

Практическая работа 10.
КВАНТОВОЕ ШИФРОВАНИЕ

1. Цель работы. Ознакомиться с теорией методов современной криптографии на примере программирования одного из предложенных алгоритмов. Программная реализация криптографических алгоритмов квантового шифрования.

Введение

Все предлагаемые сегодня криптосистемы с открытым ключом опираются на один из следующих типов односторонних преобразований.

1. Разложение больших чисел на простые множители (алгоритм RSA).
2. Вычисление дискретного логарифма или дискретное возведение в степень (алгоритм Диффи-Хеллмана-Меркле, схема Эль-Гамала).
3. Задача об укладке рюкзака (ранца) (авторы Хеллман и Меркл).
4. Вычисление корней алгебраических уравнений.
5. Использование конечных автоматов (автор Тао Ренжи).
6. Использование кодовых конструкций.
7. Использование свойств эллиптических кривых.

10.1. Основы квантовой физики

Квант (от лат. quantum - «сколько») - неделимая порция какой-либо величины в физике. В основе понятия лежит представление о том, что некоторые физические величины могут принимать только определенные (дискретные) значения, величина которых кратна некоторому минимальному значению (постоянной Планка). Постоянная Планка (квант действия) - коэффициент, связывающий величину энергии электромагнитного излучения с его частотой (или некоторую другую пару физических величин)
$$h = \frac{E}{\nu} = 6.62606957(29) \cdot 10^{-34}$$
, где E – энергия электромагнитного излучения, Дж; ν – частота электромагнитного излучения, 1/с.

На текущий момент большинство ученых считает, что на макроскопическом уровне (звезд, людей, молекул) действуют законы классической физики, а на микроскопическом (элементарных частиц – кварков, фотонов, электронов) – иные, в т.ч. и квантовой. В рамках квантовой физики любая элементарная частица рассматривается как квант возбуждения поля, характерной для этой частицы. Квантовые поля могут взаимодействовать между собой, в результате чего кванты (частицы) могут превращаться друг в друга.

Одной из элементарных частиц является фотон. Фотон (от др.-греч. φῶς - «свет») – квант электромагнитного излучения (электромагнитная волна) с нулевыми массой покоя и зарядом. Согласно современным представлениям фотону свойственен корпускулярно-волновой дуализм. С одной стороны, фотон демонстрирует свойства волны в явлениях дифракции¹ и интерференции² в том случае, если размеры препятствий сравнимы с длиной волны фотона. С другой стороны, процессы взаимодействия фотонов с веществом (излучение и поглощение) можно успешно истолковать только на основе представлений о нем, как о дискретной частице.

Излучение светящегося тела можно представить как потоки фотонов, направленных от него во все стороны.

Эти потоки распространяются, как правило, вдоль прямолинейного луча, за исключением прохода малых препятствий (см. дифракцию) или вблизи массивных тел (планет, звезд). Т.о. поток фотонов можно представить как набор электромагнитных волн, каждая из которых колеблется (поляризована) в одной плоскости.



Рис.7.1. Излучение светящегося тела

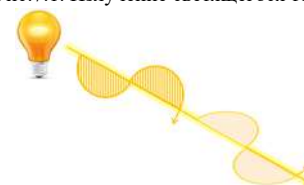


Рис.7.2. Поток из двух фотонов (электромагнитных волн)

¹ Дифракция (лат. diffractus - буквально разломанный, переломанный) – отклонение света (световых волн, фотонов) от прямолинейного распространения при прохождении сквозь малые отверстия или огибании малых препятствий.

² Интерференция света – перераспределение интенсивности света в результате наложения (суперпозиции) нескольких световых волн.

При пропускании оптического излучения через линейный поляризатор (например, призму Глана) на выходе можно получить поток фотонов с требуемой поляризацией. Образно этот процесс можно представить, как прохождение фотонов через фильтр с плоским отверстием, который проходит только часть фотонов – те, плоскость поляризации которых совпадает с ориентацией отверстия фильтра.

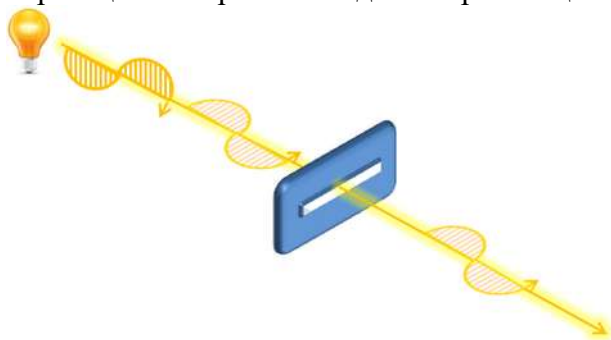


Рис.7.3. Прохождение потока фотонов сквозь фильтр

Если сгенерировать поток фотонов с требуемой поляризацией можно, то точно определить поляризацию произвольно перехваченных фотонов современные измерительные устройства не позволяют. Это обстоятельство и позволило использовать квантовую механику для шифрования информации.

