ТИ.Вторая лабораторная..aac

Симметричная криптосистема. Могу вам рассказать почему. Бывают симметричные, бывают асимметричные. Потоковые атмосферы симметричные.

Потому что один ключ. Операция используется одна и та же. И при шифровании это исключающая операция. Значит, поскольку шифрование у нас либо обычно по битовой, это бывает по байтовой, например, 24, потом по фаршевой прямой, то ключ должен быть равен длине шифрованной информации.

А если шифруемая информация у нас длинная, то ключ будет довольно длинный. Передавать такой ключ небезопасно, поэтому придуманы разные способы задания всех случайных последователей. Один из них это регистрирование с обратной связью, вернее, и вы его будете реализовывать в своей работе. Значит, недостаточно, чтобы наши программы просто расшифровали и расшифровали.

Это еще неправильно. Если вы будете так тестировать свою программу, то это еще не значит, что я вас не отправлю переделывать. Самая важная, основная часть вашей работы, да, это правильно запрограммировать работу регистра гений-моды с обратной связью. Для этого, чтобы проверить, я буду проверять каждый регистр, вы даете определенному его, этого регистра, именно битовую последовательность.

Если битовая последовательность у вас генерируется неправильно, значит, либо вы неправильно что-то делаете, либо неправильно вы вводите, такое тоже бывает, но в любом случае, придя сюда, вы должны протестировать свою программу, проверить работу с битового регистра. Если вы это не сделаете, сделаем, значит, вашу проблему. Да, кто это пришел? Машина. Машина.

Откройте, пожалуйста, теорию, где у нас потоковые шифры, там же у нас ревизтор. Значит, у каждого из вас будет дан примитивный многочлен, из которого вы будете брать нужную информацию для того, чтобы запрограммировать работу регистра. Значит, многочлен называется примитивным и должен быть примитивным для того, чтобы последовательность, генерируемая данным регистром, построенная на базе этого многочлена была максимальной.

Но, если регистр будет генерировать последовательность в каким-нибудь не очень большим периоде, то в какой-то момент времени наша последовательность через период начнет повторяться, правильно? Что, если содержать преднастойкости, подвергает злоупотреблённый текст. Поэтому задача, чтобы регистр генерировал как можно большую последовательность, большую длину. Для этого они должны быть примитивные, но и как можно длиннее сами регистры должны быть.

Но длина регистров не бесконечна, поэтому существуют и другие способы. Комбинация регистров, да, чтобы пленнее наступать и увеличить период. Программы rt4. Все это вот эти два способа у вас описаны. Кто хочет по центру повыше, значит, должен узнать. Мы реализовываем только регистр 1. Вот, значит, открыли, да? Смотрим. Вот у вас там написано, что полином у нас x4 плюс x плюс 1.

Нашли?

Нашли. Теперь, смотрите. Максимальная степень полинома задает длину регистра, то есть количество ячеек. Вот у нас 4 таких кубика, прямоугольника, на короткую сторону нарисованную, да? Есть. Дальше. Степени при х задают обратную связь. То есть те ячейки, с которых мы будем доставать содержимое, их содержимое и выполняете операцию, включая ячейки.

В данном случае это 4 и 1. Правильно? Правильно. Так, почему редиктор называется сдвигом из линейной обратной связи? Потому что на каждом шаге содержимое каждой его ячейки сдвигается. Теперь обратите внимание, если сдвигать можно влево, можно вправо, это не имеет значения, но мы с вами будем сдвигать влево, вот как у вас в примере. Если ваш алгоритм будет сдвигать вправо, Значит, я скажу, что неправильно, поставлю минус балл, и вы ровно пойдете переделывать.

Потому что, ну, общее занятие для того и существует, чтобы я вам постаралась сделать постановку задачи. Значит, сдвигаем влево. Ну, вот, сдвигаем влево. То есть, например. Сдвигаем влево и, ну, прежде чем сдвинуть, нужно достать, в данном случае, из четвертой и первой ячейки содержимое, сксорить.

Дальше сдвигаем каждую ячейку, то есть четвертая ячейка выйдет уже, содержимое четвертой ячейки вытолкнется из регистра, это уже будет первый бит ключа. Содержимое третьей запишется в четвертую, вторую в третью, первую во вторую. Ну и первая как-то освободится. И в первую мы заносим результат нашего ксора.

