СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Уважаемые старшеклассники!

Вам предлагается комплект практических работ в двух частях по темам, составляющим основу предпрофессиональной подготовки обучающихся по предметам информационно-технологического цикла.

Тематика работ ориентирована на такие рекомендуемые для инженерных классов направления, как:

- моделирование, прототипирование, прикладная математика;
- робототехника и микроэлектроника;
- информационные технологии (ИТ);
- прикладные технологии и социальный инжиниринг.

Практические работы рассчитаны на изучение определённых тем непосредственно в ходе выполнения работ, отработку необходимых навыков работы в используемой программной среде и/или получение прототипа изделия. При этом сформируется необходимый опыт проектной или исследовательской работы, поскольку тематика работ предполагает её возможное расширение в индивидуальный или групповой проект либо учебное исследование.

Темы практических работ охватывают значимый круг интересов инженерной и ИТ-сфер, используется современный контекст, доступные оборудование и программное обеспечение (ПО). Дополнительно совершенствуется умение программировать на Python или PascalABC.NET. В проектах вы познакомитесь с возможностями Си-подобных языков программирования и языком Java.

Практикум рассчитан на нулевой начальный уровень подготовки по теме. Вся минимально необходимая теория и задания даны в практических работах. Отдельное рассмотрение теоретических вопросов не требуется. Если практикум используется в классе, то необходима первичная постановка задачи (проблемы) в режиме коллективного обсуждения («мозгового штурма»). Продолжение и защита работы могут быть групповыми или индивидуальными (по желанию исполнителей).

Все практические работы были апробированы в образовательных организациях Москвы и Московской области практикующими учителями информатики и студентами МПГУ в ходе мероприятий «Университетская среда» и на педагогической практике в течение трёх лет.

Практикум состоит из двух частей.

Часть 1 включает три темы.

1. Использование основ криптографии при решении задач обеспечения информационной безопасности. Технология блокчейн.

Данная тематика интегрирует вопросы прикладной математики, информационных технологий и пропедевтику вопросов социального инжиниринга.

Вопросы математических основ шифрования логически продолжают тему *кодирования*, изучаемую в курсе информатики. Прикладное использование

основных алгоритмов шифрования для обеспечения защиты информации поддерживает актуальную тему информационной безопасности при работе в компьютерных сетях. Именно сюда включены такие вопросы, как: подбор паролей, хеш-функции, закрытые каналы связи при использовании асимметричных ключей, понятия «блокчейн» и «криптосистема». В итоге можно выполнить проектное задание.

2. Основы микроэлектроники и робототехники.

Здесь продолжается тема *устройства компьютера* и собираются его компоненты. Эта часть содержит два блока материалов: 1) сборка основных компонентов сумматора, устройств памяти — триггеров (всего три работы); 2) проект с использованием микроконтроллера для изготовления бытовых приборов как элементов «умного» дома. Предлагается также проектное задание «Новогодняя гирлянда».

3. Разработка мобильного приложения «Помощник инженера» для Android.

По этой теме предлагается самая сложная проектная работа. Проделав её, можно освоить основы разработки мобильных приложений под Android в интегрированной среде Android Studio. Предлагается разработать приложение, использующее камеру смартфона или планшета в качестве сканера штрихкодов, анализирующее зашифрованную в них информацию и получающее сведения о предмете из облачной базы данных, которую также нужно создать и подключить самим.

Часть 2. Моделирование и прототипирование.

В этой части фактически интегрируются все перечисленные выше направления, реализуемые в инженерных классах.

Тема представлена двумя различными приложениями — системой автоматизированного проектирования (САПР) Autodesk Fusion 360 и средой моделирования динамических систем и производственных процессов AnyLogic.

Образцы трёхмерных моделей предполагают их печать с использованием наиболее распространённых трёхмерных (3D) принтеров (дан обзор двух видов). В работе рассматриваются наиболее важные аспекты подготовки модели к печати на 3D-принтере.

Для исследовательских целей в самых разных областях деятельности, прогнозирования последствий и принятия управленческих решений, оптимизации производственных процессов используется имитационное моделирование. Вам предлагается практическая работа в AnyLogic на изучение процессов автоматизации склада.

Желаем успехов!

Использование основ криптографии при решении задач обеспечения информационной безопасности. Технология блокчейн

Данный раздел посвящён основам криптографии, некоторым популярным шифрам и алгоритмам шифрования и их использованию при решении типовых задач обеспечения информационной безопасности. Проблема информационной безопасности актуальна для каждого современного человека и общества в целом. Мы все используем пароли, чтобы обеспечить сохранность личной информации (*хеш-функции*), развивается электронный бизнес (*алгоритм RSA для цифровой подписи документов*), появились криптовалюты и новые сервисы, связанные с ними (*блокчейн и пр.*).

