Министерство образования Российской Федерации

Санкт-Петербургский государственный институт точной механики и оптики (технический университет)

Ю.А.Гатчин, А. Г. Коробейников

Основы криптографических алгоритмов

Учебное пособие

Санкт-Петербург 2002

УДК 511
Ю.А.Гатчин, А. Г. Коробейников. Основы криптографических алгоритмов Учебное пособие. СПб: ГИТМО (ТУ), 2002. 29 с.

В учебном пособии рассматриваются основы современных математических криптографических алгоритмов, фундаментом которых является прикладная теория чисел.

Рассмотрены криптосистемы с секретным ключом (одноключевые, симметричные или классические), а также криптосистемы с открытым ключом (асимметричные). Кроме того, представлены основные положения криптографического протокола "электронная подпись". В каждом разделе рассмотрены примеры на соответствующие темы.

Предназначено для студентов, обучающихся по специальности 0754 "Комплексная защита объектов информатизации".

Илл. – 3, список литературы – 8 наим.

ВВЕДЕНИЕ

Математическая криптография возникла как наука о шифровании информации, т.е. как наука о криптосистемах. В классической шенноновской модели системы секретной связи имеют два полностью доверяющих друг-другу участника, которым необходимо передавать между собой информацию, не предназначенную для третьих лиц. Такая информация называется конфиденциальной или секретной. Отсюда возникает задача обеспечения конфиденциальности, т.е. защита секретной информации от противника. Эта задача, по крайней мере исторически, – первая задача криптографии. Она традиционно решается с помощью криптосистем.

При обмене информацией между участниками часто возникает ситуация, когда информация не является конфиденциальной, но важен факт поступления сообщений в неискаженном виде, т.е. наличие гарантии, что никто сумеет не подделать сообщение. Такая гарантия называется обеспечением целостности информации и составляет вторую задачу криптографии.

Для предотвращения угрозы контроля за источниками информации (откуда пересылаются сообщения) необходима система контроля за доступом к ресурсам, которая должна удовлетворять двум, казалось бы, взаимно исключающим требованиям. Во – первых, всякий желающий должен иметь возможность обратиться к этой системе анонимно, а во – вторых, при этом все же доказать свое право на доступ к ресурсам. Примером могут служить бумажные купюры. Если ресурсом является некоторый товар, то наличие у покупателя достаточного количества купюр является доказательством его права на доступ к ресурсу. С другой стороны, хотя каждая бумажная купюра и имеет уникальный номер, отслеживать купюры по номерам практически невозможно, т.е. определить, кто ее использовал и в каких платежах, практически невозможно. Аналог этого свойства в криптографии называется неотслеживаемостью. Обеспечение неотслеживаемости –третья задача криптографии.

Если задача обеспечения конфиденциальности решается с помощью криптосистем, то для обеспечения целостности и неотслеживаемости разрабатываются криптографические протоколы.

В первой части кратко рассмотрена история криптографии и её основные понятия. Приведены основные классические шифры, такие как, шифр Цезаря, маршрутная транспозиция, таблица Виженера, одноразовый блокнот и т.д.

Во второй части изучаются основные свойства диофантова уравнения и метод его решения при помощи алгоритма Евклида. Рассмотрена криптосистема без передачи ключей.

В третьей части представлена криптосистема с открытым ключом, рассмотрена основные положения системы шифрования RSA, дан анализ стойкости системы с открытым ключом.

В четвертой части рассмотрены основные положения криптографического протокола "электронная подпись".

В пятой части рассмотрено использование криптографических алгоритмов для защиты программного обеспечения. Дан анализ их применения в некоторых программных продуктах.

Каждая часть сопровождается соответствующими примерами.

Криптографические средства и программные продукты, упоминаемые в пособии, используются только для иллюстрации общих криптографических идей, так как в работе не ставится цель сравнения имеющихся на рынке криптографических средств.

1. КЛАССИЧЕСКИЕ ШИФРЫ И ОСНОВНЫЕ ПОНЯТИЯ

1.1. ИЗ ИСТОРИИ КРИПТОГРАФИИ

Термин *криптография* (тайнопись) ввел Д. Валлис. Потребность шифровать и передавать шифрованные сообщения возникла очень давно. Так, еще в V-IV вв. до н. э. греки применяли специальное шифрующее устройство. По описанию Плутарха, оно состояло из двух палок одинаковой длины и толщины. Одну оставляли себе, а другую отдавали отъезжающему. Эти палки называли *скиталами*. Когда правителям нужно было сообщить какую-нибудь важную тайну, они вырезали длинную и узкую, вроде ремня, полосу папируса, наматывали ее на свою скиталу, не оставляя на ней никакого промежутка, так чтобы вся поверхность палки была охвачена этой полосой. Затем, оставляя папирус на скитале в том виде, как он есть, писали на нем все, что нужно, а написав, снимали полосу и без палки отправляли адресату. Так как буквы на ней разбросаны в беспорядке, то прочитать написанное можно только при помощи соответствующей скиталы, намотав на нее без пропусков полосу папируса.

Аристотелю принадлежит способ дешифрования этого шифра. Надо изготовить длинный конус и, начиная с основания, обертывать его лентой с шифрованным сообщением, постепенно сдвигая ее к вершине. В какой-то момент начнут просматриваться куски сообщения. Так можно определить диаметр скиталы.

В Древней Греции (II в. до н. э.) был известен шифр, называемый *квадрат Полибия*. Это устройство представляло собой квадрат 5 х 5, столбцы и строки которого нумеровали цифрами от 1 до 5. В каждую клетку этого квадрата записывалась одна буква. (В греческом варианте одна клетка оставалась пустой, в латинском – в одну клетку помещали две буквы ***i*** и ***j***.) В результате каждой букве отвечала пара чисел и шифрованное сообщение превращалось в последовательность пар чисел.

Пример 1. 13 34 22 24 44 34 15 42 22 34 43 45 32

Это сообщение записано при использовании латинского варианта квадрата Полибия, в котором буквы расположены в алфавитном порядке.

("Cogito, ergo sum" – лат, "Я мыслю, следовательно существую"). ♦

В 1 в. н.э. Ю. Цезарь во время войны с галлами, переписываясь со своими друзьями в Риме, заменял в сообщении первую букву латинского алфавита (A) на четвертую (D), вторую (B) – на пятую (E), наконец, последнюю – на третью:

⇓ A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

⇑ D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

Пример 2. Донесение Ю. Цезаря Сенату об одержанной им победе над Понтийским царем выглядело так:

YHQL YLGL YLFL("Veni, vidi, vici" – лат. "Пришел, увидел, победил") .♦

Император Август (1 в. н. э.) в своей переписке заменял первую букву на вторую, вторую – на третью и т. д., наконец, последнюю – на первую:

⇓ A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
⇑ B C D E F G H I J K L M N O P Q R S T U V W X Y Z A

Пример 2. Любимое изречение императора Августа выглядело так: GFTUJOB MFOUF ("Festina lente" – лат. "Торопись медленно") .♦

Квадрат Полибия, шифр Цезаря входят в класс шифров, называемых *подстановка* или *простая замена*, т.е. Это такой шифр, в котором каждой букве алфавита соответствует буква, цифра, символ или какая-нибудь их комбинация.

В известных рассказах “Пляшущие человечки” Конан Дойля и “Золотой жук” Эдгара По используемые шифры относятся к указанному классу шифров. В другом классе шифров – *перестановка* – буквы сообщения каким-нибудь способом переставляются между собой. К этому классу принадлежит шифр скитала.

1.2. МАРШРУТНАЯ ТРАНСПОЗИЦИЯ

К классу перестановка относится шифр *маршрутная транспозиция* и его вариант *постолбцовая транспозиция*. В каждом из них в данный прямоугольник [$n \times m$] сообщение вписывается заранее обусловленным способом, а столбцы нумеруются или обычным порядком следования, или в порядке следования букв *ключа* – буквенного ключевого слова.