Для кодирования информации, представленной в битовом виде, достаточно двух линейных поляризаторов с разными плоскостями поляризации. Фотоны, ориентированные в одной плоскости будут соответствовать «1», в другой – «0». На этом принципе основана работа передающего устройства (генератора фотонов).

Принимающее устройство может быть построено на базе линейного поляризатора или поляризационной разделительной призмы.

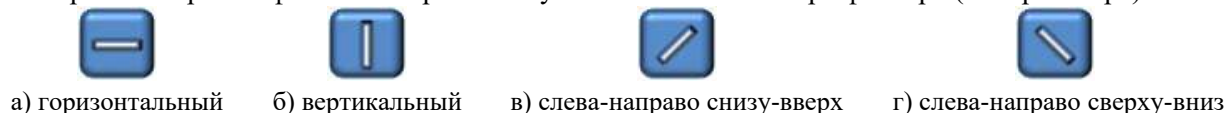
В первом случае, если принятый фотон проходит сквозь поляризатор и регистрируется стоящим за ним фотодетектором, то он идентифицируется как «1», в противном случае – как «0».

Во втором случае, при прохождении фотона через призму он перенаправляется на один из двух фотодетекторов, соответствующих двум взаимно перпендикулярным плоскостям поляризации (базису). Перенаправление выполняется на тот фотодетектор, чья плоскость поляризации наиболее близка к плоскости поляризации принятого фотона. Если передающая и принимающая стороны используют одинаковый базис поляризации (например, горизонтально-вертикальный), то принимающая сторона будет однозначно идентифицировать поступающие фотоны (например, с горизонтальной поляризацией как «1», с вертикальной - как «0»). Если принимающая сторона будет использовать другой базис поляризации, то вероятность правильной идентификации снижается. В частности, если у принимающей стороны базис будет повернут на 45° относительно передающей, то вероятность правильной идентификации будет примерно 50%.

10.2. Основы квантового шифрования

10.2.1. Шифрования с использованием линейных поляризаторов на принимающей стороне

Для отправки и приема фотонов стороны могут использовать четыре фильтра (поляризатора).



а) горизонтальный б) вертикальный в) слева-направо снизу-вверх г) слева-направо сверху-вниз

Рис.7.4. Фильтры для отправки и приема фотонов

















Если передающая и принимающая стороны для одного фотона (бита информации) будут использовать одинаковые фильтры, то он будет регистрироваться фотодетектором на принимающей стороне и идентифицироваться как «1», в противном случае – как «0».

Для обмена секретной информацией сторонам достаточно использовать два фильтра. При этом они заранее оговаривают порядок их использования на принимающей стороне, но он должен быть случайным для потенциального противника. Этот порядок будет являться ключом шифрования/дешифрования. Отправитель, зная последовательность применения фильтров получателем

(ключ), для отправки сообщения должен применить соответствующий фильтр, чтобы получатель правильно идентифицировал принятый фотон.

В следующей таблице приведен пример отправки сообщения «001101012» при использовании получателем горизонтального и вертикального фильтров.

Таблица 7.1. Пример отправки и приема сообщения

Посылаемое сообщение, бит	0	0	1	1	0	1	0	1
Фильтры, применяемые получателем (ключ)								
Фильтры, выбираемые отправителем								
Принятое сообщение, бит	0	0	1	1	0	1	0	1

Т.к. противник не знает порядок использования фильтров, то он не может правильно интерпретировать перехваченные фотоны.

В целях обеспечения стойкости данной схемы шифрования ключ, как и в шифрах гаммирования, должен быть истинно случайным и одноразовым. Для генерации таких ключей можно использовать генераторы гамм. Например, если в гамме очередной бит равен «1», то получатель должен использовать горизонтальный фильтр, иначе – вертикальный. Для генерации ключа (гаммы) можно использовать квантовые протоколы обмена ключами (например, протокол BB84).