В курсе информатики вопросы информационной безопасности немного затрагиваются при изучении тем «Кодирование» и «Компьютерные сети», в которой рассматриваются вопросы защиты информации на разных уровнях сетевого взаимодействия. Сегодня можно говорить о том, что вопросы информационной безопасности связаны с возможностями разработки программ в современных средах программирования. Программирование является средством реализации мер по обеспечению защиты информации.

В продолжении темы кодирования (возможно для основной школы) предлагаем вам познакомиться с интересной темой «Шифрование». Вначале отметим отличия этих понятий. При **кодировании** происходит преобразование сообщений из исходных в кодированные. При этом подразумевается, что существует однозначное соответствие исходного сообщения кодированному. **Шифрование** — изменение исходного текста, которое позволяет скрыть от прочих его содержание. Шифрование часто выполняется с помощью ключа — таких данных, которые используются при шифровании и позволяют выполнить обратное действие. Без ключа получение исходных данных (или повторное шифрование) становится гораздо более трудоёмким.

Комплект из алгоритма шифрования, алгоритма расшифровки (если он существует) и необходимых для их работы данных (например, таблиц) называют **шифром.**

Стоит заметить, что получение исходных данных «в обход» процедуры всё равно остаётся возможным. Поэтому, когда речь идёт о защите данных, вводят понятие **стойкости шифра**. Стойкость шифра оценивается как минимальное время, требуемое на получение расшифрованного сообщения. Для всех современных систем шифрования такой подбор возможен, поэтому не бывает абсолютно стойких систем и ключей. Когда говорят о надёжной защите, на самом деле речь идёт о достаточности мер защиты для имеющихся задач.

Классифицировать шифры можно по разным основаниям.

1. По общему принципу обработки: **поточные** и **блочные**. Поточные методы выполняют шифрование побайтно (или побитно), используя только уже полученные данные. Эти методы позволяют шифровать данные при передаче по каналам связи. Полученные данные сразу можно расшифровывать. Блочные шифруют данные блоками **заданной длины**, выполняя преобразо-

вания с каждым блоком в отдельности. Для расшифровки нужно получить блок целиком.

2. По существованию дешифрующего преобразования: **обратимое** — преобразование, для которого существует обратное преобразование (дешифрующее), и **необратимое** — такое, для которого такого преобразования не существует[1].
3. По используемым ключам: **симметричные** и **асимметричные**. Симметричные методы шифрования используют один и тот же ключ и для шифрования, и для расшифровки сообщений. Асимметричные — два разных (хотя обычно связанных) ключа.

   Исторически первыми использовались симметричные системы шифрования — те, в которых использовался один и тот же ключ для шифрования и расширофровки. Ключ должны были знать только доверенные лица. Потеря ключа означала и компрометацию канала. Чтобы затруднить вычисление ключа, их использовали целыми наборами, например в виде шифроблокнота.

Канал связи, сообщения в котором шифруются и таким образом защищаются от перехвата и подмены, часто называют *защищённым*, или *закрытым* каналом.

В современных системах для организации защищённого канала связь начинают, как правило, с выполнения специальной процедуры согласования метода шифрования и сеансового ключа, т. е. общего для двух абонентов ключа шифрования, который будет применяться ими в течение сеанса. Такая схема препятствует краже ключа и затрудняет его дешифровку, поскольку сокращается объём данных для анализа и время использования этого ключа. Предполагаемая выгода от дешифровки ключа оказывается меньше, чем затраты ресурсов на его подбор.

Возникает вопрос — если ключ согласовывается фактически при обращении, то как всё-таки понять, кто на другом конце канала связи, особенно если это совершенно неизвестный абонент.

Системы шифрования с закрытым ключом позволяют организовать быстрые и надежно защищённые каналы связи, сравнительно дешёвые в реализации. Мы рассмотрим самые простые шифры и алгоритмы шифрования.

В данном разделе предлагаются три практические работы по следующим темам.

1. Простые методы шифрования.
2. Алгоритм RSA.
3. Хеш-функции и блокчейн.

Вначале тема разбирается на примерах, далее предлагаются задания для самостоятельного выполнения и проектные задания. Все предлагаемые способы решения и алгоритмы реализованы в среде программирования PascalABC.NET и на языке Python.

