О МЕТОДИЧЕСКОМ ОБЕСПЕЧЕНИИ ДИСЦИПЛИНЫ «КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ» (НАПРАВЛЕНИЕ 10.03.01)

КОРОЛЬКОВ Юрий Дмитриевич
доктор физико-математических наук, профессор
ФГБОУ ВО «Иркутский государственный университет»
г. Иркутск, Россия

В статье приведены рекомендации по внедрению в учебный процесс по дисциплине «Криптографические методы защиты информации» серии небольших дополнительных лабораторных работ, которые могут повысить эффективность учебного процесса. Приведены обоснования и примеры таких лабораторных работ. Предложены также дополнительные занятия по смежным вопросам.
Ключевые слова: шифр, шифртекст, ключи шифра, электронная подпись, частотный анализ, зашифрование, расшифрование, сложение по модулю.

В статье рассмотрены отдельные замечания и предложения по преподаванию дисциплины «Криптографические методы защиты информации», которая читается на уровне бакалавриата по направлению 10.03.01 «Информационная безопасность» [2]. Мы здесь не претендуем на полноту или серьезные изменения методов и приемов изложения стандартного курса. Наши предложения направлены в основном на облегчение понимания достаточно сложного материала путем использования упрощенных лабораторных работ. Эти работы являются начальными для соответствующих разделов дисциплины и предваряют переход к лабораторным работам на компьютерной технике. Как показывает наш опыт, современные студенты настолько привыкли к обучению с использованием программного обеспечения, что зачастую не представляют себе, что практически все понятия, встречающиеся в курсе, могут быть изложены и использованы в обычном текстовом виде. Как показывает практика, студенты с любопытством, переходящим в интерес, воспринимают такие подходы. Это приводит к росту уровня понимания предмета перед чисто механическим уровнем использования (см. также [1]).

Перейдем к нашим примерам. Первая лабораторная работа представлена ниже как пример 1. Она предназначена для предварительного ознакомления с шифрами замены перед компьютерными занятиями по криптоанализу этих шифров. Нарочитый разговорный язык и чисто бытовые задачи используются как раз для выхода из привычного дискурса студентов. Лабораторная работа 1 представлена здесь в урезанном виде, вторая часть работы, состоящая из стандартных задач, взятых из известных источников, не приводится, так как не является предметом нашего сегодняшнего рассмотрения.

Пример 1. Лабораторная работа 1. Шифры простой замены.

1. Общие положения. Шифрованием называется видоизменение текста с целью затруднить прочтение. Переход от открытого текста (ОТ) к шифртексту (ШТ) называется зашифрованием, а обратный переход от ШТ к ОТ расшифрованием. Расшифрование всегда должно быть единственным! В состав шифра входят: алфавиты ОТ и ШТ, алгоритмы зашифрования и расшифрования, ключ и др. Ключом называется такая информация про шифр, при участии которой происходит зашифрование и расшифрование и которая должна быть известна только легальным пользователям шифра. Если злоумышленник узнает ваш ключ, то он сможет легко читать и писать ваши ШТ. Ключи шифра нужно менять как можно чаще.

2. Простейшие типы шифров. К ним относятся шифры замены и шифры перестановки. Это симметричные шифры, то есть у которых ключ для зашифрования и для расшифрования один и тот же. Исторически это самые первые и самые распространенные шифры. Зашифрование в шифрах замены

происходит заменой частей ОТ другими наборами символов. Если замены идут побуквенно, то такие шифры замены называются шифрами алфавитной или простой замены. Шифры перестановки реализуются перестановками имеющихся символов по какому-нибудь алгоритму, зависящему от ключа. Во всех симметричных шифрах отдельными кирпичиками выступают шифры замены и шифры перестановки.

