ПРОГРАММНОЕ СРЕДСТВО ДЛЯ БЛОЧНОГО ШИФРОВАНИЯ ИНФОРМАЦИИ

Д. А. Владыковский

D.Vladykovsky@gmail.com;
Научный руководитель — С. А. Вельченко, старший преподаватель

На протяжении всей своей истории со времён зарождения языка и по настоящее время роль информации как таковой, развитие способов её фиксации, хранения и передачи имели определяющее влияние на направление, темпы и степень развития человеческого общества. Сегодня, когда информационные технологии проникли и безвозвратно охватили практически все сферы социального взаимодействия, невозможно переоценить значимость проблем защиты информации от несанкционированного доступа, её видоизменения, кражи или уничтожения. Данные задачи помогает решать криптология – область знаний, изучающая и развивающая вопросы и способы безопасной связи с использованием методов шифрования, расшифрования и дешифрования. Следовательно, для защиты компьютерных данных от различных угроз необходимо использовать качественные и стойкие алгоритмы криптографии, один из которых был реализован в ходе данной работы для защиты текстовой информации по открытым каналам связи.

Ключевые слова: криптография; шифрование; алгоритмы шифрования; симметричное шифрование; ассиметричное шифрование.

ШИФРОВАНИЕ

Сообщение будем называть открытым текстом. Обратимое изменение вида открытого текста так, чтобы за кажущейся случайной последовательностью некоторых символов спрятать его суть с одновременным предоставлением доступа к нему авторизованным пользователям называется шифрованием. Важной особенностью шифрования является использование ключа, который определяет конкретный вид преобразования сообщения из совокупности возможных для избранного алгоритма.

Процесс шифрования данных может осуществляться как программно, так и аппаратно. Аппаратная реализация отличается существенно большей стоимостью, однако ей присущи и преимущества: высокая производительность, простота, защищенность и т.д. Программная реализация менее производительна, но более практична, допускает известную гибкость в использовании и переносимость.

Сегодня существует большое количество различных алгоритмов шифрования, которые обладают своими преимуществами и недостатками. Можно привести следующую классификацию.

По количеству и назначению используемых ключей:

– одноключевые или симметричные;
– асимметричные или двухключевые.
По принципу формирования шифротекста:
– блочного шифрования;
– поточного шифрования.
По принципу размещения символов в шифротексте:
– замены или подстановочные;
– перестановки;
– комбинированные.
Отдельными, совмещающим в себе признаки нескольких обозначенных выше групп, являются:
– алгоритм хеширования - преобразует входные данные любого размера в выходную битовую строку фиксированного размера;
– алгоритм гаммирования [1].

СУЩЕСТВУЮЩИЕ РЕШЕНИЯ И РЕАЛИЗАЦИИ

В настоящее время на основе базовых схем со сложной комбинацией большого числа подстановок и(или) перестановок реализовано и зарегистрировано не менее двух десятков блочных и поточных криптографических алгоритмов. Наиболее распространённые представители из них:

DES – (Data Encryption Standard) стандарт шифрования данных в США. Блочный шифр с 56-битным ключом и 32 раундами (циклами) преобразования, оперирующий 64-битными блоками на основе сети Фейстеля с пятью режимами работы: простая замена, сцепление блоков, обратной связи по «шифротексту», обратной связи по выходу, режим счётчика. Считается устаревшим, ныне используется лишь в не модернизированных системах [1].

AES – (Advanced Encryption Standard) американский стандарт шифрования. Блочный шифр с ключом 128/192/256 бит, оперирующий 128-битными блоками. Хорошо проанализирован и сейчас широко используется, как это было ранее с его предшественником DES. Является одним из самых распространённых алгоритмов симметричного шифрования [1].

ГОСТ 28147-89 – советский и российский стандарт шифрования, также является стандартом СНГ, пример DES-подобных криптосистем. Блочный шифр с 256-битным ключом и 32 раундами (циклами) преобразования, оперирующий 64-битными блоками на основе сети Фейстеля с четырьмя режимами работы: простой замены, гаммирования,

гаммирования с обратной связью, выработки имитовставки. Применяется для защиты соединений в TLS (SSL, HTTPS,WEB) [1].

RC4 – (Rivest cipher или Ron's code) потоковый алгоритм шифрования с ключом переменной длины. Широко применяется в различных системах защиты информации в компьютерных сетях (протоколах SSL, TLS, алгоритмах обеспечения безопасности беспроводных сетей WEP и WPA) [1].

Анализируя и сравнительно обобщая принципы, положенные в основу описанных выше алгоритмов и их особенности, можно прийти к следующему выводу:

– давать оценку, какой из способов шифрования лучше симметричный или ассиметричный не является целесообразным - по своей математической и практической сути это достаточно разные вещи, при этом отдельно можно выделить достоинства и недостатки каждой из групп методов.

Положительными качествами симметричного шифрования являются:

– высокая скорость преобразования;
– простота реализации, достигаемая более простыми операциями;
– уменьшенная длина ключа в отношении стойкости;
– лучшая изученность из-за более длительного практического применения.

К недостаткам можно отнести:

– достаточно сложное управление ключами в больших сетях;
– необходимы защищённые каналы для обмена ключами между абонентами;
– невозможность использования шифров в электронной цифровой подписи, так как код известен обеим сторонам.