---

[1] Чаще всего это означает, что исходное преобразование в нескольких разных случаях приводит к одному результату. Необходимое условие состоит в том, что алгоритм обратного преобразования если и существует, то требует непомерно большого количества вычислений.

Практическая работа № 1
Простые методы шифрования

Цель работы: изучить шифры Цезаря, Гронсфельда, аффинную систему шифрования и научиться их использовать.

Шифр Цезаря

Для шифрования открытого текста каждую букву послания необходимо заменить на букву того же алфавита путём сдвига по алфавиту от исходной буквы на k букв. Цезарь использовал $k = 3$. При достижении конца алфавита выполняется циклический переход к его началу.

Предположим, что используется N-буквенный алфавит с числовыми эквивалентами букв — $\{0, 1, \ldots, N - 1\}$. Тогда каждая буква шифртекста (текста, полученного после шифрования) будет найдена по правилу:

$$C = f(p) = p + k,$$

где:
- C — буква шифртекста;
- p — буква открытого текста;
- k — целое число, являющееся ключом шифрования.

Пример 1. Зашифруем букву «в» шифром Цезаря с ключом шифрования 4.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п

17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я

$$C = f(2) = 2 + 4 = 6 \rightarrow \text{ё}.$$

Можно заметить, что при шифровании букв с большим порядковым номером легко выйти за пределы алфавита. Допустим, зашифруем букву «ю» с ключом из предыдущего примера:

$$C = f(31) = 31 + 4 = 35 \rightarrow ?$$

Имея под рукой таблицу, можно циклически перейти к её началу. Но лучше всего использовать операцию mod, которая находит остаток от целочисленного деления.

Чтобы найти номер буквы в алфавите, достаточно найти остаток от деления получившегося числа на количество букв в алфавите.

$$35 \bmod 33 = 2 \bmod 33 \rightarrow \text{в}.$$

Немного усовершенствуем нашу формулу:

$$C = f(p) \equiv (p + k) (\bmod N).$$

Данная запись означает, что мы ищем остаток от деления на N значения выражения $p + k$.

Операция «эквиваленция», или «равнозначность», обозначается поразному — знаком «≡» или двусторонней стрелкой. В наших формулах есть импликация, указанная односторонней стрелкой, поэтому для равнозначности используем знак «≡».

Пример 2. Зашифруем шифром Цезаря с ключом $k = 15$ слово «мир». В русском алфавите 33 буквы (N). Шифрующее преобразование примет вид: $C = f(p) \equiv (p + 15)(\text{mod } 33)$.

$f(\text{м}) \to f(13) \equiv (13 + 15)(\text{mod } 33) \equiv 28(\text{mod } 33) \to$ ы.
$f(\text{и}) \to f(9) \equiv (9 + 15)(\text{mod } 33) \equiv 24(\text{mod } 33) \to$ ч.
$f(\text{р}) \to f(17) \equiv (17 + 15)(\text{mod } 33) \equiv 32(\text{mod } 33) \to$ я.

Ответ: «ычя».

Для дешифрования элемента шифртекста $C \in \{0, 1, \ldots, N - 1\}$ необходимо вычислить:

$p = f^{-1}(C) \equiv (C - k)(\text{mod } N)$.

Данный вид шифрования прост, но, к сожалению, не является надёжным. Зашифрованное послание можно с лёгкостью дешифровать при помощи частотного анализа (подсчёта частоты встречаемости буквы в тексте). Допустим, чаще других в шифртексте встречается буква «т». Это значит, что сдвиг преобразует «о» = 15 (наиболее часто встречаемую букву в русском алфавите) в «т» = 19.

Найдём k:

$19 \equiv (15 + k)(\text{mod } 33)$.
$k \equiv 4(\text{mod } 33)$.

Чтобы дешифровать сообщение «офмуцтжфдшмг», остаётся вычесть 4 (по модулю 33) из числовых эквивалентов букв послания:

«офмуцтжфдшмг» = 15 21 13 20 23 19 7 21 4 25 13 3 =
= 11 17 9 16 19 15 3 17 0 21 9 32 = «криптография».

Замечание. При решении сравнений могут возникать случаи, когда искомое значение равняется отрицательному числу по модулю:

$17 + x \equiv 9(\text{mod } 5)$.
$x \equiv -8(\text{mod } 5)$.

В таком случае выражение можно представить в виде:

1) $-8 = 5 \cdot (-1) - 3$ (т. е. при делении на 5 имеется отрицательный остаток -3);
2) $-8 = 5 \cdot (-2) + 2$ (при таком разложении остаток положительный).