3. Шифр Цезаря. В шифре Цезаря замена букв текста производится на буквы того же алфавита, но с некоторым сдвигом. Этот сдвиг является ключом Ш. Цезаря. Зашифруем Ш. Цезаря с ключом +2 ОТ(екст) «МЯСОСЪЕЛИ». Алгоритм зашифрования заключается в замене каждой буквы ОТ на букву, которая имеет номер на 2 больше. В нашем случае буква М будет заменена на букву О (М-Н-О), буква С – на букву У, буква О – на букву Р, и т. д. А вот буква Я будет заменена на букву Б (в алфавите идем по кругу, после Я снова А!). В результате из ОТ «МЯСОСЪЕЛИ» с ключом +2 получится ШТ «ОБУРУЬЗНК» (как обычно, буквы Е и Е отождествляют). При расшифровании из ШТ «ОБУРУЬЗНК» однозначно получится ОТ «МЯСОСЪЕЛИ», если использовать ключ +2 для уменьшения номера букв ШТ на 2!

4. Задание 1. а) Зашифровать тот же ОТ «МЯСОСЪЕЛИ» шифром Цезаря с ключами +3, +20, -10. б) Зашифровать полученный в предыдущем пункте ШТ по ключу +3 ЕЩЕ РАЗ с ключом +17. Что и почему так получилось? в) Расшифровать ШТ Цезаря с ключами: «Р Я Р Г Х Т С Й Й П М», +4; «Х Ч Р Ъ А Э Б Ф Ж Г», +21; «Б Ф Ж В Г Ъ Ц А У Щ Г», -11; г) Как вы объясните полученные в предыдущем пункте результаты? д) Сколько разных ключей существует для шифра Цезаря? е) Угадать ключ и расшифровать: «Я И Д Э Б Ф Ж Х». Используется алфавит на 32 буквы, где Е=Е.

5. Частотный анализ текстов. Частотой буквы в тексте называется отношение количества экземпляров этой буквы в заданном тексте к общему количеству букв в этом тексте. Например, частота буквы О в слове МОЛОКО равна 0,5, а частоты букв М, Л и К равны по 1/6. Одна и та же буква в разных текстах имеет разные частоты, однако эти частоты близки по величине, особенно в длинных текстах. Например, в русском языке самыми частыми буквами являются О, Е, А, И. На этом основан частотный анализ шифртекстов, полученных шифрами простой замены. Дело в том, что такие шифры сохраняют частоты букв, хотя и заменяют их другими буквами. Например, если зашифровать ОТ «МОЛОКО» шифром Цезаря с ключом +1, то получится «НПМПЛП», опять у одной буквы частота 0,5, это буква П, полученная из О заменой. На этом основан частотный анализ шифртекстов у шифров простой замены, позволяющий прочесть ШТ, не зная ключа. Или вычислить ключ. Частотный анализ позволяет взломать шифр.

6. Задание 2. а) Если в примере ШТ Цезаря «НПМПЛП» предположить, что буква П получена заменой из буквы Е, либо из А, либо из И, то какие варианты прочтения ОТ возникнут? б) С помощью частотного анализа вычислите ключ шифра Цезаря и прочтите ШТ: «О Я М Н П Я Л Я», «Х Ф Ш Ж П Й Л Ы Ф К О С О Й Ф С Ф И Ф Ц Л Н Б», «О Й Е Н Р М Л К Е П З В К Е Ц В Й Р». Алфавит на 32 буквы. Конец примера 1.

Просим обратить внимание, что в примере 1 достаточно быстро осуществляется переход о простейших примеров к вполне важным вопросам частотного анализа. Нам кажется, что у нас здесь не происходит большой потери учебного времени на простые отвлечения.

Следующий пример 2 похож на пример один, но там переход к существенным вопросам происходит достаточно быстро, хотя нестандартный язык остается до конца примера.

Пример 2. Лабораторная работа 2. Шифры перестановки и гаммирования.

1. Шифры перестановки. Как видно из названия, шифрование для этих шифров сводится к перестановкам имеющихся букв открытого текста (ОТ). Например, перестановка букв для очень известного слова «САОМВК» несколько затрудняет прочтение. Вопрос 1. Что является ключом и что является алгоритмом зашифрования и алгоритмом расшифрования для шифра перестановки? Исторически шифры перестановки использовались намного реже, чем шифры замены. Это вызвано тем, что шифры перестановки имеют принципиальный недостаток: у стойкого для прочтения шифра пере-

становки длина ключа должна быть близка к длине ОТ, а этот факт практически лишает смысла само шифрование перестановкой. Роль шифров перестановки в теории и практике шифрования заключается в другом: с помощью комбинирования шифров замены и перестановки получаются наилучшие современные симметричные шифры.

