Учреждение образования

«Белорусский государственный технологический университет»

**Кафедра информационных систем и технологий**

**«Отчёт по лабораторной работе 9»**

“ ИССЛЕДОВАНИЕ АСИММЕТРИЧНЫХ ШИФРОВ”

**Выполнил:** студент 3 курса

4 группы специальности ПОИТ

Примаков Максим Николаевич

**Проверил:** преподаватель

Блинова Евгения Александровна

Минск 2021

**Теоретическая часть**

В основу асимметричной криптографии положена идея использовать ключи парами: один – для зашифрования(открытый, или публичный, ключ), другой – для расшифрования(тайный ключ).

*Односторонней функцией* (one-wayfunction) 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*.

**Криптоалгоритм на основе задачи об укладке ранца**

**Общая характеристика алгоритма**

Алгоритм разработан Р. Мерклом и М. Хеллманом. Это первый алгоритм шифрования с открытым ключом широкого назначения.

*Ранцевый* (*рюкзачный*) *вектор* ***S*** = (*s*1, ..., *s*z) – 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 *k*1, *k*2, …, *kz* и суммарное значение *S*. Требуется вычислить значения *bz* такие, что:

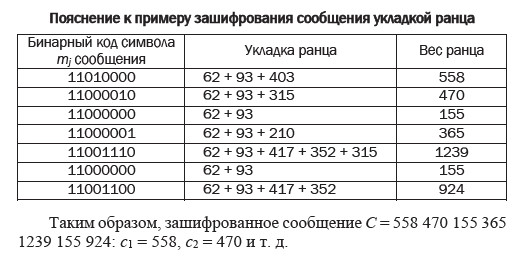


**Зашифрование соощения**

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*:

****

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***.



**Расшифрование соощения**

Для расшифрования сообщения получатель (используя свой тайный ключ ***d***: сверхвозрастающую последовательность) должен сначала определить такое обратное к *а* число *а***–**1, что:

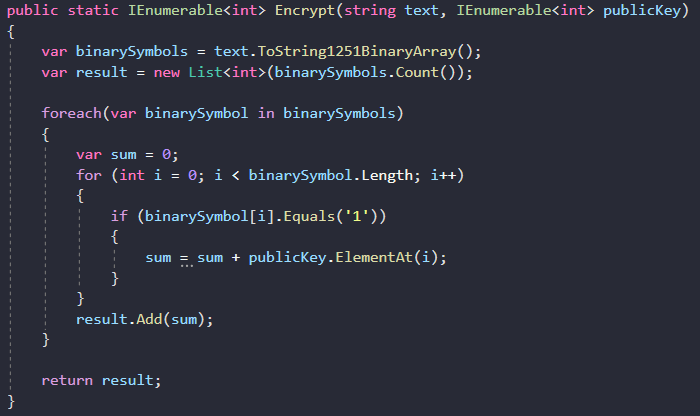


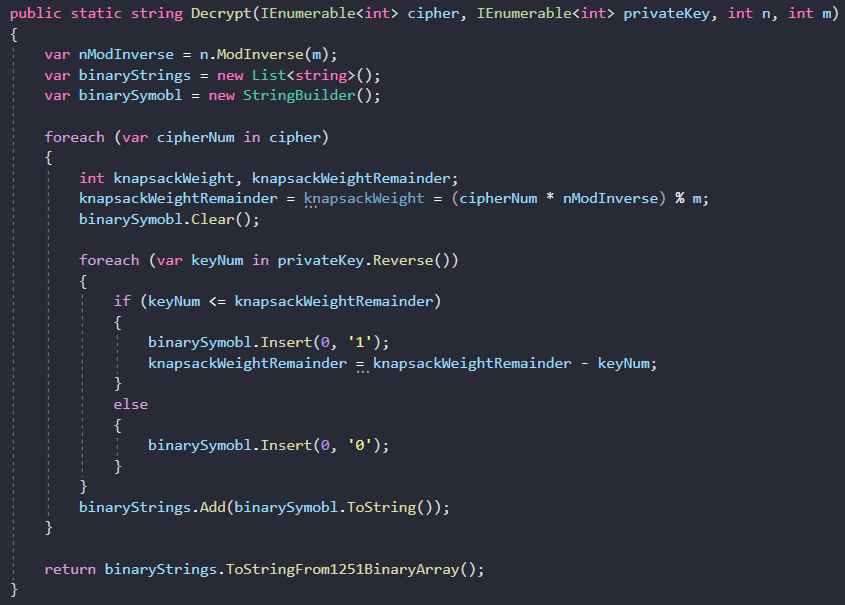
После определения обратного числа каждое значение шифрограммы (*ci*) преобразуется в соответствии со следующим соотношением:



**Практическая часть**

Код реализации алгоритма на языке C#:



****