При решении задач нам потребуется положительное решение, поэтому: $x \equiv 2(\text{mod } 5)$.

А о числах -8, -3, 2, 7 и т. д. говорят, что они сравнимы по модулю 5, так как при делении на 5 эти числа дают один и тот же положительный остаток 2.

Но даже если имеется небольшое послание, по которому нельзя определить часто встречающуюся букву, то для расшифровки есть всего 33 возможности, и можно просто попробовать их все. В конце концов лишь одному значению будет соответствовать осмысленное сообщение. Это значение и будет ключом шифрования.

Шифр Гронсфельда

Шифр Цезаря можно сделать более надёжным, если дополнить его числовым ключом. Для этого за каждой буквой исходного текста закрепляется цифра числового ключа. Если длина ключа меньше длины сообщения, то ключ циклически повторяется до конца. Ключ шифрования для каждой буквы исходного текста получается свой, определённый числовым ключом.

Такая модификация шифра Цезаря называется шифром Гронсфельда.

Пример 3. Зашифруем слово «модификация» с помощью числового ключа $k = 1572$.

1	5	7	2	1	5	7	2	1	5	7
м	о	д	и	ф	и	к	а	ц	и	я

f(м) $\to$ $f(13) \equiv (13 + 1) \pmod{33} \equiv 14 \pmod{33}$ $\to$ н.
f(о) $\to$ $f(15) \equiv (15 + 5) \pmod{33} \equiv 20 \pmod{33}$ $\to$ у.
f(д) $\to$ $f(4) \equiv (4 + 7) \pmod{33} \equiv 11 \pmod{33}$ $\to$ к.
f(и) $\to$ $f(9) \equiv (9 + 2) \pmod{33} \equiv 11 \pmod{33}$ $\to$ к.
f(ф) $\to$ $f(21) \equiv (21 + 1) \pmod{33} \equiv 22 \pmod{33}$ $\to$ х.
f(и) $\to$ $f(9) \equiv (9 + 5) \pmod{33} \equiv 14 \pmod{33}$ $\to$ н.
f(к) $\to$ $f(11) \equiv (11 + 7) \pmod{33} \equiv 18 \pmod{33}$ $\to$ с.
f(а) $\to$ $f(0) \equiv (0 + 2) \pmod{33} \equiv 2 \pmod{33}$ $\to$ в.
f(ц) $\to$ $f(23) \equiv (23 + 1) \pmod{33} \equiv 24 \pmod{33}$ $\to$ ч.
f(и) $\to$ $f(9) \equiv (9 + 5) \pmod{33} \equiv 14 \pmod{33}$ $\to$ н.
f(я) $\to$ $f(32) \equiv (32 + 7) \pmod{33} \equiv 39 \pmod{33} \equiv 6 \pmod{33}$ $\to$ ё.

Ответ: «нуккхнсвчнё».

Заметим, что одинаковые буквы при шифровании переходят в разные, а разным буквам может соответствовать одна и та же буква шифртекста, что затрудняет частотный анализ.

Несомненным достоинством шифра Гронсфельда является то, что количество возможных числовых ключей практически неисчерпаемо. Это делает частотный анализ затруднительным, но всё же возможным, если учесть, что в числовом ключе каждая цифра имеет только десять значений, а значит, имеется лишь десять вариантов прочтения каждой буквы шифртекста. Однако шифр Гронсфельда допускает дальнейшие модификации, повышающие его стойкость, в частности двойное шифрование разными числовыми ключами.

Аффинный шифр

Для шифрования буквы исходного послания пользуются аффинными отображениями:

$$C \equiv (a \cdot p + b)(\mathrm{mod}\ N),$$

где a и b — фиксированные целые числа (они образуют ключ шифрования).

Замечание. На выбор a накладывается ограничение: a и N должны быть взаимно просты. В противном случае невозможно выразить p через C для дешифрования сообщения, так как одной букве шифртекста будет отвечать несколько букв открытого текста, и поэтому нельзя будет однозначно восстановить исходный текст.