2. Шифр вертикальной перестановки. Рассмотрим один из известных шифров перестановки. Для уменьшения длины ключа, сначала нарежем ОТ на отрезки небольшой одинаковой длины, а потом будем переставлять буквы в каждом таком отрезке одинаково. Тогда размер ключа будет равен размеру отрезков, а не размеру самого ОТ (почему?). Если мы сложим эти отрезки вертикальной стопкой друг на друга, то, переставляя буквы в каждом отрезке одинаково, мы тем самым получаем перестановку вертикальных столбцов (см. диаграмму). Пример 1. Пусть дан ОТ «ВЕРТИ|КАЛЬН|АЯ», уже нарезанный на отрезки по 5 букв. Обратите внимание, в последнем отрезке всего 2 буквы, потому что количество букв в ОТ не кратно 5, так часто бывает. Придется дополнять последний отрезок, например, тремя тире (-), чтобы подравнять длины. Теперь выкладываем вертикальную стопку из этих отрезков.

3. Задание 1. а) Задайте какой-нибудь ОТ букв на 15-20 и зашифруйте его двумя разными вертикальными перестановками с разным количеством столбцов, передайте на расшифрование соседу и получите от него подобное же задание. Оба сделайте и убедитесь, что все получилось правильно. б) Прочтите шифртексты вертикальных перестановок, не зная ключей: «ИЛПРАОАМ»; «ОАВРПЕЗХУО-Л- -А».

4. Шифр гаммирования. Он похож на шифр Цезаря, только каждая буква при зашифровании сдвигается на разные сдвиги. Делается это так. Задается не очень длинный текст – гамма – и подписывается под ОТ подряд столько раз, пока не кончится ОТ, затем ОТ складывается побуквенно с гаммой по модулю 32. В нашем примере ОТ есть «О Н П О Ш Е Л В Т Е А Т Р», гамму мы выбрали слово «Б А Р».

Сложение по модулю 32 двух чисел: если сумма меньше 33, то она остается, если сумма больше 32, то из суммы нужно вычесть 32.

Обратите внимание вот на какую особенность шифра гаммирования на этом же примере. При зашифровании буквы ОТ с номерами 1, 4, 7, 10, 13, … складываются с буквой Б гаммы. Буквы ОТ с номерами 2, 5, 8, 11, … складываются с буквой А гаммы. Буквы ОТ с номерами 3, 6, 9, 12, … складываются с буквой Р гаммы. Таким образом, шифр с гаммой длины 3 расщепляется на три шифра Цезаря, в данном примере со сдвигами 2, 1 и 17. Это помогает взламывать шифр гаммирования, если известна длина гаммы. Длину гаммы можно и не знать, а действовать перебором. Рано или поздно, наткнемся на правильную гамму и прочтем ОТ.

5. Задание 2. а) Задайте какой-нибудь ОТ букв на 15-20 и зашифруйте его двумя разными гаммами, передайте на расшифрование соседу и получите от него подобное же задание. Оба сделайте и убедитесь, что все получилось правильно. б) Прочтите шифртекст гаммирования, зная только, что длина гаммы равна 3 (взломать): «СПХРМСМЮХРДСНПЕВ».

6. Шифртекст «К А Л А А Ш Ш О У С И С А Л С А И Е С О О П С Ш Ш С» получен из исходного сообщения перестановкой его букв, а шифртекст «А Б В Г В А В Д Е А Е Г Г Э Ю Г Е Г В Б В Г Ш А С Ю» получен из того же исходного сообщения простой заменой. Восстановите исходное сообщение. Конец примера 2.

Лабораторная работа 2 также приведена в обрезанном виде по тем же причинам.