Для повышения стойкости шифра рекомендуется менять пары фильтров на стороне получателя. Это позволит также определить факт прослушивания канала связи. При перехвате фотона противник вынужден создать его копию (клон) и послать ее законному получателю. Если противник будет использовать не ту пару фильтров или разделительную призму, то поляризацию части фотонов он не сможет правильно определить, а значит и создать требуемые копии. Для проверки перехвата сообщения отправитель и получатель могут вычислить хеш-образы (контрольные суммы), соответственно, посланного и принятого сообщений. Сравнив хеш-образы, которые можно передавать по открытому каналу не защищая, они могут сделать вывод о прослушивания канала связи или о корректности передачи (целостности) данных.




10.2.2. Шифрования с использованием поляризационной разделительной призмы на принимающей стороне

Для передачи секретной информации передающая и принимающая стороны используют два базиса поляризации: прямолинейный и диагональный. При этом порядок чередования базисов для отдельных фотонов (битов информации), как и в предыдущей схеме, должен быть известен сторонам и случайным для потенциального противника. Этот порядок представляет собой ключ шифрования/дешифрования, для формирования которого можно использовать генераторы гамм или протокол BB84. При этом, если в гамме очередной бит равен «1», то стороны должны использовать прямолинейный базис, иначе – диагональный.

Для отправки фотонов передающая сторона применяет четыре фильтра

Таблица 7.2. Фильтры для отправки фотонов

Базис	Тип фильтра	Значение бита
<div> <div>прямолинейный</div>  </div>	горизонтальный 	0
	вертикальный 	1
диагональный	слева-направо снизу-вверх	0

		
	слева-направо сверху-вниз	1
		

Тип фильтра для передачи отдельного фотона выбирается в зависимости от определенного сторонами порядка использования базисов. Аналогичным образом поступает и принимающая сторона – применяет базис поляризации в зависимости от ключа.

Таблица 7.3. Пример отправки и приема сообщения

Посылаемое сообщение, бит	0	0	1	1	0	1	0	1
Базисы, применяемые получателем (ключ)								
Фильтры, выбираемые отправителем								
Принятое сообщение, бит	0	0	1	1	0	1	0	1

Противник, перехватив фотон, не может со стопроцентной уверенностью определить его поляризацию: действительно он угадал применяемый базис (\approx идентифицировал отправленный бит) или это был базис, расположенный под углом 45° к применяемому? В последнем случае вероятность правильной идентификации бита равна 50%.

Это обстоятельство позволяет также определить факт прослушивания канала связи. При перехвате фотона противник вынужден создать его копию (клон) и послать ее законному получателю. Определив значение бита для перехваченного фотона, у него будет два равновероятных варианта поляризации для копии, соответствующие двум разным базисам. Для проверки перехвата сообщения передающая и принимающая стороны могут вычислить хеш-образы (контрольные суммы), соответственно, посланного и принятого сообщений и сравнить их.

Вопросы для самопроверки

1. Дайте определение понятиям «квант» и «фотон».
2. В чем заключается природа корпускулярно-волнового дуализма фотона?
3. В чем суть шифрования с помощью фотонов?

3. Практическое задание

3.1Р. Используя описанную идею квантового шифрования, составить программу на языке программирования для шифрования и дешифрования текстов.

3.1Е. Реализация шифрования в Microsoft Excel формулами.

Лабораторная работа № 10
Волновой метод криптографии

1. ЦЕЛИ РАБОТЫ: Ознакомиться с теорией методов современной криптографии на примере программирования одного из предложенных алгоритмов.

2. ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

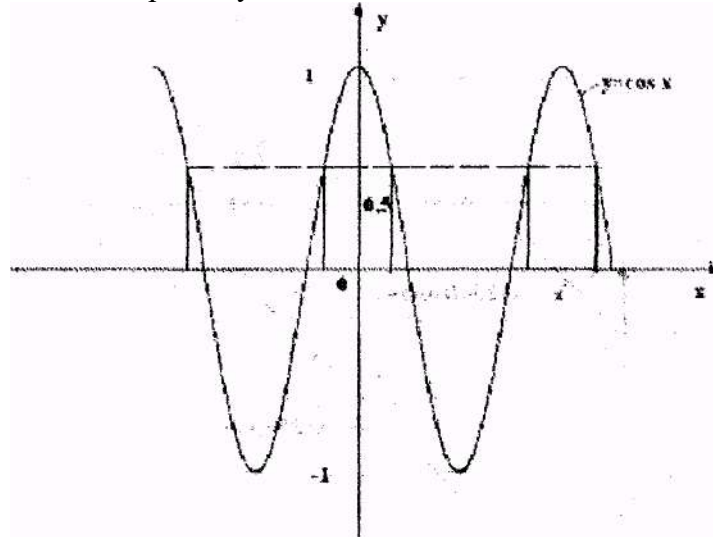
2.1. Волновой метод криптографии

Поставленная цель достигается тем, что изменяем стандартный способ шифрования на новый. Схема представлена ниже. Путем использования периодических функций типа $y = \cos(x)$ и уравнения «волны» типа $y = \cos(x+dx)$.