Пример 4. Зашифруем сообщение «криптография», используя аффинное отображение с ключом шифрования $a = 7$, $b = 4$.

f(к) $\to f(11) \equiv (7 \cdot 11 + 4)(\mathrm{mod}\ 33) \equiv 81(\mathrm{mod}\ 33) \equiv 15(\mathrm{mod}\ 33) \to$ о.
f(р) $\to f(17) \equiv (7 \cdot 17 + 4)(\mathrm{mod}\ 33) \equiv 24(\mathrm{mod}\ 33) \to$ ч.
f(и) $\to f(9) \equiv (7 \cdot 9 + 4)(\mathrm{mod}\ 33) \equiv 1(\mathrm{mod}\ 33) \to$ б.
f(п) $\to f(16) \equiv (7 \cdot 16 + 4)(\mathrm{mod}\ 33) \equiv 17(\mathrm{mod}\ 33) \to$ р.
f(т) $\to f(19) \equiv (7 \cdot 19 + 4)(\mathrm{mod}\ 33) \equiv 5(\mathrm{mod}\ 33) \to$ е.
f(о) $\to f(15) \equiv (7 \cdot 15 + 4)(\mathrm{mod}\ 33) \equiv 10(\mathrm{mod}\ 33) \to$ й.
f(г) $\to f(3) \equiv (7 \cdot 3 + 4)(\mathrm{mod}\ 33) \equiv 25(\mathrm{mod}\ 33) \to$ ш.
f(р) $\to f(17) \equiv (7 \cdot 17 + 4)(\mathrm{mod}\ 33) \equiv 24(\mathrm{mod}\ 33) \to$ ч.
f(а) $\to f(0) \equiv (7 \cdot 0 + 4)(\mathrm{mod}\ 33) \equiv 4(\mathrm{mod}\ 33) \to$ д.
f(ф) $\to f(21) \equiv (7 \cdot 21 + 4)(\mathrm{mod}\ 33) \equiv 19(\mathrm{mod}\ 33) \to$ т.
f(и) $\to f(9) \equiv (7 \cdot 9 + 4)(\mathrm{mod}\ 33) \equiv 1(\mathrm{mod}\ 33) \to$ б.
f(я) $\to f(32) \equiv (7 \cdot 32 + 4)(\mathrm{mod}\ 33) \equiv 30(\mathrm{mod}\ 33) \to$ э.

Ответ: «очбрейшчдтбэ».

Для дешифрования сообщения, зашифрованного с применением аффинного отображения, нужно выразить p через C:

$$p \equiv (a^{-1} \cdot C + b^{-1})(\mathrm{mod}\ N),$$

где a^{-1} — обратное к a по модулю число, $b^{-1} = -a^{-1} \cdot b$.

Пример 5. Определим, какая буква алфавита шифруется буквой «л» при аффинном преобразовании из прошлого примера.

1. Сначала найдем a^{-1}:

$7 \cdot a^{-1} \equiv 1(\mathrm{mod}\ 33)$.
$a^{-1} \equiv 19(\mathrm{mod}\ 33)$.

Замечание. При нахождении неизвестного x из сравнения $k \cdot x \equiv m(\mathrm{mod}\ N)$ советуем найти такое целое x, при котором $k \cdot x$ равнялось бы одному из чисел $m + N$, $m + 2N$, $m + 3N$ и т. д.

В разбираемом примере:

$7 \cdot x = 34$ — нет такого целого x;
$7 \cdot x = 67$ — нет такого целого x;

$7 \cdot x = 100$ — нет такого целого x;
$7 \cdot x = 133$ — есть такое целое $x = 19$.

2. Дешифрующее преобразование примет вид:

$p = (19 \cdot C - 19 \cdot 4)(\text{mod } 33)$.
$p = (19 \cdot C - 76)(\text{mod } 33)$.

3. Подставим вместо C порядковый номер буквы «л»:

$p \equiv 19 \cdot 12 - 76(\text{mod } 33) \equiv 152(\text{mod } 33) \equiv 20(\text{mod } 33) \rightarrow$ у.

Ответ: буква «у» при данном шифровании переходит в букву «л».

Для нахождения ключа при криптоанализе необходимо знать две буквы шифртекста и соответствующие им буквы открытого текста, для того чтобы можно было составить и решить систему сравнений.

Пример 6. Допустим, в шифртексте чаще всего встречаются буквы «т» и «к». Разумно предположить, что ими зашифрованы две наиболее часто встречающиеся буквы «о» и «е». Заменяя буквы их числовыми эквивалентами и подставляя последние в формулу дешифрования, получаем:

$19 \cdot a^{-1} + b^{-1} = 15(\text{mod } 33)$.
$11 \cdot a^{-1} + b^{-1} = 5(\text{mod } 33)$.

Замечание. Система сравнений в данном случае решается как система уравнений. Методом вычитания получим:

$8 \cdot a^{-1} = 10(\text{mod } 33)$.
$a^{-1} = 26$.