Пример 3. В первом прямоугольнике столбцы нумеруются в обычном порядке следования – слева направо, а во втором – в порядке следования букв слова “Пушкин”. Используя расположение букв этого ключа в алфавите, получим набор чисел [4 5 6 2 1 3]:

1	2	3	4	5	6
д	е	л	а	д	а
в	н	о	м	и	н
у	в	ш	и	х	д
н	е	й	п	р	е
д	а	н	ь	я	с
т	а	р	и	н	ы
г	л	у	б	о	к
о	й	а	б	в	г

4	5	6	2	1	3
д	е	л	а	д	а
в	н	о	м	и	н
у	в	ш	и	х	д
н	е	й	п	р	е
д	а	н	ь	я	с
т	а	р	и	н	ы
г	л	у	б	о	к
о	й	а	б	в	г

В первом случае шифрованный текст найдем, если будем выписывать буквы очередного столбца в порядке следования столбцов (прямом или обратном), во втором, – если будем выписывать буквы столбца в порядке следования букв ключа. Таким образом, будем иметь:

1) двундтго енвеаалй лошйнруа амипьибб дихрянов андесыкг;
2) дихрянов амипьибб андесыкг двундтго енвеаалй лошйнруа. ♦

Термин “шифр” арабского происхождения. В начале XV в. арабы опубликовали энциклопедию “Шауба Аль-Аща”, в которой есть специальный раздел о шифрах. В этой энциклопедии указан способ раскрытия шифра простой замены. Он основан на различной частоте повторяемости букв в тексте. В этом разделе есть перечень букв в порядке их повторяемости на основе изучения текста Корана. Заметим, что в русском тексте чаще всего встречается буква “О”, затем буква “Е” и на третьем месте стоят буквы “И” и “А”. Более точно: на 1000 букв русского текста в среднем приходится 90 букв “О”, 72 буквы “Е” или “Ё”, 60 букв “И” и “А” и т.д.

Неудобство шифров типа подстановка (простая замена) в случае использования стандартного алфавита очевидно. Таблица частот встречаемости букв алфавита позволяет определить одни или несколько символов, а этого иногда достаточно для дешифрования всего сообщения (“Пляшущие человечки” Конан Дойля или “Золотой жук” Эдгара По). Поэтому обычно пользуются разными приемами, чтобы затруднить дешифрование. Для этой цели используют *многобуквенную систему шифрования* – систему, в которой одному символу отвечает одна или несколько комбинаций двух и более символов. Другой прием – использование нескольких алфавитов. В этом случае для каждого символа употребляют тот или иной алфавит в зависимости от ключа, который связан каким-нибудь способом с самим символом или с его порядком в передаваемом сообщении.

1.3. ТАБЛИЦА ВИЖЕНЕРА

В процессе шифрования (и дешифрования) используется *таблица Виженера*, которая устроена следующим образом: в первой строке выписывается весь алфавит, в каждой следующей осуществляется циклический сдвиг на одну букву. Так получается квадратная таблица, число строк которой равно числу столбцов в алфавите. Чтобы зашифровать какое-нибудь сообщение, поступают следующим образом. Выбирается слово – лозунг и подписывается с повторением над буквами сообщения.

Чтобы получить шифрованный текст, находят очередной знак лозунга, начиная с первого в вертикальном алфавите, а ему соответствующий знак сообщения в горизонтальном.

Пример 4. Таблица 1, составлена из 31 буквы русского алфавита (без букв Ё и Ъ).

Выбираем лозунг – математика. Находим столбец, отвечающий букве "м" лозунга, а затем строку, соответствующую букве "к". На пересечении выделенных столбца и строки находим букву "ц". Так продолжая дальше, находим весь шифрованный текст.

м а т е м а т и к а м а т е м а т и к а м а т е м а
к р и п т о г р а ф и я с е р ь е з н а я н а у к а

таблица 1

А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я
Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А
В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б
Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В
Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г
Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д
Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е
З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж
И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З
Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И
К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й
Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К
М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л
Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М
О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н
П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О
Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П
С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р
Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С
У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т
Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У
Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф
Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х
Ч	Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц
Ш	Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч
Щ	Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш
Ь	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ
Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь
Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы
Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э
Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю

ц р ь ф я о х ш к ф ф я д к э ь ч п ч а л н т ш ц а ♦

Наконец, к сообщению можно применять несколько систем шифрования.

1.4. МОДИФИЦИРОВАННЫЙ ШИФР ЦЕЗАРЯ

Аббат Тритемеус – автор первой печатной книги о тайнописи (1518 г.) – предложил несколько шифров и среди них шифр, который можно считать усовершенствованием шифра Цезаря. Этот шифр устроен так. Все буквы алфавита нумеруются по порядку (от 1 до 31 в русском варианте). Затем выбирают какое-нибудь слово, называемое "ключом", и подписывают под сообщением с повторением.

Чтобы получить шифрованный текст, складывают номер очередной буквы с номером соответствующей буквы ключа. Если полученная сумма больше 31, то из нее вычитают 31. В результате получают последовательность чисел от 1 до 31. Вновь заменяя числа этой последовательности соответствующими буквами, получают шифрованный текст. Разбиваем этот текст на группы одной длины, получают шифрованное сообщение.

Пример 5. Выбираем ключевое слово "Пособие". Составляем сообщение "сессия начинается в конце семестра"

с е с с и я н а ч и н а е т с я в к о н ц е с е м е с т р а
п о с о б и е п о с о б и е п о с о б и е п о с о б и е п о

Шифруем, разбиваем текст на группы длины 6, и получаем шифрованное сообщение:

в ф д а и и у р з ь э в о ш в о ф щ р ц э х б ч ы з ь ш б п ♦

Чтобы получить шифрованный текст, складывают номер очередной буквы с номером соответствующей буквы ключа. Если полученная сумма больше 33, то из нее вычитают 33. В результате получают последовательность чисел от 1 до 33. Вновь заменяя числа этой последовательности соответствующими буквами, получают шифрованный текст. Разбивал этот текст на группы одной длины (например, по 5*),* получают шифрованное сообщение.

Если под ключом шифра понимать однобуквенное слово “В” (в русском варианте), то мы получим шифр Цезаря.

Пример 6. Для сообщения из примера 5, получим:

ф и ф ф л в р г ь л р г и х ф в в н т р щ и ф и п и ф х у г ♦

1.5. ОДНОРАЗОВЫЙ БЛОКНОТ

Почти все используемые на практике шифры характеризуются как условно надежные, поскольку они могут быть раскрыты в принципе при наличии неограниченных вычислительных возможностей. Абсолютно надежные шифры нельзя разрушить даже при наличии неограниченных вычислительных возможностей. Доказательство существования и единственности абсолютно надежного шифра получил К.Шеннон с помощью разработанного им теоретико-информационного метода исследования шифров. Таким образом, единственный абсолютно надежный шифр, который используется на практике, это так называемый *одноразовый блокнот*, в основе которого лежит та же идея, что и шифре Цезаря. Рассмотрим его основную идею.

В русском варианте число символов *расширенного алфавита*, т.е. совокупности букв, а также знаков препинания и пробела между словами, равно 44. Занумеровав все символы расширенного алфавита числами от 0 до 43, можно рассматривать любой передавамый текст, как последовательность $\{a_n\}$ чисел множества $\mathbf{A}=\{\mathbf{0,1,2,\ldots,43}\}$. Имея случайную последовательность $\{c_n\}$ из чисел множества $\mathbf{A}$ той же длины что и передаваемый текст (ключ), складываем по модулю 44 число a_n передаваемого текста с соответствующим числом c_n ключа

$$a_n+c_n\equiv b_n(\mathbf{mod}\ 44),\ 0\le b_n\le 43,$$

получим последовательность $\{b_n\}$ знаков шифрованного текста.

