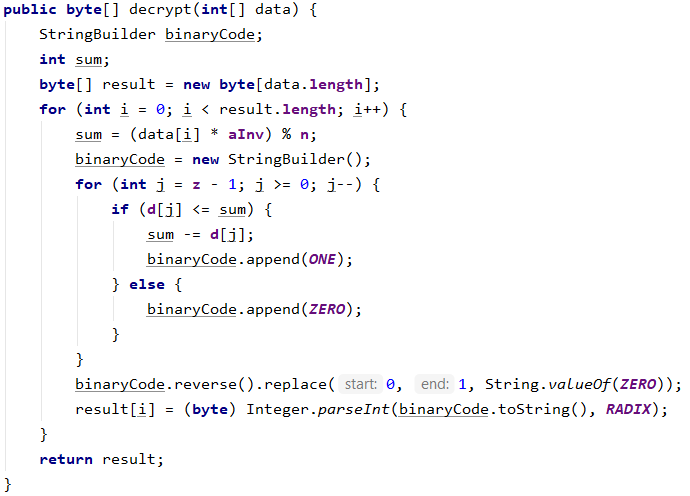


Рисунок 2.2 – Дешифрование на основе укладки ранца

Результат выполнения этого алгоритма представлен ниже (Рисунок 2.3):

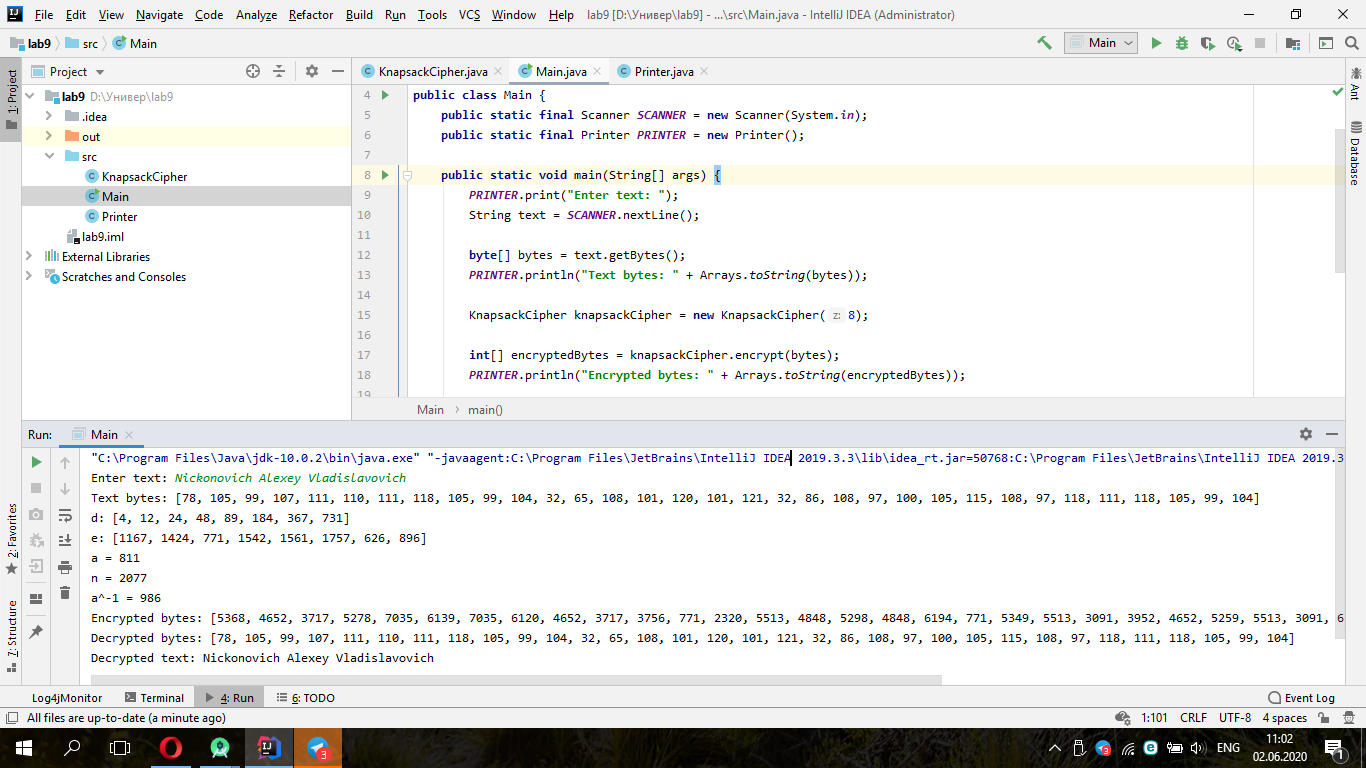


Рисунок 2.3 – Результат

**Вывод**

Таким образом, в ходе лабораторной работы были реализованы программно шифрование на основе укладки ранца. Также теоретически изучены основы алгоритма укладки ранца на основе сверхвозрастающей последовательности