Находим b^{-1}, подставляя a^{-1} в любое сравнение системы и решая его:
$b^{-1} = 16$.
То есть всё сообщение может быть дешифровано применением формулы:

$p \equiv (26 \cdot C + 16)(\text{mod } 33)$.

Задания для самостоятельного выполнения

Задание 1.
Зашифруйте сообщение при помощи шифра Цезаря (используется полный 33-буквенный русский алфавит; пробелы и запятые оставлены для удобства прочтения — шифровать их не нужно):
а) «начинаем», используя ключ $k = 8$;
б) «старт», используя ключ $k = 11$;
в) «победа», используя ключ $k = 17$;
г) «тренировка», используя ключ $k = 4$;
д) «полководец», используя ключ $k = 5$;
е) «римская империя», используя ключ $k = 28$;
ж) «пришёл, увидел, победил», используя ключ $k = 13$.

Совет. Можно шифровать вручную, но лучше написать программу и выполнить шифрование в автоматизированном режиме.

Задание 2.

Поупражняемся в дешифровании сообщений, зашифрованных при помощи шифра Цезаря (пунктуация сохранена только для удобства прочтения).

а) На вопрос о том, какая смерть самая лучшая, Цезарь отвечал: «ачбщыцтаатс» ($k = 19$).

б) Древнеримский драматург Децим Лаберий так говорил о Цезаре: «Ицжьвщж фхцкрэ лцуомх ьць, тцкц ицжьщж фхцкрм» ($k = 8$).

в) Актуальный вопрос: «Ж шухй зв Етпр Эложчг фл клтжщг хкфхичлулффх шщхтгсх клт, шсхтгсх ухнлу фл клтжщг ув?» (писатель Аркадий Давидович) ($k = 7$).

Задание 3.

Поупражняемся в дешифровании сообщений. Найдите результаты двух выражений. Для этого нужно расшифровать два сообщения, зашифрованных шифром Цезаря с указанным значением ключа. В сообщениях зашифрованы названия арифметических операций. Подставьте эти арифметические операции на место троеточий («...») в соответствующие арифметические выражения, вычислите их значения.

а)

№	Сообщение	Значение ключа	Выражение
1	ёяымцдсми	4	4 ... 3 =
2	зиписми		28 ... 7 =

б)

№	Сообщение	Значение ключа	Выражение
1	ыфхцомхрм	8	3 ... 3 =
2	лмумхрм		28 ... 7 =

в)

№	Сообщение	Значение ключа	Выражение
1	хпткисми	4	4 ... 3 =
2	фдлстхца		8 ... 7 =

г)

№	Сообщение	Значение ключа	Выражение
1	ыфхцомхрм	8	1 ... 3 =
2	лмумхрм		27 ... 3 =

Совет. Можно дешифровать вручную, но лучше написать программу и выполнить дешифрование в автоматизированном режиме.

Задание 4.

Зашифруйте шифром Гронсфельда с ключом 1734 (предполагаемый год создания этого алгоритма):

а) имя создателя шифра — «Гронсфельд»;

б) страну рождения автора шифра — «Бельгия».

Совет. Можно шифровать вручную, но лучше написать программу и выполнить шифрование в автоматизированном режиме.

Задание 5.
Декодируйте с помощью шифра Гронсфельда сообщение ($k = 127$):
а) «шжщьтл»;
б) «рбщэ»;
в) «утп»;
г) «гршёог».

Совет. Можно дешифровать вручную, но лучше написать программу и выполнить дешифрование в автоматизированном режиме.

Задание 6.
Зашифруйте названия достопримечательностей Афин при помощи аффинного шифрования:
а) «Микены», используя ключ: $a = 5$, $b = 2$;
б) «Парфенон», используя ключ: $a = 10$, $b = 3$;
в) «Акрополь», используя ключ: $a = 7$, $b = 2$.

Совет. Можно шифровать вручную, но лучше написать программу и выполнить шифрование в автоматизированном режиме.

Задание 7.
Дешифруйте, используя указанные ключи шифрования (пунктуация сохранена только для удобства прочтения):
а) «Пхыуч... Ъвпоч ы гщшвяч,» при $a = 5$, $b = 16$;
б) «Гидж, хо уоёб брдькеж» при $a = 7$, $b = 9$;
в) «Ёйлжяв, нглёфь ъкгт юхнж» при $a = 8$, $b = 15$;
г) «Ъ лвжч, лдылик юыжчз...» при $a = 28$, $b = 3$.