Чтобы получить передаваемый текст, можно воспользоваться тем же ключом:

$$a_n\equiv b_n-c(\mathbf{mod}\ 44),\ 0\le a_n\le 43.$$

У двух абонентов, находящихся в секретной переписке, имеются два одинаковых блокнота, составленных из отрывных страниц, на каждой из которых напечатана таблица со случайными числами или буквами, т.е.

случайная последовательность чисел из множества **A**. Таблица имеет только две копии: одна используется отправителем, другая – получателем. Отправитель свой текст шифрует указанным выше способом при помощи первой страницы блокнота. Зашифровав сообщение, он уничтожает использованную страницу и отправляет его второму абоненту. Получатель шифрованного текста расшифровывает его и также уничтожает использованный лист блокнота. Нетрудно видеть, что одноразовый шифр нераскрываем в принципе, так как символ в тексте может быть заменен любым другим символом и этот выбор совершенно случаен.

2. ДИОФАНТОВЫ УРАВНЕНИЯ

2.1. ДИОФАНТОВО УРАВНЕНИЕ ПЕРВОЙ СТЕПЕНИ

Рассмотрим задачу отыскания целочисленного решения уравнения:

$$ax-my=1, \qquad (2.1)$$

где наибольший общий делитель (НОД) a и m равен 1, т.е. НОД(a,m)=1, $a>0$, $m>0$.

Для решения этой задачи число a/m обращают в конечную цепную дробь при помощи *алгоритма Евклида*:

$$a=mq_0+a_1,$$
$$m=a_1q_1+a_2,$$
$$a_1=a_2q_2+a_3,$$
$$a_2=a_3q_3+a_4,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$a_{k-2}=a_{k-1}q_{k-1}+a_k,$$
$$a_{k-1}=a_{k+1}q_k+0;$$

Цепная дробь имеет вид: $a/m = [q_0,q_1,q_2,\ldots q_k]$, а последовательности $\{\mathbf{P_n}\}$ и $\{\mathbf{Q_n}\}$ числителей и знаменателей подходящих дробей к цепной дроби определяются рекуррентно:

$$\mathbf{P_{-2}}=0,\ \mathbf{P_{-1}}=1;$$
$$\mathbf{Q_{-2}}=1,\ \mathbf{Q_{-1}}=0;$$
$$n\geq 0 \Rightarrow\ \mathbf{P_n} = q_n\mathbf{P_{n-1}} + \mathbf{P_{n-2}},$$
$$n\geq 0 \Rightarrow\ \mathbf{Q_n} = q_n\mathbf{Q_{n-1}} + \mathbf{Q_{n-2}}.$$

Их вычисление удобно оформлять в виде таблицы:

n	-2	-1	0	1	2	…	k-1	k
q_n			q_0	q_1	q_2	…	q_{k-1}	q_k
$\mathbf{P_n}$	0	1	$\mathbf{P_0}$	$\mathbf{P_1}$	$\mathbf{P_2}$	…	$\mathbf{P_{k-1}}$	$\mathbf{P_k}$
$\mathbf{Q_n}$	1	0	$\mathbf{Q_0}$	$\mathbf{Q_1}$	$\mathbf{Q_2}$	…	$\mathbf{Q_{k-1}}$	$\mathbf{Q_k}$

Но известно, что $\mathbf{P_kQ_{k-1}}-\mathbf{P_{k-1}Q_k}=(-1)^{k-1}$ и $a/m = \mathbf{P_k}/\mathbf{Q_k}$. Следовательно

$$(-1)^{k-1}\mathbf{P_kQ_{k-1}}-\mathbf{P_{k-1}}(-1)^{k-1}\mathbf{Q_k}=1.$$

А так как НОД(a,m)=1, то $\mathbf{P_k} = a$, $\mathbf{Q_k} = m$. Поэтому

$$(-1)^{k-1}\mathbf{Q_{k-1}}a - m(-1)^{k-1}\mathbf{P_{k-1}}=1.$$

Другими словами, пара (x,y), где $x=(-1)^{k-1}\mathbf{Q_{k-1}}$; $y=(-1)^{k-1}\mathbf{P_{k-1}}$, являются целочисленным решением уравнения (2.1).

2.2. РЕШЕНИЕ СРАВНЕНИЯ ПЕРВОЙ СТЕПЕНИ

Чтобы найти решение сравнения $ax\equiv 1 \pmod m$, где НОД(a,m)=1, обычно пользуются алгоритмом Евклида, и тогда $x\equiv(-1)^{k-1}\mathbf{Q_{k-1}} \pmod m$,, где $\mathbf{Q_{k-1}}$ – знаменатель предпоследней подходящей дроби разложения a/m в цепную дробь, или теоремой *Ферма-Эйлера*, которая утверждает, что если НОД(a,m)=1, то

$$a^{\varphi(m)} \equiv 1 (\mathbf{mod}\ m),$$

где $\varphi(m)$ – функция Эйлера.

Следовательно

$$x \equiv a^{\varphi(m)-1} (\mathbf{mod}\ m).$$

Пример 7. Решить сравнение

$$7283*x \equiv 1 (\mathbf{mod}\ 190116)$$

Имеем

$$7283=190116*0+7283$$
$$190116=7283*26+758$$
$$7283=758*9+461$$
$$758=461*1+297$$
$$461=297*1+164$$
$$297=164*1+133$$
$$164=133*1+31$$
$$133=31*4+9$$
$$31=9*3+4$$
$$9=4*2+1$$
$$4=1*4+0$$

n			0	1	2	3	4	5	6	7	8	9	10
q_n			0	26	9	1	1	1	1	4	3	2	4
P_n	0	1	0	1	9	10	19	29	48	221	711	1643	7283
Q_n	1	0	1	26	235	261	496	757	1253	5769	18560	42889	190116

Действительно, k=10; $x \equiv (-1)^9 \times 42889$ (**mod** 190116)= -42889 (**mod** 190116) = = 147227(**mod** 190116); (7283*147227-1)/ 190116=5640 ♦

2.3. КРИПТОСИСТЕМА БЕЗ ПЕРЕДАЧИ КЛЮЧЕЙ

Пусть абоненты ***A, B, C,*** ... условились организовать секретную переписку между собой. Для этой цели они выбирают достаточно большое простое число p и такое, что p-1 хорошо разлагается на не очень большие простые множители. Если среди множителей такого числа кратных нет, то число p-1 называют *евклидовым.* Каждый из абонентов независимо один от другого выбирает случайное число, натуральное, взаимно простое с числом p-1**:** ***A, B, C,*** ... – абоненты; a, b, c, ... – выбранные ими случайные числа. Далее, абонент A находит число α из условия

$$a \cdot \alpha \equiv 1 (\mathbf{mod}\ \varphi(p)),\ 0 < \alpha < p-1; \qquad (2.2)$$

абонент B находит число β из условия

$$b \cdot \beta \equiv 1 (\mathbf{mod}\ \varphi(p)),\ 0 < \beta < p-1, \qquad (2.3)$$

где $\varphi(p)$ – функция Эйлера, a, α – секретные ключи абонента A; b, β – секретные ключи абонента B и т.д.