Итак, будем на каждом шаге делать столько раз, сколько нам нужно для того, чтобы сгенерировать ключ для шифрования Ваша эта функция или метод, что там у вас будет, согласно вашему языку, да, должна вызываться на этапе шифрования, когда вы шифруете очередной байт, например, да, то есть байт взяли для шифрования, 8 бит вы сейчас генерировали, дальше пошли. Не надо так делать, как делают некоторые. Неправильно берут содержимое всей ячейки, например, всего регистра, например, 37, сразу записывают в выходной ключ.

Неправильно, потому что если нам зашифровать нужно только один байт, то куча будет лишняя, нам не нужная, правильно? Нет, мы должны генерировать столько ключа, сколько нам нужно. Вытолкнуть столько бит ключа, сколько нам нужно. Вот. Итого. Допустим, наш регистр будет заполнен всеми единицами. Заполнен. Значит, мы достанем, для этого принома, достанем из четвертой единицу, достанем из первой единицы, с XOR получится 0.

Дальше из четвертой пойдет бит ключа в ключ 1, из третьей получится в четвертую 1, из второй в третью 1, и в первую мы запишем 0. На следующем шаге из четвертой достанем 1, 1 достанем в ноль, ссорим, получим единицу, из четвертой вытолкнем в ключ, вторая единица будет, из третьей запишем четвертую единицу, из второй в третью единицу, из первой в вторую в ноль, и в первую запишем единицу.

Вот. Если у нас полином примитивный, у нас примитивный, то период регистра будет равен 2 степени, а m это у нас длина регистра, то есть параметра ячеек, минус 1. То есть для данного полинома период будет очень маленький. То есть через 15 шагов у нас все начнет повторяться. Ничего мы не сможем зашифровать данного, да? Как работает? Я понятно объяснила, как регистр работает? Все нормально, да? Тогда можно, наверное, переходить к объяснению, что вам нужно сделать.

Смотрите, еще раз озвучиваю, что ваша программа должна быть консольная, и ваша программа обязательно должна шипровать и дешипровать файлы с любым расширением, с любым содержимым, будь то текстовые, звук, видео, картинка, любые. Соответственно, не для того, чтобы проверить, я прошу выводить в битом виде, и это зависит от языка программирования, например, на битоне, либо в Delphi, там, в окно, это выводится очень медленно.

Поэтому, если вы дома не протестируете, он приходит сюда, начинает тестировать, а ваша программа выяснит 5 минут, там, шифрует там совсем небольшой файл. Поэтому вы должны либо реализовать так, чтобы ваша программа работала быстрее, да, протестировать, либо на экран можно выводить не все содержимое файла, если вы видите, что ваша программа объяснит, вы никак не способны сделать, чтобы она работала быстрее, да, а часть какую-то.

Значит, что нужно вводить? Вот у вас есть длина регистра, например, 37. В этой стене мы заполнили 7 единиц, поэтому вывести на экран нужно вот это 37 два раза. То есть две длины регистра первых и две длины регистра последних. Поняли, да? А по серединочке уже можно не вводить. Это вот, например, в исходном файле то же самое включили, то же самое в зашифрованном файле.

И вы должны проверить, что у вас нигде не сбивается, потому что они проверяют, я начинаю проверять сор, а он не совпадает. А почему? Вроде все правильно, а на самом деле при выводе бит получается сбой. То есть все это вы должны оттестировать. Чтобы я брала, например, бит ключа единица, бит исходной информации на той же позиции единица, и в ключе должен быть ноль, а не единица. Вы должны это все проверить и тестировать.

Итого, что должно быть в вашей программе? Запускаем. Должно быть поле для ввода ключа в битомомбиле. Значит, если мы введем последовательность короче или длиннее нашего регистра, программа не должна вылетать с ошибкой. Она должна либо попросить ввести заново, либо не пускать, сделать больше-меньше.

И если мы введем что-то кроме нулей и единиц, тоже программа не должна вылетать с ошибкой. Все. Дальше. Кнопка с диалоговым окном «Выбрать нужно файлик», с любым расширением выбираем. После нажать «Зашифровать», что у нас должно произойти? Ну, либо, когда уже выбираем файл в основной этапе, после того, как выбрали, содержимое исходного файла в виде нуля или единицы выводится в специальное поле на экране.

Таких файлей должно быть три. Не в файле, обращая ваше внимание, а на экране, потому что так будет быстрее. И когда вы ко мне будете подходить, уже будет что-то загружено, у вас запущено, я не буду ждать, пока у вас там будет преобразовываться. Вот, вы ее нажали зашифровать, выводится в поле там, где ключ, биты ключа. Обращаю ваше внимание, что выводятся биты ключа, а биты ключа это то, что вытолкнулось из регистра, straighten out, а не состоянии регистра.