Совет. Можно дешифровать вручную, но лучше написать программу и выполнить дешифрование в автоматизированном режиме.

Проектное задание.
Результат проекта — прототип реального объекта (рис. 1).

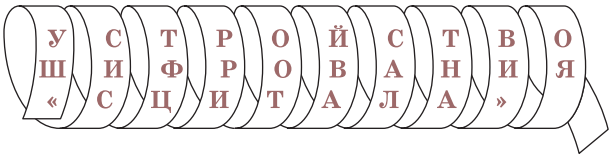

Рис. 1. Устройство (предмет) для шифрования

1. В дополнительных источниках найдите описание различных предметов (устройств), которые использовали для шифрования, изготовьте их прототипы и придумайте обучающие задания (игры) для использования этих предметов (устройств).
2. Организуйте конкурс на лучшее воплощение таких предметов (устройств) для шифрования.

Практическая работа № 2
Цифровая подпись

Цель работы: изучить основы асимметричных систем шифрования, разобрать реализацию алгоритма RSA (рис. 2) и понять его математические основы.

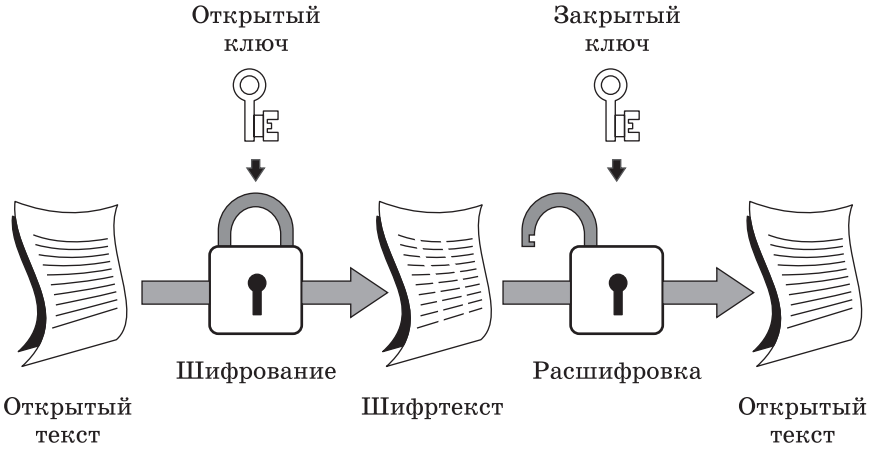

Рис. 2. Схема работы алгоритма RSA

Криптографическая система с открытым ключом RSA названа в честь учёных из Массачусетского технологического института: Рональда Ривеста, Ади Шамира и Леонарда Адлемана. RSA — аббревиатура от их фамилий Rivest, Shamir и Adleman.

Алгоритм включает несколько этапов.

Этап 1
Генерация открытого и закрытого ключей шифрования

Выберем два различных простых числа p и q:

$p = 17,\ q = 13.$

Найдём произведение этих чисел n. Это будет один из открытых ключей абонента.

$n = 17 \cdot 13 = 221.$

Найдём количество натуральных чисел, меньших числа n и взаимно простых с ним (функция Эйлера). Так как n раскладывается только на два простых делителя, а для простых чисел все числа, меньшие их самих, с ними взаимнопросты, то $\varphi(n) = (p - 1)(q - 1)$.

$\varphi(n) = (17 - 1)(13 - 1) = 16 \cdot 12 = 192.$

В качестве открытого ключа a (открытой экспоненты) выберем число, взаимно простое с $\varphi(n)$ и меньшее $\varphi(n)$.

$a = 5.$

НОД(5, 192) = 1.

Вычислим закрытый ключ α: $\alpha \cdot a \equiv 1(\text{mod } (n))$.

$5 \cdot \alpha \equiv 1(\text{mod } 192)$.

Замечание. При нахождении неизвестного x из сравнения $k \cdot x \equiv m(\text{mod } N)$ советуем найти такое целое x, при котором $k \cdot x$ равнялось бы одному из чисел $m + N$, $m + 2N$, $m + 3N$ и т. д.

В разбираемом примере:

$5 \cdot \alpha = 193$ — нет такого целого α;
$5 \cdot \alpha = 385$ — есть такое целое $\alpha = 77$.

Таким образом, у всех абонентов есть свой открытый ключ (a, n), передаваемый другим абонентам, и закрытый (α, n), который передавать не следует.