Пусть абонент A решает послать сообщение m абоненту B. Можно предполагать, что $0 < m < p$-1. Тогда он сначала зашифровывает это сообщение своим первым секретным ключом, находит:

$$m_1 \equiv m^a (\mathbf{mod}\ p),\ 0 < m_1 < p \qquad (2.4)$$

и отправляет абоненту ***B.*** Абонент ***B,*** в свою очередь, зашифровывает вновь это сообщение также своим первым ключом:

$$m_2 \equiv m_1^{b} (\mathbf{mod}\ p),\ 0 < m_2 < p \qquad (2.5)$$

и пересылает его обратно абоненту ***A.*** Абонент ***A,*** получив обратно свое дважды зашифрованное сообщение, шифрует его же в третий раз своим вторым ключом:

$$m_3 \equiv m_2^{\alpha} (\mathbf{mod}\ p),\ 0 < m_3 < p \qquad (2.6)$$

и вновь отправляет его абоненту ***B.*** Последний расшифровывает эту шифротелеграмму при помощи своего второго ключа:

$$m_4 \equiv m_3^{\beta} (\mathbf{mod}\ p),\ 0 < m_4 < p.$$

В самом деле, из сравнений (2.4) – (2.6) имеем:

$$m_4 \equiv m^{k} (\mathbf{mod}\ p),$$

где $k \equiv a \cdot \alpha \cdot b \cdot \beta (\mathbf{mod}\ p\text{-}1)$.

В силу (2.2) и (2.3) $k \equiv 1 (\mathbf{mod}\ \varphi(p))$. Поэтому $m_4 \equiv m (\mathbf{mod}\ p)$, а так как каждое из них положительно и меньше p, то $m_4 = m$.

Пример 8. Пусть абоненты **A** и **B** решили установить между собой скрытую связь без передачи ключей. Они выбрали для этого простое число p = 9551. Тогда p-1=9550.

Абонент **A** выбирает случайное число a=8159, а абонент **B** – b=7159. Абонент **A** решает сравнение: $8159 \cdot \alpha \equiv 1 (\mathbf{mod}\ \varphi(9551))$, $0 < \alpha < 9550$ и находит α= 6639, а абонент **B** решает сравнение: $7159 \cdot \beta \equiv 1 (\mathbf{mod}\ \varphi(9551))$, $0 < \beta < 9550$ и находит β= 6139.

Абонент **A** решает послать секретное сообщение абоненту **B** m=7032. Тогда он сначала шифрует сообщение своим первым ключом: $m_1 \equiv m^{a} (\mathbf{mod}\ p) = 7032^{81593} (\mathbf{mod}\ 9551) = 153$.

Абонент **B**, получив это сообщение, шифрует его своим первым ключом: $m_2 \equiv m_1^{b} (\mathbf{mod}\ p) = 153^{7159} (\mathbf{mod}\ 9551) = 4896$, и пересылает его абоненту ***A***, который, получив зашифрованное сообщение, шифрует его же в третий раз своим вторым ключом: $m_3 \equiv m_2^{\alpha} (\mathbf{mod}\ p) = 4896^{6639} (\mathbf{mod}\ 9551) = 7577$ и отправляет его абоненту ***B***, который расшифровывает эту шифротелеграмму при помощи своего второго ключа: $m_4 \equiv m_3^{\beta} (\mathbf{mod}\ p) = 7577^{6139} (\mathbf{mod}\ 9551) = 7032$.♦

Пример 9. А теперь рассмотрим похожий пример, но с большими числами, а именно пусть абоненты **A** и **B** выбирают случайное число p =3 6185027886661311069865932815214971204146870208012676262330495002 47285301313. Далее абонент **A** выбирает случайное число a=32910091146 42412084309938365114701009965471731267159726697218119, а абонент **B** – b=72133456729194312009114642445656781208430934647938365165454 65843. Абонент **A** решает сравнение: 3291009114642412084309938365114 70100996547173126715972669721811 9·α≡1(**mod** φ(3618502788666131106 98659328152149712041468702080126762623304950024728530131 3)), 0 < α < 3618502788666131106986593281521497120414687020801267626233049500 247285301312 и находит α=7182890946724276712267540712060414209

9575840582862256961336950427223165477 5, а абонент **B** решает сравнение: 7213345672919431200911464244565678120843093464793836516545465843·β ≡1(**mod** φ(11972621413014756705924586149611790497021399392059391)), 0 < β < 11972621413014756705924586149611790497021399392059390 и находит β= 20507850089479826167721544736489099017840580106896795952493654865076402209 87.

Абонент **A** решает послать секретное сообщение абоненту **B** ***m***=164395308562370233597340474556219234532123890 86. Тогда он сначала шифрует сообщение своим первым ключом: $m_1 \equiv m^a \pmod{p}$= 164395308562370233597340474556219234532123890 86$^{32910091146424120843099383651147010099654717312671597266972181 19}$(**mod** 36185027886661311069865932815214971204146870208012676262330495002472853013 13)=2340488471726089607124556756264169338202290949701335616973062664572414115995.

Абонент **B**, получив это сообщение, шифрует его своим первым ключом: $m_2 \equiv m_1^b \pmod{p}$= 2340488471726089607124556756264169338202290949701335616973062664572414115995^{72133456729194312009114642445656781208430934647938351616545465843}(**mod** 36185027886661311069865932815214971204146870208012676262330495002472853013 13) =2008471523091061336918900208993851807662985672512619192514870979350742436070, и пересылает его абоненту ***A.*** Абонент ***A,*** получив зашифрованное сообщение, шифрует его же в третий раз своим вторым ключом: $m_3 \equiv m_2^{\alpha} \pmod{p}$ =2008471523091061336918900208993851807662985672512619192514870979350742436070$^{7182890946724276712267540712060414209957584058286225696133695042722316547 75}$(**mod** 3618502788666131106986593281521497120414687020801267626233049500247285301313) = 3374267956066404491443963921356203649752330364752225196611392536160948437196 и отправляет его абоненту ***B***, который расшифровывает эту шифротелеграмму при помощи своего второго ключа: $m_4 \equiv m_3^{\beta} \pmod{p}$= 3374267956066404491443963921356203649752330364752225196611392536160948437196$^{20507850089479826167721544736489099017840580106896795952493654865076402209 87}$ (**mod** 3618502788666131106986593281521497120414687020801267626233049500247285301313)=164395308562370233597340474556219234532123890 86♦

3. КРИПТОСИСТЕМА С ОТКРЫТЫМ КЛЮЧОМ

3.1. КРАТКАЯ ИСТОРИЯ ВОПРОСА

В 1976 году американцы Уитфилд Диффи и Мартин Хеллман (Diffi W., Hellman M.) в статье "Новые направления в криптографии" предложили новый принцип построения криптосистем, не требующий не только передачи ключа принимающему сообщение, но даже сохранения в тайне метода шифрования. Эти шифры позволяют легко зашифровывать и дешифровать текст и их можно использовать многократно.

В 1978 г. Р. Ривест, А. Шамир и Л. Адлема (R.L.Rivest, A.Shamir, L.Adleman) предложили пример функции, обладающей рядом замечательных свойств. На ее основе была построена реально используемая система шифрования, получившая название по первым буквам фамилий авторов – система RSA. Рассмотрим ее основные положения на примере криптосистемы с открытым ключом.

3.2. ОСНОВНЫЕ ПОЛОЖЕНИЯ КРИПТОСИСТЕМЫ С ОТКРЫТЫМ КЛЮЧОМ

Пусть абоненты A и B условились организовать секретную переписку между собой с открытым ключом. Тогда каждый из них, независимо от другого, выбирает два достаточно больших простых числа, находит их произведение, функцию Эйлера от этого произведения и выбирает случайное число, меньшее этого вычисленного значения функции Эйлера и взаимно простое с ним. Итак,

$$A: p_1, p_2,\ r_A = p_1 p_2,\ \varphi(r_A),\ (a, \varphi(r_A)) = 1,\ 0 < a < \varphi(r_A),$$
$$B: q_1, q_2,\ r_B = q_1 q_2,\ \varphi(r_B),\ (b, \varphi(r_B)) = 1,\ 0 < b < \varphi(r_B).$$

Затем печатается телефонная книга, доступная всем желающим, которая имеет вид:

A: r_A, a
B: r_B, b

r_A – произведение двух простых чисел, известных только A, a – открытый ключ, доступный каждому, кто хочет передать секретное сообщение A, r_B – произведение двух простых чисел, известных только B. b – открытый ключ, доступный каждому, кто хочет передать секретное сообщение B.