Предложенная совокупность признаков обладает новизной и существенными отличиями. Впервые для защиты информации используется периодическая функция и уравнение волны. В отличие от прототипа объем исходного текста равен объему шифровки.

На криптостойкость также не влияет объем исходного текста и его содержание (он может состоять из одной буквы). Также на криптостойкость не влияет знание алгоритма зашифрования, так как нельзя имея на руках исходный текст и шифровку поставить перед машинными средствами задачу по расшифрованию. Сущность способа пояснена ниже :

Существует огромное количество периодических функций, имеющих постоянную амплитуду, которые определены и непрерывны на всем промежутке



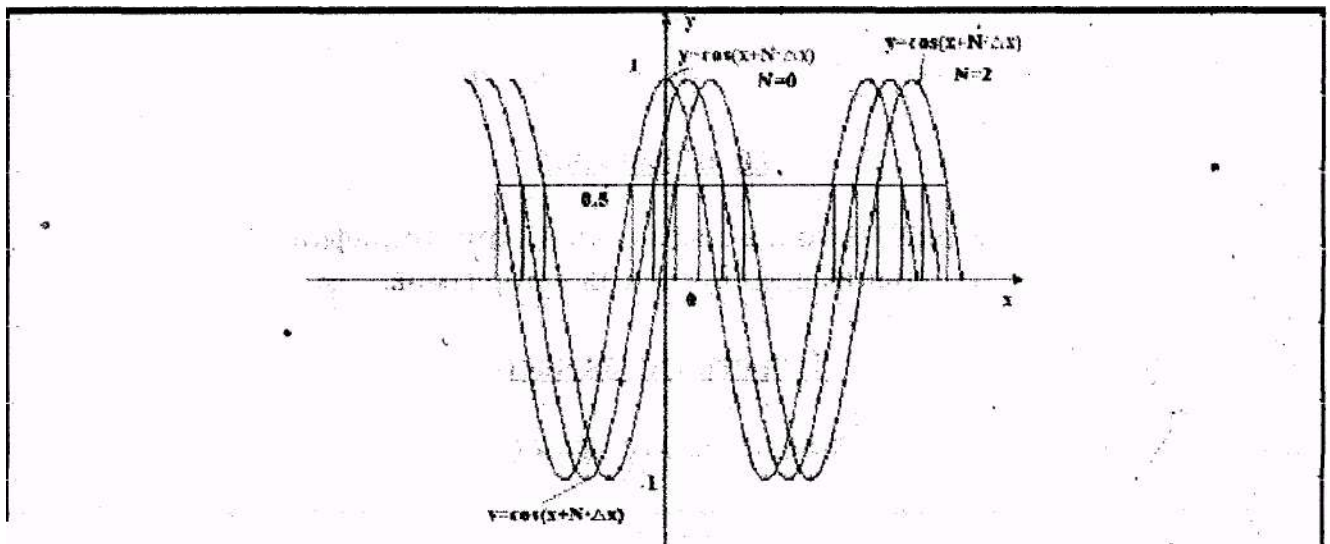
x (“-” бесконечность; “+” бесконечность).

На графике представлена функция $y = \cos(x)$. Особенность периодической функции в том, что, к максимальному значению $y = 0,5$ соответствует бесконечное количество значений x .

Применяя уравнение волны $y = \cos(x + N \cdot dx)$, где N - любое целое число, а $dx \rightarrow 0$, получаем, что при

$N \cdot i$

$y = 0,5x$ может принимать любые значения от



”-”бесконечности до ”+”бесконечности.

Предложенный способ осуществляется следующим образом. Создается компьютерная программа. По оси x расставляют и номеруют те символы, которые нужно зашифровать, а по оси y те, которые будут использованы в шифровке. Зашифрование идет по линейной функции $y=x$, которая перемещается по осям координат. Перемещение линейной функции $y=x$ происходит по уравнению волны.

Пример реализации способа:

По координатным осям X и Y расставляются компьютерные символы в любом порядке. Всего используется в компьютере 256 символов. Они все расставляются по оси X в любом порядке, по оси Y расставляем те же самые символы в любом порядке. Три линейные функции 1,2,3 описываются как: Y_1 , Y_2 , Y_3 ,

$$Y_1 = X + 256 * [\cos(z + N * dx)] + 256$$

$$Y_2 = X + 256 * [\cos(z + N * dx)]$$

$$Y_3 = -X + 256 * [\cos(z + N * dx)] - 256$$

Где: X - тот байт (знак), который нужно зашифровать;

Z - любое число.