Некоторые начинают выводить на каждом шаре состояние регистра. Если вам нужно на каждом шаре состояние регистра, вы можете дома выводить для своего тестирования. Мне состояние режима вашего не нужно. И не надо мне здесь сидеть и доказывать, что это тоже правильно. Understand? Я прошу вас выводить BIT и ключа, мне состояние регистра не нужно. Состояние регистра вашего я увижу в вашей таблице, которую вы должны сделать.

Понятно? Понятно. Не надо кучу пространства тратить на регистры, где я должна буду встать в ключ, и встать, и непонятно где, если он длинный. Вот. Битов ключа должно быть столько, сколько вы вывели битов исходной информации шифровой. И в третьем поле выводятся биты зашифрованной информацией, тоже ровно столько, сколько у нас было исходного текста, скажем так, и ключа.

Что должно записаться на диск? А на диск должен записаться файлик, то есть мы вывели на экран его содержимое, да, что должно записаться на диск. Чтобы потом, когда мы захотим дешифровать, не к этому сразу захотим дешифровать, а может мы через длинный захотим дешифровать, правильно? У нас был файл. Значит, что в этом файлике должно лежать? В этом файлике должны лежать не нули и единицы, а в этом файлике должны лежать, то есть туда поток байта записан.

Записали. Дальше. Мы решили расшифровывать. Как будет расшифровка происходить? Расшифровка будет происходить в обратном порядке. Ну, как в обратном. Точно так же, да. Ключ возим. Все. Делаем все проверки. Если ключ ведем неправильно, значит ничего у нас не должно дешифроваться, да? Выбрали файлик опять. Все. Выявили в битовом виде содержимое. Назвали дешифровать. Все. Опять выявили в битовом виде. И на диск записался файлик, уже наш расшифрованный, тоже по киллбайкам, да.

Хотите сразу, можете решение подставлять, хотите, потом уже вручную находим его на место, да. И когда мы запускаем этот файлик, он должен открыться, сыграть на содержимое. Ну, если там будет текст, значит, мы должны прочитать текст, который точно такой же должен быть, в соответствии с региональным. Ну, если была картинка, значит, картинка. Музыка, значит, музыка. Видео, значит, видео.

Так. Вы должны с собой принести обязательно файлики с разным расширением, на которых вы будете демонстрировать работу своей программы.

Текстовые, видео, аудио, картинка, и протестировать, что ваши программы на них виснуть не будут. Теперь, смотрите, если у нас ключ будет все-все нули, то что у нас произойдет, когда мы должны нашифровать? Ну, просто все, вы посмотрели? Ничего не зашифровали, да? Поэтому все нули в ключе быть не должны, Но вы не ставьте защиту, пускай программа ваша разрешает ввести все нули, я все равно буду смотреть, как у вас работает со всеми нулями, но вы должны знать, что все нули, такой ключ нам не нужен.

Потом, потом, потом. Ну и, естественно, протестируйте, как ваша программа будет работать, например, когда один символ или два символа появятся. На экран вывестись должно ровно столько, сколько у нас байт с шифровым. Здесь это было 2, 2×8, 16. Они все содержимые регистра. Вот. Теперь, что плюс к программе у вас должно быть? Ну, парики тестируете, которые тестируете, которые вы носите. И вот эта табличка, которая примет.

У каждого там сверху будет свой регистр. Заполняем 7 единицами, потому что на всех единицах проще всего отследить. И какой длины должна быть эта табличка? Две длинные регистры. Ну, естественно, вы должны знать, что из теории, когда вы спрашиваете. Какой укрытая система, что потоковая, что она симметричная, формулы шифрования и дешифрования.

Из гефе ключик этот длинненький, который генерируется схемой гефе, да, что такое последовательность, то есть максимально, максимально последовательность, максимально возможно для заднего регистра последовательность является, вот, и должны уместиться, естественно, должны знать операцию XOR, да, я напишу какие-то примерчики вместо XOR'а, и напишу какой-нибудь такой богенький, ну, линейный,

Скажу вам, что это регистр и попрошу, ввиду ячейки, которые будут участок в обратной связке, попрошу три шага, например, показать, отобразить три шага работы регистра. То есть, на каждом шаге состояние регистра и три битовых участка регистра. Так, вопросы пока возникли, не возникли? Возникли, а вот если открывать очень большие файлы, долгие видео…

Даже вам это сказала уже. Вы слушали? Я говорила, если вы открывать будете, самая большая тормоза начинается на этапе конвертации в битовую форму, правильно, или единице. Поэтому выводить можно не весь файл, правильно, а частями. Какими частями я вам тоже сказала, не меньше двух длинного регистра, сначала и с конца. Всё, тогда это ускорит процесс.