Каждый из абонентов находит свой секретный ключ из сравнений

$a \cdot \alpha \equiv 1 (\mathbf{mod}\ \varphi(r_A)),\ 0 < \alpha < \varphi(r_A),\ \ b \cdot \beta \equiv 1 (\mathbf{mod}\ \varphi(r_B)),\ \ 0 < \beta < \varphi(r_B),$

Итак,

Абонент	Открытые ключи	Секретные ключи
A	r_A, a	α
B	r_B, b	β

Пусть абонент A решает послать сообщение m абоненту B:

A: $m \to B$ и пусть $0 < m < r_B$, иначе текст делят на куски длины r_B.

Сначала A зашифровывает сообщение открытым ключом абонента B, который есть в телефонной книге, и находит:

$$m_1 \equiv m^b (\mathbf{mod}\ r_B),\ 0 < m_1 < r_B,$$

и отправляет абоненту B. Абонент B, расшифровывает это сообщение своим секретным ключом:

$$m_2 \equiv m_1^{\beta} (\mathbf{mod}\ r_B),\ 0 < m_2 < r_B,$$

и получает $m_4 = m$.

В самом деле:

$$m_2 \equiv m_1^{\beta} \equiv (m^{\beta})^b \equiv m^{b\beta} (\mathbf{mod}\ r_B).$$

Но $b \cdot \beta \equiv 1 (\mathbf{mod}\ \varphi(r_в))$, следовательно $m_2 \equiv m (\mathbf{mod}\ r_B)$. Но так как $0 < m < r_B$, $0 < m_2 < r_B$ то $m_2 = m$.

Пример 9. Пусть абоненты **A** и **B** решили установить между собой скрытую связь с открытым ключом.

Абонент **A** выбрал простые числа p_1=7643 и p_2=8753, их произведение r_A=66899179, функцию Эйлера $\varphi(r_A) = p_1 p_2 (1-1/p_1)(1-1/p_2)$=66882784. Затем он выбирает случайное число a=9467 (открытый ключ) и находит секретный ключ из решения сравнения: $a \cdot \alpha \equiv 1 (\mathbf{mod}\ \varphi(r_A)) = 9467 \cdot \alpha \equiv 1 (\mathbf{mod}$ 66882784), $0 < \alpha < \varphi(r_A)$, т.е. α=30993427.

Абонент **B** выбрал простые числа q_1=7481 и q_2=9539, их произведение r_B=71361259, функцию Эйлера $\varphi(r_в) = r_в (1-1/q_1)(1-1/q_2)$=71344240. Затем он выбирает случайное число b=74671 (открытый ключ) и находит секретный ключ из решения сравнения: $b \cdot \beta \equiv 1 (\mathbf{mod}\ \varphi(r_B)) = 74671 \cdot \beta \equiv 1 (\mathbf{mod}$ 71344240), $0 < \beta < \varphi(r_B)$, т.е. β=33289711.

Следовательно имеется таблица:

Абонент	Открытые ключи	Секретные ключи
A	66899179, 9467	30993427
B	71361259, 74671	33289711

Абонент **A** решает послать сверхсекретное сообщение абоненту **B** m=95637. Тогда он шифрует сообщение открытым ключом абонента **B**:

$$m_1 \equiv m^b (\mathbf{mod}\ r_B) = 95637^{74671} (\mathbf{mod}\ 71361259) = 25963634.$$

Абонент **B**, получив это сообщение, расшифровывает его своим секретным ключом:

$$m_2 \equiv m_1^{\beta} (\mathbf{mod}\ p) = 25963634^{33289711} (\mathbf{mod}\ 71361259) = 95637. \blacklozenge$$

Пример 10. А теперь рассмотрим похожий пример, но с большими числами, а именно: p_1=7643 и p_2=8753, их произведение r_A=66899179, $\varphi(r_A) = p_1 p_2 (1-1/p_1)(1-1/p_2)$=66882784, a=9467 и α=30993427. Далее, q_1=17014118346046923173168730371588410572 7, q_2=1035079443105516238671861923746823456 9, b=1826877046663628647754606040895335377456991567871. Тогда имеем: r_B=1761096414255759626214007376557990993955085697884921213758143162998032276663, $\varphi(r_в) = r_в (1-1/q_1)(1-1/q_2)$= 1761096414255759626214007376557990993774593719993396819639737240044679936368. Находим секретный ключ из решения сравнения: $b \cdot \beta \equiv 1 (\mathbf{mod}$

$\varphi(r_B))=182687704666362864775460604089535377456991567871\cdot\beta\equiv 1(\mathbf{mod}$ 176109641425575962621400737655799099377459371999339681963973724 0044679936368), $0<\beta<\varphi(r_B)$, т.е. $\beta=$165135868322368842056118800995582 359759484780795385425947817990598187973011 1.

Таким образом имеется таблица:

Абонент	Открытые ключи	Секретные ключи
A	66899179, 9467	30993427
B	176109641425575962621400737655799099395508 569788492121375814316299803227666 3, 182687704666362864775460604089535377456991567871	165135868322368842056118800995582359759484780795385425947817990598187973011 1

Абонент **A** решает послать сверхсекретное сообщение абоненту **B** $\boldsymbol{m}=$95637123523488976723896413962186095671 72. Тогда он шифрует сообщение открытым ключом абонента **B**: $\boldsymbol{m_1}\equiv\boldsymbol{m}^{b}(\mathbf{mod}\ r_B)=$9563712352348897 6723896413962186095671 72$^{182687704666362864775460604089535377456991567871}(\mathbf{mod}$ 176 109641425575962621400737655799099395508569788492121375814316299 8032276663)=832554716009872190233325937808786727841226137505920445 944782239429736569 48.

Абонент **B**, получив это сообщение, расшифровывает его своим секретным ключом: $\boldsymbol{m_2}\equiv\boldsymbol{m_1}^{\beta}(\mathbf{mod}\ p)=$832554716009872190233325937808786727 841226137505920445944782239429736569 48$^{165135868322368842056118800995582359759484780795385425947817990598187973011 1}(\mathbf{mod}$ 176109641425575962621400737655799099395508569788492121375814316299 8032276663)=95637123523488976723896413962186095671 72.♦

3.3. НАДЕЖНОСТЬ СИСТЕМЫ С ОТКРЫТЫМ КЛЮЧОМ

В рассмотренной криптосистеме с открытым ключом для перехвата сообщения $\boldsymbol{m}$ необходимо найти секретный ключ β. Это возможно в двух случаях:

1) если известно разложение r_B на простые множители;
2) если известен модуль $\varphi(r_B)$ сравнения $b\cdot\beta\equiv 1(\mathbf{mod}\ \varphi(r_B))$.

Но так как $r_B=q_1q_2$, то $\varphi(r_B)=\varphi(q_1)\varphi(q_2)=(q_1-1)(q_2-1)=q_1q_2-(q_1+q_2)+1$ и $(q_1-q_2)^2=q_1^2+q_2^2-2q_1q_2=(q_1+q_2)^2-4q_1q_2$.

Следовательно мы имеем равенства:

$$\varphi(r_B)=r_B-(q_1+q_2)+1,$$
$$(q_1-q_2)^2=(q_1+q_2)^2-4q_1q_2,$$

а значит, зная $\varphi(r_B)$, можно решить эту систему и найти q_1 и q_2, а зная q_1 и q_2, легко вычислить $\varphi(r_B)$. Таким образом, оба подхода определения ключа β эквивалентны, т.е. задачи одной сложности.