Абонент A	p_1 и q_1	n_A	a	α
Абонент B	p_2 и q_2	n_B	b	β
Абонент C	p_3 и q_3	n_C	c	γ
...	...	...	...	...

Нашим открытым ключом является пара (5, 221), а закрытым — (77, 221).

Этап 2
Передача зашифрованного сообщения

Чтобы передать сообщение, необходимо знать открытый ключ адресата (a, n_A). Сообщением является число m.

Пусть открытым ключом нашего собеседника является (5, 221), а передаваемое сообщение $m = 6$.

Зашифрованное сообщение m_1 получается после вычисления следующей операции:

$m_1 \equiv m^a(\text{mod } n_A)$,
$m_1 \equiv 6^5(\text{mod } 221)$,
$m_1 \equiv 41(\text{mod } 221)$.

Этап 3
Дешифрование полученного сообщения

Дешифрование осуществляется с использованием закрытого ключа самим получателем сообщения следующим образом:

$m_2 = m_1^{\alpha} \equiv m(\text{mod } n)$,
$m_2 = 41^{77}(\text{mod } 221)$. (Прекрасная задача, не правда ли?)

Замечание. При нахождении степеней по модулю промежуточные результаты также преобразуйте по модулю — это облегчит задачу. И не забывайте про свойства степеней!

$41^2 = 1681 = 134 (\mathrm{mod}\ 221)$,
$41^3 = 134 \cdot 41 = 5494 = 190 (\mathrm{mod}\ 221)$,
$41^5 = 41^2 \cdot 41^3 = 134 \cdot 190 = 25\ 460 = 45 (\mathrm{mod}\ 221)$,
$41^{10} = 41^5 \cdot 41^5 = 45 \cdot 45 = 2025 = 36 (\mathrm{mod}\ 221)$,
$41^{20} = 41^{10} \cdot 41^{10} = 36 \cdot 36 = 1296 = 191 (\mathrm{mod}\ 221)$,
$41^{40} = 41^{20} \cdot 41^{20} = 191 \cdot 191 = 36\ 481 = 16 (\mathrm{mod}\ 221)$,
$41^{70} = 41^{40} \cdot 41^{20} \cdot 41^{10} = 16 \cdot 191 \cdot 36 = 110\ 016 = 179 (\mathrm{mod}\ 221)$,
$41^{77} = 41^{70} \cdot 41^5 \cdot 41^2 = 179 \cdot 45 \cdot 134 = 1\ 079\ 370 = 6 (\mathrm{mod}\ 221)$.

В реальной жизни используют крайне большие простые числа (не 17 и 13, а намного большие). К примеру, самими авторами в качестве открытых ключей системы использовались 129-значное число n и $a = 9007$.

В 2010 году учёные успешно расшифровали данные, зашифрованные с использованием ключа стандарта RSA длиной 768 бит, и советовали не использовать ключи длиной менее 1024 бит.

Задания для самостоятельного выполнения

Задание 1.

1) Подготовьте программу на любом языке программирования для вычисления открытого и закрытого ключей шифрования и дешифрования методом RSA.
2) Выберите и вычислите открытые и закрытые ключи для двух абонентов. Используйте числа $p = 19$, $q = 17$ и минимальную экспоненту.
3) Для теста зашифруйте числа $A = 19$ и $B = 7$ для второго абонента с помощью чисел $p = 19$, $q = 17$ и минимальной экспоненты.
   Для проверки работы алгоритма самостоятельно расшифруйте эти числа.
4) Вы создали пару ключей для чисел $p = 19$, $q = 17$ и выбрали экспоненту 5. Было получено сообщение:
   «282 166 дтбимяъбгфргхръфрбнхсёмгръм».
   Расшифруйте его.
5) Какой максимальной длины в битах ключ вы можете использовать? Почему?

Задание 2.

1) Используя готовую программу, выберите и вычислите открытые и закрытые ключи для двух абонентов. Используйте числа $p = 23$, $q = 13$ и минимальную экспоненту.
2) Для теста зашифруйте числа $A = 13$ и $B = 11$ для второго абонента с помощью чисел $p = 23$, $q = 13$ и минимальной экспоненты.
   Для проверки работы алгоритма самостоятельно расшифруйте эти числа.
3) Вы создали пару ключей для чисел $p = 23$, $q = 13$ и выбрали экспоненту 5. Для вас получено сообщение:
   «234 189 звшркфбьдйъуднъбйъьонюпкдъбк».
   Что вам написали?
4) Если вы написали программу не в среде PascalABC.NET, то какой максимальной длины в битах ключ вы можете использовать? Почему?