N - номер по счету шифруемого знака в исходном тексте;

dx - любое число.

Для примера зашифруем исходный текст состоящий из пяти букв А.

АААА А - исходный текст.

Для примера порядок расстановки знаков по осям X и Y одинаковый. Например, знак А занимает промежуток (0-1) по оси X , знак Б-(1-2); В-(2-3)...Я-(255-256). То же самое по оси Y , Имея три формулы, подставляем значение 0,5 - середину промежутка (0-1) - буква А.

Пусть: $Z = 0$ (для удобства);

$N = 1$ (т.к. шифруется первый по счету знак из исходного текста, потом 2,3,4,5);

$dx = 32$.

Подставляем эти цифры в формулу

$$Y_1 = 0,5 + 256 * [\cos(z + 1 * 32)] + 256 = 437,6$$

$$Y_2 = 0,5 + 256 * [\cos(z + 1 * 32)] = 217,6$$

$$Y_3 = 0,5 + 256 * [\cos(z + 1 * 32)] - 256 = -38,39$$

Из трех значений Y_1 , Y_2 , Y_3 выбираем Y_2 , так как оно попало в промежуток от 0 до 256 и округляем значение Y_2 до большего целого $Y_2 = 218$.

Шифруем второй знак исходного текста:

$$Y_1 = 0,5 + 256 * [\cos(Z + 2 * 32)] + 256 = 368,7$$

$$Y_2 = 0,5 + 256 * [\cos(Z + 2 * 32)] = 112,7$$

$$Y_3 = 0,5 + 256 * [\cos(Z + 2 * 32)] - 256 = -143,28$$

В шифровку, соответственно, записываем $Y_2 = 113$.

Соответственно получаем третий, четвертый и пятый знаки шифровки:

Третий знак - 230

Четвертый знак- 99

Пятый знак- 16

В итоге из числового ряда 0,5; 0,5; 0,5; 0,5; 0,5 - исходный текст А А А А А получили числовой ряд 218; 113; 230; 99; 16 -шифровка.

Для расшифровки применяют те же самые формулы.

$$X1 = Y - 256 * [\cos(z + N * dx)] - 256$$

$$X2 = Y - 256 * [\cos(z + N * dx)]$$

$$X3 = Y - 256 * [\cos(z + N * dx)] + 256$$

Подставляя уже известные значения получаем:

$$X1 = 217,5 - 256 * [\cos(0 + 1 * 32)] - 256 = -255,6$$

$$X2 = 217,5 - 256 * [\cos(0 + 1 * 32)] = 0,4$$

$$X3 = 217,5 - 256 * [\cos(0 + 1 * 32)] + 256 = 265,4$$

$$X = 0,4$$

Подставляя следующие значения получаем остальные значения: 0,3; 0,7; 0,6; 0,56; все эти значения попали в промежуток (0-1), соответственно получили текст

А А А А А.

В данном частном случае использовалась всего одна переменная dx , а их можно использовать неограниченное количество. Кроме того, исходный текст можно зашифровать не один раз, а несколько. Теоретически возможно зашифровать стихи Пушкина стихами Лермонтова или наоборот.

3. Практическое задание

3.1Р. Используя описанную идею волнового шифрования, составить программу на языке программирования для шифрования и дешифрования текстов.

3.1Е. Реализация шифрования в Microsoft Excel формулами.

Лабораторная работа № 10

Алгоритм на основе задачи об укладке рюкзака (Knapsack Cryptosystem)

1. Цель работы. Криптоанализ и программная реализация криптографических алгоритмов шифрования на основе задачи об укладке рюкзака для шифрования и дешифрования исходного текста.

2. Краткие теоретические сведения о методе шифровании

В 1978 г. Меркл и Хеллман предложили использовать задачу об укладке ранца (рюкзака) для асимметричного шифрования [1]. 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 M_1, M_2, \dots, M_n и суммарное значение S ; требуется вычислить значения b_i такие что

$$S = b_1M_1 + b_2M_2 + \dots + b_nM_n, \quad (1.1)$$

где n – количество предметов;

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

Например, веса предметов имеют значения 1, 5, 6, 11, 14, 20, 32 и 43. При этом можно упаковать рюкзак так, чтобы его вес стал равен 22, использовав предметы весом 5, 6 и 11. Невозможно упаковать рюкзак так, чтобы его вес стал равен 24.