В теории чисел, несмотря на многолетнюю ее историю и на очень интенсивные поиски в течение последних 30 лет, эффективный алгоритм

разложения натуральных чисел на множители так и не найден. Конечно, можно, перебирая все простые числа до $(\boldsymbol{r}_\mathbf{B})^{1/2}$, и деля на них $\boldsymbol{r}_\mathbf{B}$, найти требуемое разложение. Но учитывая, что количество простых чисел в этом промежутке асимптотически равно $2\cdot(\boldsymbol{r}_\mathbf{B})^{1/2}\cdot(\ln \boldsymbol{r}_\mathbf{B})^{-1}$, находим, что при $\boldsymbol{r}_\mathbf{B}$, записываемом 100 десятичными цифрами, найдется не менее $4\cdot10^{42}$ простых чисел, на которые придется делить $\boldsymbol{r}_\mathbf{B}$ при разложении его на множители, что при современных возможностях вычислительной техники затянется на долгие годы.

Известны и более эффективные алгоритмы разложения целых чисел на множители, чем простой перебор простых делителей, но и они работают очень медленно.

4. ЭЛЕКТРОННАЯ ПОДПИСЬ

Криптосистема "открытый ключ" неудобна в том смысле, что получатель сообщения не знает, кто является отправителем сообщения. Этого недостатка лишены протоколы "электронной подписи". Рассмотрим их основную идею.

Пусть имеется банкир A и несколько вкладчиков – $\mathbf{B}_1$, $\mathbf{B}_2$, $\mathbf{B}_3$, …. Банкир и каждый из вкладчиков независимо друг от друга выбирают два больших простых числа и держат их в секрете. Пусть $\mathbf{P}$ и $\mathbf{Q}$ – простые числа банкира, p_i и q_i – простые числа вкладчика $\mathbf{B}_i$, $i = 1, 2, 3, \ldots$. Пусть далее $\mathbf{R} = \mathbf{PQ}$, $r_i = q_i p_i$, $i = 1, 2, 3, \ldots$. И пусть банкир выбирает случайно целое число $\mathbf{S}$ с условиями $0 < \mathbf{S} < \varphi(\mathbf{R})$, $(\mathbf{S}, \varphi(\mathbf{R}))=1$, а каждый из вкладчиков также случайно и независимо друг от друга выбирает число s_i с условиями $0 < s_i < \varphi(r_i)$, $(s_i, \varphi(r_i))=1$, $i = 1, 2, 3, \ldots$. После этого публикуется всем доступная телефонная книга:

A: $\mathbf{R}$, $\mathbf{S}$
$\mathbf{B}_1$: r_1, s_1
$\mathbf{B}_2$: r_2, s_2
.....

Далее каждый из них, и банкир и вкладчики, находят свои секретные $\mathbf{T}$, t_i ключи из условий:

$$\mathbf{S}\cdot\mathbf{T}\equiv 1 (\mathbf{mod}\ \varphi(\mathbf{R})),\ 0 < \mathbf{T} < \varphi(\mathbf{R}),$$
$$s_i \cdot t_i \equiv 1 (\mathbf{mod}\ \varphi(r_i)),\ 0 < t_i < \varphi(r_i),\ i = 1, 2, 3, \ldots .$$

Пусть вкладчик $\mathbf{B}_k$ собирается дать распоряжение m банкиру A, и пусть

$$0 < r_k < \mathbf{R}.$$

Последнее неравенство существенно для дальнейшего. Положим для удобства записи $\mathbf{B}=\mathbf{B}_k$, $r=r_k$, $t=t_k$, $s=s_k$. Будем считать $m < r$ и $(m, r)=1$. Вкладчик $\mathbf{B}$ шифрует распоряжение m сначала своим секретным ключом:

$$m_1 \equiv m^t (\mathbf{mod}\ r),\ 0 < m_1 < r,$$

а потом открытым ключом банкира:

$$m_2 \equiv m_1^{\mathbf{S}} (\mathbf{mod}\ \mathbf{R}),\ 0 < m_2 < \mathbf{R}.$$

Банкир A, получив шифрованную телеграмму m_2, расшифровывает ее пользуясь сначала своим секретным ключом $\mathbf{T}$:

$$m_3 \equiv m_2^{\mathbf{T}} (\mathbf{mod}\ \mathbf{R}),\ 0 < m_3 < \mathbf{R}.$$

а потом открытым ключом s вкладчика:

$$m_4 \equiv m_3^{s} (\mathbf{mod}\ r),\ 0 < m_4 < r,$$

и получает $m_4 = m$.

Действительно, так как $m_3 \equiv m_2^{\mathbf{T}} (\mathbf{mod}\ \mathbf{R})$, а $m_2 \equiv m_1^{\mathbf{S}} (\mathbf{mod}\ \mathbf{R})$, то $m_3 \equiv m_1^{\mathbf{TS}} (\mathbf{mod}\ \mathbf{R})$, где $\mathbf{S}\cdot\mathbf{T}\equiv 1 (\mathbf{mod}\ \varphi(\mathbf{R}))$. Если $(m_1, \mathbf{R})=1$, то по теореме Ферма-Эйлера $m_1^{\mathbf{TS}} \equiv m_1 (\mathbf{mod}\ \mathbf{R})$, т.е. $m_3 \equiv m_1 (\mathbf{mod}\ \mathbf{R})$. Но $0 < m_3 < \mathbf{R}$,

$0 < m_1 < r < \mathbf{R}$, следовательно $m_3 \equiv m_1$. Имеем $m_4 \equiv m_3^s \equiv m_1^s \equiv m^{st} (\mathbf{mod}\ r)$, $s \cdot t \equiv 1 (\mathbf{mod}\ \varphi(r))$ и $(m,r)=1$, а значит $m_4 \equiv m (\mathbf{mod}\ r)$, но каждое из них меньше r и больше 0. Следовательно, эти числа равны, т.е. $m_4 \equiv m_1$. Таким образом, банкир *A* получит распоряжение m от вкладчика **B**.

Пример 11. Пусть банкир *A* выбирает простые числа 10243 и 57037. Вкладчик **B** выбирает простые числа 175261 и 817549. Таким образом, $\mathbf{R}=10243 \cdot 57037=584229991$ и $r=175261 \cdot 817549=143284455289$.

Пусть 381259693 и 3387425143 – открытые ключи банкира и вкладчика соответственно.

Находим секретный ключ банкира из условия:

$\mathbf{S} \cdot \mathbf{T} \equiv 1 (\mathbf{mod}\ \varphi(\mathbf{R}))=381259693 \cdot \mathbf{T} \equiv 1 (\mathbf{mod}\ \varphi(584229991)),\ 0 < \mathbf{T} < 584162712.$

Откуда $\mathbf{T}=182938789$.

Далее находим секретный ключи вкладчика из условия:

$s \cdot t \equiv 1 (\mathbf{mod}\ \varphi(r))=3387425143 \cdot t \equiv 1 (\mathbf{mod}\ \varphi(143284455289)),\ 0<t<143283462480$

Откуда $t=111788667367$.

Тогда открытая телефонная книга имеет вид:

A: 584229991, 381259693;

B: 143284455289, 3387425143.