Опять-таки, вы принесете свои файлы, не приносите очень большие. Зачем нам очень большие, чтобы ваша программа висла, правильно? Вы должны подобрать такие файлы адекватные, чтобы ваша программа не висла. Вот. Еще какие вопросы возникли? Нету пока вопросов. Тогда идем дальше. Теперь подходим к тому, что вы мне должны прислать. Ну, первое еще раз возвращаюсь.

В теме письма теперь указываем номер группы и номер лагу. Дальше, прикрепляем на гит-хаб еще раз, озвучиваю. Хотелось сдвинуть, конечно, этот лайнер 21.0, так я уже притомилась до вечера уловить ваши усилаторы. Не знаю, ладно, пока еще потерплю. Может быть, сдвинуть на следующий лайнер, потому что, ну, все уже.

Пока у нас же длайн 21.00 на кануне, так? Так, опять-таки озвучиваю. Если вас отправили там раньше-раньше, да? У меня зависит от расписания. Бывает, что неделя у меня более-менее свободная, я тогда сразу проверяю. Каждый день проверяю, чтобы не накапливалось. А бывает, что у меня каждый день, например, 4 разные группы, и 4 группы мне до 21-го на нахидают лад, представляете? Или у меня там почтовый ящик.

Поэтому я проверяю, буду проверять именно тех, у кого на завтрашний день ЛАГО, правильно? Поэтому ваши ЛАГО могут лежать, бывает, что неделю лежат, в зависимости от того, кого вы мне расписали. Поэтому не надо мне слать постольно ничего, оно там лежит, это не значит, что я не получила. Просто у меня нет времени, я занята другими группами, другими предметами. Вот. Опять-таки озвучиваю. Если я вот сделаю какое-то замечание, а вы мне отвечаете, отвечать в теме письма, опять же, должна только быть моя группа, больше ничего, вы должны видеть это, чтобы меня не лазить взглядом.

Все, дальше, что мы вложим на гитхаб? На гитхаб, еще раз озвучиваю, что это должна быть прямая ссылка, чтобы я людей не лазила, не искала, должен быть связь ваш проект. И плюс к проекту для данной работы должна быть вот эта вот текстовая фарма в орде, наверное, да, табличка, да, работа регистра.

Обязательно она должна быть правее, сгенерируют. Ваши программы такую последовательность не генерируют, потому что приходят сдавать, я сначала проверяю эту табличку, там все правильно, потом садимся и начинаем тестировать программу, а программе неправильно. Что это такое вообще? Как такое может быть? Я не представляю. Ну, мы что-то там написали. Надо же проверить. А правило программы работает элементарно. Вот. И вы должны положить мне еще плюс к этому текстовому парусу таблички вашей.

Скрины работы программы. Теперь будем думать, что должно быть в этих скринах. Ну, во-первых, должны быть… Короче, на этих скринах я должна увидеть обязательно… Пускай будет много, не будем. Будем уже здесь сделать тогда сведения. Давайте два типа файлов. Вы показываете, что работает. Картинка и текстовый, да? Для этого я должна увидеть. Думайте как. Некоторые там в реализацию пишут программу, чтобы сразу видеть путь, куда там файл прописывается, да? Я должна видеть файл.

Физически не то, что вы мне там написали, да? Мало что вы написали. А путь, по которому вы взяли файл, да? Еще и откройте мне свойства, чтобы я видела время создания. Вот исходная файл. Если не видно, ну, вся информация не будет видна в программе, значит, то, что не видно, отдельно мне скрин положите.

Я видела свойства файла. Когда он создан, где он там у вас лежит? При шифровании. Результат. После того, как нажали на кнопку зашифровать, все, вот я видела, что у биттера на видении есть. И при расшифровке тоже. Вот я видела, что есть еще один стрим, и стрим, что картинка у нас получилась. И рядышком свойства этой картинки, да? Когда он там изменен, и где он там лежит.

Как-то так. И то же самое с текстовым параметром. Подразумевается, что, скорее всего, что у меня не будет времени, я проверяю, что программа, в принципе, работает. Насколько она работает корректно, ну, вряд ли я смогу проверять, да, поскольку, говорю, расписание, поэтому не удивляйтесь, если вы не оттестировали, я вам напишу, принято, принято, а потом вы уйдете, раз уж у вас какие-то деташи. Я вас смотрю на спины, программа, в принципе, работает, все, я вас допускаю. Предполагается, что вы люди адекватные, программу оттестировали. Приходите сдавать.