Третий пример хотя и получен тем же приемом упрощения и даже опрощения текстов заданий, но преследует несколько другие цели. Здесь нам было важно не только попытаться достичь дополнительного понимания новых понятий и новых задач, но и на ручной работе с обычными текстами выработать требуемые навыки наложения, снятия и проверки электронной подписи. Навыки вырабатываются на очень упрощенной схеме электронной подписи с примитивным шифрованием, но с полным сохранением последовательности действий, составляющих процессы наложения, снятия и проверки электронной подписи и их содержания.

Пример 3. Лабораторная работа 3. Электронная подпись.

1. Общие положения. Сначала выдержки

из Федерального закона Российской Федерации от 6 апреля 2011 г. N 63-ФЗ «Об электронной подписи»: Для целей настоящего Федерального закона используются следующие основные понятия: 1) электронная подпись – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию. 5) Ключ электронной подписи – уникальная последовательность символов, предназначенная для создания электронной подписи; 6) ключ проверки электронной подписи – уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи (далее - проверка электронной подписи).

В п. 1, в частности, сказано, что эл. подпись (ЭП) неотделима от подписываемого эл. документа. Точно так же собственноручная подпись на бумажном документе неотделима от него без нарушения целостности. В п. 5 подчеркивается, что ключ ЭП – это не сама ЭП. В п.6 подчеркивается, что ключ проверки ЭП однозначно связан с ключом ЭП, но они отделены друг от друга. Например, зная один из ключей практически невозможно вычислить второй. Поэтому ключ ЭП, хранящийся в секрете у владельца, нельзя вычислить по ключу проверки ЭП, который может сообщаться любому лицу. Такие ключи создаются сложной математикой на серьезных устройствах, что в наших занятиях недоступно. В этой лаб. работе мы будем практиковаться в создании (наложении) ЭП на эл. документ и в проверке ЭП. Под документом будем понимать любой открытый текст (ОТ) в алфавите на 32 буквы.

2. Хэш-функции – это такие особые функции, которые, получая на входе ОТ произвольных размеров, дают на выходе небольшие тексты фиксированной длины (у нас будут 3 буквы). Главная особенность хэш-функций – умение различать ОТ даже на небольшом количестве букв. Мы будем использовать следующую упрощенную хэш-функцию Н(ОТ). Сначала разделим ОТ на отрезки по 3 буквы (последний может быть 1 или 2 буквы), затем начинаем сложение трехбуквенных слов по модулю 32 по схеме: 1-й отрезок складываем со 2-ым, получатся снова три буквы, их складываем с 3-им отрезком ОТ. Что получится, складываем с 4-ым отрезком ОТ и т.д., пока не закончатся отрезки ОТ. В итоге останутся три буквы, которые и будут являться значением хэш-функции Н(ОТ). Пример. ОТ = «ВЫДАТЬТРИРУБЛЯ». Разделим: ВЫД-АТЬ-ТРИ-РУБ-ЛЯ. Складываем по очереди по модулю 32: ВЫД+АТЬ = ГОБ; ГОБ+ ТРИ = ЦЯК; ЦЯК+РУБ = ЗРМ; ЗРМ+ЛЯ = ЗЬМ. Значение хэш-функции на данном ОТ равно «ЗЬМ».

3. Задание 1. Вычислить хэш от текстов «ВЫДАТЬДВАРУБЛЯ», «ВЫДАТЬЧЕТЫРЕРУБЛЯ».

4. Создание ключей ЭП. Каждый студент создает для себя два ключа: ЭП и проверки ЭП. Ключ ЭП (секретный) – это любые три буквы. Ключ проверки ЭП (открытый) – это три буквы, дополняющие буквы ключа ЭП до 32 (до Я). В сумме по модулю 32 два ключа должны давать ЯЯЯ. Например, если ключ ЭП = УБЮ (20-2-31), то ключ проверки будет ЛЭА (12-30-1), УБЮ+ЛЭА = ЯЯЯ.

5. Задание 2. Каждому создать свои два ключа: ключ ЭП и ключ проверки ЭП.