Вкладчик **B** дает поручение $m=134645771$ своему банкиру *A* и замечая, что $\mathbf{R}<r$, шифрует его сначала открытым ключом банкира, а потом своим секретным ключом:

$$m_1 = 134645771^{381259693} \equiv 116030491 (\mathbf{mod}\ 584229991),$$

$$m_2 = 116030491^{111788667367} \equiv 38467700641 (\mathbf{mod}\ 143284455289).$$

Банкир *A*, получив шифрованную телеграмму $m_2 = 38467700641$, и замечая, что $\mathbf{R}<r$, расшифровывает ее пользуясь сначала открытым ключом s вкладчика, а потом своим секретным ключом **T**:

$$m_3 = 38467700641^{3387425143} \equiv 116030491 (\mathbf{mod}\ 143284455289),$$

$$m_4 = 116030491^{182938789} \equiv 134645771 (\mathbf{mod}\ 584229991).$$

А так как $134645771<584229991$, то банкир делает вывод, что 134645771 и есть распоряжение вкладчика. ♦

Пример 12. А теперь рассмотрим похожий пример, но с большими числами, а именно пусть банкир *A* выбирает простые числа **P**=194266889 222572907091946190682351890664240683905213952125181240973890428520520849822 1 и **Q**=198929294563914656862152899258728336040182460318939086976185590757263798805013350213277 7. Вкладчик **B** выбирает простые числа **p**=417184967953302750467777676986240647383340727022783744130281564027777290191531357426359782635 1 и **q**=266998379490113760299377713271194014325338065294581596243380200977777465722580068752870260867081. Таким образом, $\mathbf{R}=\mathbf{P} \cdot \mathbf{Q}$=386453752301725834469535189093198734429892732970643499865723525145151914228956042462678624503308500172665088313240333435082043678656140995027867677682140428067146871028971 7 и $r=\mathbf{p} \cdot \mathbf{q}$=111387710391166875455106728654792268674151086602748045180156067331525272636930600256492012003146814

8253170286172899436920943665754995898474223242784122623243533278
1707353985214366888130251431.

Пусть **S**=123876132205208335762278423601 и **s**=178639387836316
4227858270210279 – открытые ключи банкира и вкладчика соответствен
но.

Находим секретный ключ банкира из условия:
S·**T**≡1(**mod** φ(**R**))=123876132205208335762278423601·**T**≡1(**mod** φ(386537
5230172583446953518909319873442989273297064349986572352514515191
1422895604246267862450330850017266508831324033343508204367865614
0995027867677682140428067146871028971 7)), 0 < **T** < 386 45375230172
5834469535189093198734429892732970643499865723525145151914228956
0424624795009418553629428958434677909227471511969776532966940995
5690568390273883361299996587 20. Откуда **T**=230726595042411533980460
0398128368899935333772682076091680201008526293671242848480878979
9917823868683915465119790318161456991662717340564119766903857227
137940434810257460401.

Далее находим секретный ключ вкладчика из условия:
s·***t***≡1(**mod** φ(***r***))=178639387836316422785827021027 9·***t***≡1(**mod** φ(11138771
0391166875455106728654792268674151086602748045180156067331525272
6369306002564920120031468182531702861728994369209436657549958984
7422324278412262324353327817073539852143668881302514 31)), 0<***t***< 111
3877103911668754551067286547922686741510866027480451801560673315
2527263693060025649201200311970123025332149411903137193956011291
5981326966761840754154941871472646872948983203975427155 8000.
Откуда ***t***=109056550252289161829269902041753432224720341556643787 8
8024777350532831723572544893478202253631321430022366880579196823
4988454323890072579294198446361623371822691409185898377739703441
6153319.

Вкладчик **B** дает поручение ***m***=812341242521515435903200431245
12334367495173751 6 своему банкиру ***A*** и замечая, что **R**<***r***, шифрует его
сначала открытым ключом банкира, а потом своим секретным ключом:
m_1=812341242521515435903200431245123343674951737516^{123876132205208335762278423601}≡248511822777937811551654127521464327437717812899563233066063749613826855197883217523405222393087208805419033892041887892647937592033770628485113897513162317038526866909513 0 (**mod** 38653
7523017258344695351890931987344298927329706434998657235251451519
1422895604246267862450330850017266508831324033343508204367865614
0995027867677682140428067146871028971 7), ***m*****2**=248511822777937811551
6541275214643274377178128995632330660637496138268551978832175234
0522239308720880541903389204188789264793759203377062848511389751
3162317038526866909513 0$^{109056550252289161829269902041753432224720341556643787880247773505328317235725448934782022536313214300223668805791968234988454323890072579294198446361623371822691409185898377739703441615331 9}$≡734897425544020604546917028096311869328177678130575024408820168981154372959237321022592300520039883948751936

807163535166855427900196918680433211395236453568380666048559059355500695895883062 (**mod** 111387710391166875455106728654792268674151086602748045180156067331525272636930600256492012003146818253170286172899436920943665754995898474223242784122623243533278170735398521436688813025143 1), m_4=248511822777937811551654127521464327437717812899563233066063749613826855197883217523405222393087208805419033892041887892647937592033770628485113897513162317038526866909513 0 (**mod** 111387710391166875455106728654792268674151086602748045180156067331525272636930600256492012003146818253170286172899436920943665754995898474223242784122623243533278170735398521436688813025143 1), m_3=734897425544020604546917028096311869328177678130575024408820168981154372959237321022592300520039883948751936807163535166855427900196918680433211395236453568380666048559059355500695895883062$^{178639387836316\ \ 4227858270210279}$≡248511822777937811551654127521464327437717812899563233066063749613826855197883217523405222393087208805410903389204188789264793759203377062848511389751316231703852686690951 30 (**mod** 111387710391166875455106728654792268674151086602748045180156067331525272636930600256492012003146818253170286172899436920943665754995898474223242784122623243533278170735398521436688813025143 1), m_4=248511822777937811551654127521464327437717812899563233066063749613826855197883217523405222393087208805419033892041887892647937592033770628485113897513162317038526866909513 0$^{230726595042411533980460039812836889993533377268207609168020100852629367124284848087897991782386868391546511979031816145699166271734056411976690385722713794043481025746040 1}$≡812341242521515435903200431245123343674951737516 (**mod** 386537523017258344 695351890931987344298927329706434998657235251451519142289560424626786245033085001726650883132403334350820436786561409950278676776821404280671468710289717, то банкир делает вывод, что 812341242521515435903200431245123343674951737516 и есть распоряжение вкладчика. ♦

m_2 = 7348974255440206045469170280963118693281776781305750244088201689811543729592373210225923005200398839487519368071635351668554279001969186804332113952364535683806660485590593555006958958830621 78639387836316 4227858270210279 m3 m4 230726595 0424115339804600398128368899935333772682076091680201008526293671242848480878979917823868683915465119790318161456991662717340564119766903857227137940434810257460401

5. КРИПТОГРАФИЧЕСКИЕ АЛГОРИТМЫ И ЗАЩИТА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

В последнее время защита информации перестала быть задачей только для государственных структур. С нею приходится сталкиваться и многим обычным пользователям персональных компьютеров (ПК). Идя навстречу их пожеланиям, многие производители программного обеспечения ст али включать свои продукты функции защиты данных. Однако в большинстве случаев разработчики не ставят своей целью использовать в них сколько-нибудь стойкие алгоритмы. Они считают своей основной задачей предоставить пользователю возможность защитить информацию либо от случайного несанкционированного доступа, либо от неквалифицированного взломщика. Они, скорее, маскируют информацию, чем реализуют алгоритмы надежного криптографического закрытия. Продемонстрируем данное утверждение на двух программных продуктах.

Многие пользователи используют в работе Microsoft Word. Эта система предоставляет пользователю большой спектр возможностей для работы с документами, в том числе и шифрования информации. Но выбранная в начальных версиях Microsoft Word схема шифрования информации останавливала лишь начинающего взломщика. Рассмотрим ее подробнее.

Из пароля пользователя Word вырабатывает массив длиной 16 байт, называемый гаммой (gamma[0…15]). далее, каждый байт открытого текста (open_text[i]) последовательно складывается побитно (XOR) с байтом гаммы. В результате получается шифрованный текст (cripto_text[i]), который мы можем видеть в файле с паролем, т.е. шифрование производится согласно формуле:

cripto_text[i]=open_text[i] XOR gamma[i mod 16],

где mod 16 – операция получения остатка от целочисленного деления на 16.