В основе алгоритма, предложенного Мерклом и Хеллманом, лежит идея шифрования сообщения на основе решения серии задач укладки рюкзака. 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 , а текст является полученным суммарным весом. Пример шифрограммы, полученной с помощью задачи об укладке рюкзака, показан в следующей таблице.

Таблица 1.1. Пример шифрования на основе задачи об укладке ранца

Открытый текст	1	1	1	0	0	1	0	0	0	1	0	1	1	0	0	1	0	0	0	0	0	0	0	0
Рюкзак (ключ)	1	5	6	11	14	20	32	43	1	5	6	11	14	20	32	43	1	5	6	11	14	20	32	43
Шифрограмма	32 (1+5+6+20)								73 (5+11+14+43)								0							

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. Например, последовательность {2, 3, 6, 13, 27, 52, 105, 210} является сверхвозрастающей, а {1, 3, 4, 9, 15, 25, 48, 76} - нет.

Решение для сверхвозрастающего ранца найти легко. В качестве текущего выбирается полный вес, который надо получить, и сравнивается с весом самого тяжелого предмета в ранце. Если текущий вес меньше веса данного предмета, то его в рюкзак не кладут, в противном случае его укладывают в рюкзак. Уменьшают текущий вес на вес положенного предмета и переходят к следующему по весу предмету в последовательности. Шаги повторяются до тех пор, пока процесс не закончится. Если текущий вес уменьшится до нуля, то решение найдено. В противном случае, нет.

Например, пусть полный вес рюкзака равен 270, а последовательность весов предметов равна {2, 3, 6, 13, 27, 52, 105, 210}. Самый большой вес – 210. Он меньше 270, поэтому предмет весом 210 кладут в рюкзак. Вычитают 210 из 270 и получают 60. Следующий наибольший вес последовательности равен 105. Он больше 60, поэтому предмет весом 105 в рюкзак не кладут. Следующий самый тяжелый предмет имеет вес 52. Он меньше 60, поэтому предмет весом 52 также кладут в рюкзак. Аналогично проходят процедуру укладки в рюкзак предметы весом 6 и 2. В результате полный вес уменьшится до 0. Если бы

этот рюкзак был бы использован для дешифрования, то открытый текст, полученный из значения шифртекста 270, был бы равен 10100101.

Открытый ключ представляет собой не сверхвозрастающую (нормальную) последовательность. Он формируется на основе закрытого ключа и, как принято считать, не позволяет легко решить задачу об укладке ранца. Для его получения все значения закрытого ключа умножаются на число n по модулю m . Значение модуля m должно быть больше суммы всех чисел последовательности, например, 420 ($2+3+6+13+27+52+105+210=418$). Множитель n должен быть взаимно простым числом с модулем m , например, 31. Результат построения нормальной последовательности (открытого ключа) представлен в следующей таблице.

Таблица 1.2. Пример получения открытого ключа

Закрытый ключ, k_i	2	3	6	13	27	52	105	210
Открытый ключ, $(k_i \cdot n) \bmod m = (k_i \cdot 31) \bmod 420$	62	93	186	403	417	352	315	210

Для шифрования сообщение сначала разбивается на блоки, по размерам равные числу элементов последовательности в рюкзаке. Затем, считая, что единица указывает на присутствие элемента последовательности в рюкзаке, а ноль – на его отсутствие, вычисляются полные веса рюкзаков – по одному рюкзаку для каждого блока сообщения.

В качестве примера возьмем открытое сообщение «АБРАМОВ», символы которого представим в бинарном виде в соответствии с таблицей кодов символов Windows 1251. Результат шифрования с помощью открытого ключа {62, 93, 186, 403, 417, 352, 315, 210} представлен в следующей таблице.

Таблица 1.3. Пример шифрования

Открытое сообщение		Сумма весов	Шифрограмма (рюкзак), s_i
Символ	Bin-код		
А	1100 0000	62+93	155
Б	1100 0001	62+93+210	365
Р	1101 0000	62+93+403	558
А	1100 0000	62+93	155
М	1100 1100	62+93+417+352	924
О	1100 1110	62+93+417+352+315	1239
В	1100 0010	62+93+315	470

В качестве другого примера возьмем открытое сообщение «НИКИФОРОВА», символы которого представим в бинарном виде в соответствии с таблицей кодов символов Windows 1251. Результат шифрования с помощью открытого ключа {62, 93, 186, 403, 417, 352, 315, 210} представлен в следующей таблице.