6. Наложение и проверка ЭП. **Наложение ЭП:** берется ОТ, вычисляется хэш от ОТ, к хэшу прибавляется по модулю 32 ключ ЭП. Пример. ОТ = «ВЫДАТЬТРИРУБЛЯ», хэш равен ЗЬМ, ключ ЭП пусть УБЮ, хэш плюс ключ ЗЬМ+УБЮ = ЫЮЛ (это и есть ЭП). **Посылается соседу:** ОТ = «ВЫДАТЬТРИРУБЛЯ», ЭП = ЫЮЛ, ключ проверки ЛЭА. **Проверка ЭП:** вычисляется хэш от ОТ (ЗЬМ), к ЭП прибавляется по модулю 32 ключ проверки ЭП (ЫЮЛ+ЛЭА = ЗЬМ), полученная сумма сравнивается с хэш от ОТ. Если они совпадают (как в нашем примере), то делаем ДВА вывода: а) текст не подделан; б) подписан действительно тем, кто послал. Если не совпадают, то либо текст не тот, либо подпись не та.

Внимание! Документ посылается в открытом виде, учтите, что ЭП не предназначена для шифрования документа!

Задание 3. а) Наложить свою ЭП на три текста из примера п.2 и задания 1 (про рубли) и послать соседу. б) Проверить три ЭП, полученные от соседа про рубли. в) Наложить свою ЭП на СВОИ тексты и послать соседу. г) Проверить новые ЭП, полученные от соседа.

Кроме этих трех примеров мы предлагаем и другие небольшие дополнения к стандартному изложению материала дисциплины. Во-первых, это добавление в самом начале следующих разделов: повторение теории чисел в части вычислений по модулю (как простого, так и составного модуля), вплоть до дискретного логарифмирования и сопутствующих теорем. Во-вторых, повторение следующих начальных разделов абстрактной алгебры: теории групп, в основном абелевых, теории колец, в основном коммутативных, теории конечных полей. В третьих, особенностей работы с большими числами и рядами, в том числе с большими простыми числами.

Последнее, что хочется добавить это желание внедрить простейшие вспомогательные программы для ЭВМ, которые позволяют облегчить и ускорить вспомогательные же вычисления частот букв, поисков и запоминаний сделанных и отмененных подстановок и других вычислений в текстах при изучении взломов простейших шифров. Мы такие программные средства создали и внедрили, однако это выходит за рамки этой статьи.

В заключение вместо выводов предлагаем защитить следующие положения.

Смело внедряйте небольшие вставки, помогающие студентам в понимании нового материала и приобретении новых навыков, небольшая потеря времени окупится выросшей скоростью приобретаемых навыков и умений.

Смело внедряйте небольшие программы для ЭВМ, позволяющие экономить время на вспомогательных и не принципиальных вычислениях и расчетах.

Мы для защиты этих положений представляем некоторый опыт преподавания.

СПИСОК ЛИТЕРАТУРЫ

1. *Буйневич М.В., Матвеев А.В., Смирнов А.С.* Актуальные проблемы подготовки специалистов в области информационной безопасности МЧС России и конструктивные подходы к их решению // Научно-аналитический журнал «Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России». – 2022. – № 3. – С. 1-17.

2. ФГОС ВО 10.03.01 Информационная безопасность (Уровень бакалавриата). – URL: http://www.consultant.ru/document/ cons_doc_LAW_209323/ d47286fd71b f546c93cf728b97 aa6758d2277aca/ (дата обращения: 21.10.2022).

ABOUT THE METHODOLOGICAL SUPPORT OF THE DISCIPLINE «CRYPTOGRAPHIC METHODS OF INFORMATION PROTECTION» (DIRECTION 10.03.01)

KOROLKOV Yury Dmitrievich
Doctor of Physical and Mathematical Sciences, Professor
Irkutsk State University
Irkutsk, Russia

The article contains recommendations for introducing a series of small additional laboratory works in the educational process on discipline «Cryptographic methods of information protection», which can improve the effectiveness of the learning process. Reasons and examples of such laboratory works are given. Additional classes on related issues are also offered.

Key words: cipher, ciphertext, cipher keys, electronic signature, frequency analysis, encryption, decryption, modulo addition.