Прогресс в развитии вычислительной техники существенно увеличил возможности применения более ресурсоёмких методик криптопреобразований, при этом существенно выросли и объемы обрабатываемых данных. Не следует забывать, что с недавнего времени возник, существует и продолжает развиваться целый класс мобильных и встраиваемых устройств, для которых ключевой характеристикой является низкое энергопотребление, а, следовательно, к ним предъявляются повышенные требования экономности алгоритмов в плане вычислений. Среди таких устройств можно выделить смарт-карты, в которых может быть необходима функция шифрования данных, мобильные устройства, подключающиеся к беспроводным сетям. Оба этих класса устройств переживают в настоящее время расцвет, что привлекает внимание к таким алгоритмам, как:

Алгоритм ГОСТ 28147-89

ГОСТ является 64-битовым алгоритмом с 256-битовым ключом. ГОСТ также использует дополнительный ключ. В процессе работы алгоритма на 32 этапах последовательно выполняется простой алгоритм шифрования. В основе криптографического алгоритма лежит отработанная с годами схема Фестеля, хорошо зарекомендовавшая себя в криптографическом алгоритме DES. Использование схемы Фейстеля позволяет избежать каких-либо ошибок при создании самого алгоритма, так и при его реализации, что качественно отличает его от DES. Кроме этого, использование такой конструкции позволяет сделать зашифрование и расшифрование биективным и отличие заключается только в том, что ключи подаются в обратном порядке. В алгоритме ГОСТ предусмотрено 32 раунда шифрования [1]. Структура алгоритма шифрования приведена на рисунке 1.

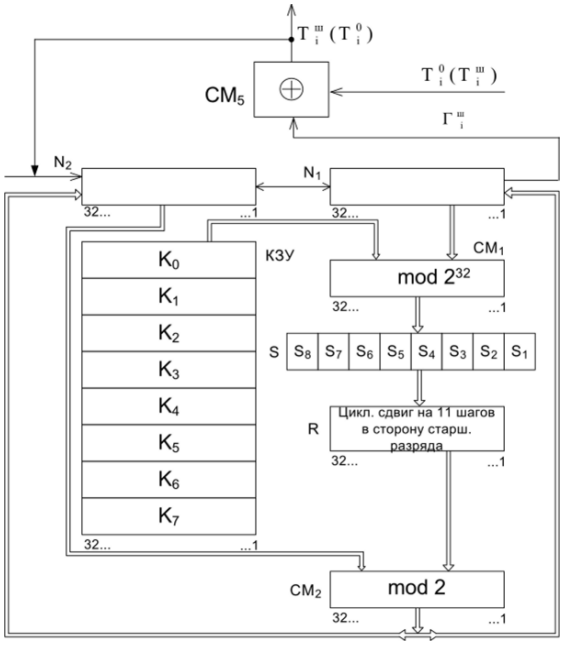

Рис. 1. Структура алгоритма шифрования ГОСТ в режиме гаммирования

РЕАЛИЗАЦИЯ ПРОГРАММНОГО СРЕДСТВА

Для реализации программного средства (см. рис. 2) был выбран алгоритм шифрования ГОСТ 28147-89 и технология разработки .Net [2]. В качестве интерфейса была выбрана технология WPF. Программное средство позволяет сгенерировать ключ случайным образом перемещая курсор по координатной сетке. С помощью сгенерированного ключа можно зашифровывать информацию. Чтобы расшифровать полученное сообщение пользователю необходимо знать ключ, который использовался в моменте шифрования, а также зашифрованную информацию. В

приложении реализован функционал загрузки, очистки, сохранения ключа и сообщения. Реализовано контекстное меню, которое содержит кнопки «Справка», «О программе» и «Выход».

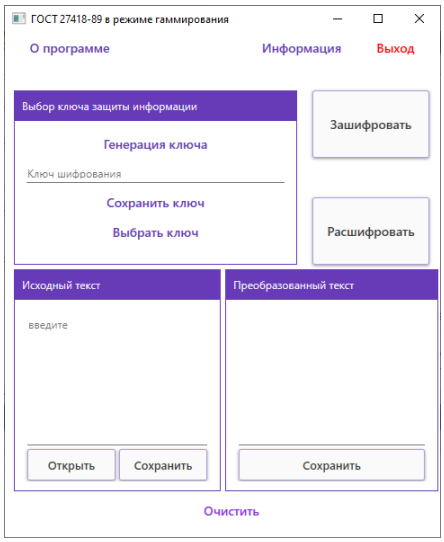

Рис.2. Программное средство

ЗАКЛЮЧЕНИЕ

В ходе данной работы было разработано программное средство для выполнения криптографических преобразований с использованием алгоритма ГОСТ 28147-89, полностью соответствующее требованиям задания на проектирование. Разработанное программное средство может быть использовано в различных сферах деятельности, где присутствует необходимость, защитить не только текстовую информацию посредствам шифрования для передачи по открытым каналам связи, но и иные файлы в любом формате. Можно отметить, что ГОСТ 28147-89 обладает такими преимуществами, как бесперспективность атаки полным перебором, эффективность реализации и, соответственно, высокое быстродействие на современных компьютерах; наличие защиты от навязывания ложных данных (выработка имитовставки) и одинаковый цикл шифрования во всех четырёх алгоритмах стандарта. Но его ключевой проблемой является неполнота стандарта в части генерации ключей и таблиц замен.

Библиографические ссылки

1. *Шнайдер Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. М.: Триумф, 2012. 518 с.
2. *Троелсен Э.* C# и платформа .NET. Библиотека программиста. СПб.: Питер, 2002. 800 с.