Таблица 1.4. Пример шифрования

Открытое сообщение		Сумма весов	Шифрограмма (рюкзак), s_i
Символ	Bin-код		
Н	1100 1101	$62 + 93 + 417 + 352 + 210 =$	1134
И	1100 1000	$62 + 93 + 417 =$	572
К	1100 1010	$62 + 93 + 417 + 315 =$	887
И	1100 1000	$62 + 93 + 417 =$	572
Ф	1101 0101	$62 + 93 + 403 + 352 + 210$	1120
О	1100 1110	$62+93+417+352+315$	1239
Р	1101 0000	$62+93+403$	558
О	1100 1110	$62+93+417+352+315$	1239
В	1100 0010	$62+93+315$	470
А	1100 0000	$62+93$	155

Для расшифрования сообщения получатель должен сначала определить *обратное* число n^{-1} , такое что $(n \cdot n^{-1}) \bmod m = 1$. После определения обратного числа каждое значение шифрограммы умножается на n^{-1} по модулю m и с помощью закрытого ключа определяются биты открытого текста.

В нашем примере сверхвозрастающая последовательность равна {2, 3, 6, 13, 27, 52, 105, 210}, где $m = 420$, $n = 31$. Значение n^{-1} равно 271 (т.к. $31 \cdot 271 \bmod 420 = 1$).

Таблица 1.5. Пример расшифрования

Шифрограмма (рюкзак), c_i	$(c_i \cdot n^{-1}) \bmod m = (c_i \cdot 271) \bmod 420$	Сумма весов	Открытое сообщение	
			Символ	Bin-код
155	5	2+3	1100 0000	А
365	215	2+3+210	1100 0001	Б
558	18	2+3+13	1101 0000	Р
155	5	2+3	1100 0000	А
924	84	2+3+27+52	1100 1100	М
1239	189	2+3+27+52+105	1100 1110	О
470	110	2+3+105	1100 0010	В

В нашем втором примере сверхвозрастающая последовательность равна $\{2, 3, 6, 13, 27, 52, 105, 210\}$, где $m = 420$, $n = 31$. Значение n^{-1} равно 271 (т.к. $31 \cdot 271 \bmod 420 = 1$). **Самостоятельно получите таблицу расшифрования.**

В своей работе авторы рекомендовали брать длину ключа, равную 100 (количество элементов последовательности). В заключении следует отметить, что задача вскрытия данного способа шифрования успешно решена Шамиром и Циппелом в 1982 г.

Итак, **Задача об укладке ранца** формулируется следующим образом. Задан вектор $C = |c_1, c_2, \dots, c_n|$, который используется для шифрования сообщения, каждый символ s_i которого представлен последовательностью из n бит $s_i = |x_1, x_2, \dots, x_n|$, где $x_k \in \{0, 1\}$.

Шифртекст получается как скалярное произведение $C \otimes s_i$.

Пример. Открытый текст: "ПРИКАЗ" ("16 17 09 11 01 08").

Вектор $C = \{1, 3, 5, 7, 11\}$.

Запишем код каждой буквы открытого текста в двоичном виде, используя пять разрядов.

П	Р	И	К	А	З
10000	10001	01001	01011	00001	01000

Произведем соответствующие операции:

$$y_1 = 1 \otimes 1 + 0 \otimes 3 + 0 \otimes 5 + 0 \otimes 7 + 0 \otimes 11 = 1$$

$$y_2 = 1 \cdot 1 + 1 \cdot 11 = 12$$

$$y_3 = 1 \otimes 3 + 1 \otimes 11 = 14$$

$$y_4 = 1 \cdot 3 + 1 \cdot 7 + 1 \cdot 11 = 21$$

$$y_5 = 1 \otimes 11 = 11$$

$$y_6 = 1 \cdot 3 = 3.$$

Шифртекст: "01 12 14 21 11 03".

3. Практическое задание

3.1Р. Используя описанную идею шифрования криптосистемы Меркля-Хеллмана, составить программу на языке программирования для шифрования и дешифрования текстов.

Криптосистема Меркля-Хеллман в качестве секретного ключа выбирает задачу о рюкзаке с прогрессивно возрастающей последовательностью весов и по ней (используя секретное преобразование) формулирует «сложную» задачу о рюкзаке – открытый ключ. Секретно преобразование опирается на скрываемые взаимно простые натуральные числа n и m . Он заключается в умножении все весов прогрессии в возрастающей последовательности на $n \pmod{m}$.

Пусть, например, секретный ключ состоит из последовательности $\{2, 3, 6, 13, 27, 52\}$, где $n = 31$ и $m = 105$. Соответствующий открытый ключ — «сложная» задача о рюкзаке с весами $\{62, 93, 81, 88, 102, 37\}$.

Считается, что только знающий числа n и m способен трансформировать «сложную» задачу о рюкзаке в простую.