Таким образом, перед нами типичный пример криптографической схемы гаммирования короткой гаммой. Так как каждый шестнадцатый символ шифрованного текста получается прибавлением к символу открытого текста одного и того же значения гаммы, можно считать, что мы имеем дело с 16-ю простыми заменами. Для каждой из шестнадцати позиций символа в тексте подсчитаем таблицу частот его значений, после чего выберем в каждой из них значения символа, встретившегося чаще других.

Самый частый символ в документе Word – это пробел (его значение в кодировке ASCII есть 0x20). Следовательно, самым частым символам в таблице частот соответствуют зашифрованные пробелы. Складывая побитно значения этих символов с 0x20, мы получим все 16 знаков гаммы. Далее, зная гамму, расшифровываем весь текст.

На эту очевидную слабость многие обратили внимание. Поэтому фирма Microsoft для версий текстового процессора Microsoft Word, начиная с Word 97, полностью изменила алгоритм шифрования файлов, встроив в него алгоритмы шифрования RC4 и хеширования VD5.

Теперь посмотрим, как защищаются пароли пользователя в операционных системах (ОС) Microsoft Windows 95 первых версий (до OSR 2).

ОС Microsoft Windows 95 не является многопользовательской и не предоставляет возможность пользователям разделять свои ресурсы. Тем не менее, она запрашивает у пользователя при входе в систему его имя и пароль. Но если он ничего не ответит (нажмет кнопку Esc), ОС все равно разрешит ему работать дальше. Но для того, что бы работать в локальной вычислительной сети (ЛВС), где ПК доступны ресурсы или серверы, необходимы соответствующие пароли, причем, возможно, различные. Чтобы пользователю не нужно было их все запоминать, ОС Microsoft Windows 95 записывает пароли для доступа к ресурсам ЛВС в специальный файл с именем "имя_пользователя.pwl". В этом файле данные шифруются на том самом пароле, который система запрашивает у пользователя при его входе в систему. Если пароль введен правильно, то в дальнейшем ОС сама подставляет соответствующий пароль при запросе пользователя на доступ к ресурсам или серверам ЛВС.

Данные в *.pwl файлах шифруются следующим образом. Из пароля пользователя по алгоритму шифрования RC4 вырабатывается гамма. Каждый пароль на доступ к соответствующему ресурсу вместе с некоторой служебной информацией суммируется побитно с полученной гаммой. То есть каждый раз при шифровании используется одна и та же гамма. Если учесть, что *.pwl файл содержит зашифрованную запись, начинающегося с имени пользователя, дополненного до 20 символов пробелами, то задача вскрытия пароля становится элементарной. Получив первые 20 знаков гаммы, мы можем прочитать любой сохраненный в файле пароль (учитывая то обстоятельство, что редко когда используют пароли длиной более 10 символов).

Следует отметить, что сам по себе алгоритм RC4 довольно сложный, и в данном случае использовались слабости не самого алгоритма, а схемы его применения, а именно многократное использование одной и той же гаммы.

ЗАКЛЮЧЕНИЕ

За рамками данной работы остались многие вопросы, такие как генерация случайной последовательности, построение больших простых чисел, распознавание простоты наугад взятого числа, содержащего 125 и более цифр в десятичной записи, генерация ключей и т.д и т.п. Всем интересующихся данными вопросами можно порекомендовать обратиться к соответствующей литературе, часть из которой приведена в списке.

ЛИТЕРАТУРА

1. *Иванов М.А.* Криптографические методы защиты информации в компьютерных системах и сетях. – М.: КУДИЦ-ОБРАЗ, 2001, - 368 с.
2. *Кон П.* Универсальная алгебра. - М.:Мир. - 1968. 351 с
3. *Коробейников А. Г.* Математические основы криптографии. Учебное пособие. СПб: СПб ГИТМО (ТУ), 2002. 41 с
4. *Левин М.* Криптография. Руководство пользователя. - М.: Познавательная книга плюс, 2001, - 320 с.
5. *Левин Максим.* Криптография. Руководство пользователя. - М.: Познавательная книга плюс, 2001, - 320 с.
6. *Молдовян А.А., Молдовян Н.А., Советов Б.Я.* Криптография. – СПб.: Издательство "Лань", 2001, - 224 с.
7. *Смирнов В.И.* Курс высшей математики, том III, часть I – М:. Наука, Главная редакция физико-математической литературы, 1974. 324 с.
8. *Чмора А.Л.* Современная прикладная криптография. 2-е изд. – М.: Гелиос, АРВ, 2002. – 256 с. ил.

ОГЛАВЛЕНИЕ

ИСТОРИЯ КАФЕДРЫ

1945-1966 гг. РЛПУ (кафедра радиолокационных приборов и устройств). Решением Советского правительства в августе 1945 г. в ЛИТМО был открыт факультет электроприборостроения.

Приказом по институту от 17 сентября 1945 г. на этом факультете была организована кафедра радиолокационных приборов и устройств, которая стала готовить инженеров, специализирующихся в новых направлениях радиоэлектронной техники, таких как радиолокация, радиоуправление, теленаведение и др. Организатором и первым заведующим кафедрой был д.т.н., профессор С. И. Зилитинкевич (до 1951 г.). Выпускникам кафедры присваивалась квалификация инженер-радиомеханик, а с 1956 г. – радиоинженер (специальность 0705).

В разные годы кафедрой заведовали доцент Б.С. Мишин, доцент И.П. Захаров, доцент А.Н. Иванов.

1966–1970 гг. КиПРЭА (кафедра конструирования и производства радиоэлектронной аппаратуры). Каждый учебный план специальности 0705 коренным образом отличался от предыдущих планов радиотехнической специальности своей четко выраженной конструкторско–технологической направленностью. Оканчивающим институт по этой специальности присваивалась квалификация инженер–конструктор–технолог РЭА.

Заведовал кафедрой доцент А.Н. Иванов.

1970–1988 гг. КиПЭВА (кафедра конструирования и производства электронной вычислительной аппаратуры). Бурное развитие электронной вычислительной техники и внедрение ее во все отрасли народного хозяйства потребовали от отечественной радиоэлектронной промышленности решения новых ответственных задач. Кафедра стала готовить инженеров по специальности 0648. Подготовка проводилась по двум направлениям– автоматизация конструирования ЭВА и технология микроэлектронных устройств ЭВА.

Заведовали кафедрой д.т.н., проф. В.В. Новиков (до 1976 г.), затем проф. Г.А. Петухов.

1988–1997 гг. МАП (кафедра микроэлектроники и автоматизации проектирования). Кафедра выпускала инженеров–конструкторов–технологов по микроэлектронике и автоматизации проектирования вычислительных средств (специальность 2205). Выпускники этой кафедры имеют хорошую технологическую подготовку и успешно работают как в производстве полупроводниковых интегральных микросхем, так и при их проектировании, используя современные методы автоматизации проектирования. Инженеры специальности 2205 требуются микроэлектронной промышленности и предприятиям–разработчикам вычислительных систем.

Кафедрой с 1988 г. по 1992 г. руководил проф. С.А. Арустамов, за-

тем снова проф. Г.А. Петухов.

С **1997 г. ПКС** (кафедра проектирования компьютерных систем). Кафедра выпускает инженеров по специальности 220500 "Проектирование и технология электронно-вычислительных средств". Область профессиональной деятельности выпускников включает в себя проектирование, конструирование и технологию электронных вычислительных средств, отвечающих целям их функционирования, требованиям надежности, дизайна и условиям эксплуатации. Кафедра готовит также специалистов по специальности 075400 – "Комплексная защита объектов информатизации". Область профессиональной деятельности включает в себя методы, средства и системы обеспечения защиты всех видов конфиденциальной информации.

С 1996 г. кафедрой заведует доктор технических наук, доцент Ю.А. Гатчин.

За время своего существования кафедра выпустила 4037 инженера, из них по специальности 0705 – 2472 чел. и по специальности 0648 (2205) – 1565 чел. На кафедре защищено 50 кандидатских и 9 докторских диссертаций.