Чтобы зашифровать сообщение, Боб разбивает открытый текст на блоки, размер которых совпадает с числом весов в задаче, и складывает те веса, у которых соответствующие биты в блоке равны 1.

Пусть, например, открытый текст имеет вид: СООБЩЕНИЕ = 011000 110101 101110.

Первый блок сообщения – 011000 говорит о том, что нужно сложить второй и третий веса. При этом получится $93 + 81 = 174$ — первое число шифротекста. Второй блок, 110101, диктует сложить веса с номерами 1, 2, 4 и 6: $62 + 93 + 88 + 37 = 280$. Наконец, сумма, соответствующая последнему блоку, равна $62 + 81 + 88 + 102 = 333$. Таким образом, Боб получает шифротекст: 174, 280, 333.

Законный пользователь осведомлен о секретном ключе n, m последовательность $\{2, 3, 6, 13, 27, 52\}$. Поэтому, умножая каждый блок шифротекста на $n^{-1} \pmod{m}$, сводит сложную задачу рюкзака к простой. В нашем примере $n^{-1} = 61 \pmod{m}$, получаем

$$174 \cdot 61 = 9 = 3 + 6 = 011000,$$

$$280 \cdot 61 = 70 = 2 + 3 + 13 + 52 = 110101,$$

$$333 \cdot 61 = 48 = 2 + 6 + 13 + 27 = 101110.$$

Процесс расшифровывания опирается на простую задачу о рюкзаке с весами $\{2, 3, 6, 13, 27, 52\}$ и приведенный выше алгоритм ее решения.

При оформлении отчета необходимо привести исходное сообщение (фамилию) и таблицы генерации ключей, шифрования и расшифрования. Код символа определяется в соответствии с кодировкой Windows 1251 (табл.1.6).

Таблица 1.6. Коды символов Windows 1251 и их двоичное представление

Буква	Дес-код	Bin-код	Буква	Дес-код	Bin-код	Буква	Дес-код	Bin-код
А	192	1100 0000	Л	203	1100 1011	Ц	214	1101 0110
Б	193	1100 0001	М	204	1100 1100	Ч	215	1101 0111
В	194	1100 0010	Н	205	1100 1101	Ш	216	1101 1000
Г	195	1100 0011	О	206	1100 1110	Щ	217	1101 1001
Д	196	1100 0100	П	207	1100 1111	Ъ	218	1101 1010
Е	197	1100 0101	Р	208	1101 0000	Ы	219	1101 1011
Ж	198	1100 0110	С	209	1101 0001	Ь	220	1101 1100
З	199	1100 0111	Т	210	1101 0010	Э	221	1101 1101
И	200	1100 1000	У	211	1101 0011	Ю	222	1101 1110
Й	201	1100 1001	Ф	212	1101 0100	Я	223	1101 1111
К	202	1100 1010	Х	213	1101 0101			

Примечание. Дес-код – десятичный код символа, Bin-код – двоичный код символа.

3.1Е. Реализация шифрования в Microsoft Excel формулами.

3.2Р. Для самостоятельной работы студентов можно предложить программную реализацию криптографической системы с открытым ключом, которая использует задачу о рюкзаке. Программную реализацию можно разбить на несколько самостоятельных задач. А именно:

- формирование быстровозрастающего вектора (последовательности) В;
- формирование параметров криптографической системы на основе быстровозрастающего вектора В;
- выбор модуля m ;
- определение множителя t для вычисления маскирующего вектора В;
- вычисление обратного значения (t^{-1}) для значения маскирующего множителя t ;
- вычисления маскирующего вектора В;
- преобразование исходного текста в бинарную последовательность;
- шифровка исходного текста;
- расшифровка исходного текста.

4. Содержание отчета:

название и цель лабораторной работы;
описание алгоритма и блок-схемы программы;
результаты выполнения программы: исходный, зашифрованный и дешифрованный тексты;
расчеты статистических характеристик;
выводы, отражающие достоинства и недостатки исследуемых алгоритмов.

5. Контрольные вопросы

1. В чем заключается суть и основная предпосылка появления шифрования с открытым ключом?
2. Основные требования, предъявляемые к криптосистемам с открытым ключом.
3. Перечислите типы односторонних преобразований, применяемых при асимметричном шифровании.
4. Дайте краткую характеристику алгоритма шифрования на основе задачи укладки ранца.
5. В чем отличие сверхвозрастающей последовательности от обыкновенной?
6. Что означает обратное число по модулю?

6. Литература

1. Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Б. Шнайер – М.: ТРИУМФ, 2002. – 816 с.