УДК 378.(075).8

РЕАЛИЗАЦИЯ КРИПТОГРАФИЧЕСКОЙ СИСТЕМЫ ШИФРОВАНИЯ ТЕКСТОВЫХ ФАЙЛОВ

Лифенко В.М., Бегалин А.Ш.

Криптографические методы являются наиболее эффективными средствами защиты информации в автоматизированных системах, при передаче же по протяженным линиям связи они являются единственным реальным средством предотвращения несанкционированного доступа к ней. Метод шифрования характеризуется показателями надежности и трудоемкости [1].

Важнейшим показателем надежности криптографического закрытия информации является его стойкость – тот минимальный объем зашифрованного текста, статистическим анализом которого можно вскрыть исходный текст. Таким образом, стойкость шифра определяет допустимый объем информации, зашифровываемый при использовании одного ключа [2].

Трудоемкость метода шифрования определяется числом элементарных операций, необходимых для шифрования одного символа исходного текста.

Актуальность данной тематики в том, что сейчас остро стоит проблема защиты данных от несанкционированного доступа, данная программа помогает ее частично решить.

Программа реализована в среде визуального программирования Borland Delphi.

Для работы программы достаточно скопировать каталог с программой в любое место диска или дистрибутива и запустить файл «project1.exe».

После запуска программы появится главная форма, на которой находятся вкладки с выбором методов (*Рис. 1).*

Для того чтобы зашифровать текстовый файл, его сперва выбирают при нажатии кнопки слева от окна ввода исходного файла. Здесь можно указать существующий файл или создать новый с расширением «txt». Выбранный файл автоматически будет отображаться снизу, слева. Затем указать или создать результирующий файл – куда сохранится зашифрованный текст, также с расширением «txt».

Для начала процесса шифрования достаточно нажать кнопку «Шифровать». Зашифрованный текст появится снизу, справа. Ход выполнения процесса в процентах будет прослеживаться с помощью индикатора справа. При использовании ключей (методы RC6, Циклический сдвиг, битовых операций (xor) он указывается в соответствующей строке. При успешном выполнении шифрования выведется соответствующее сообщение.

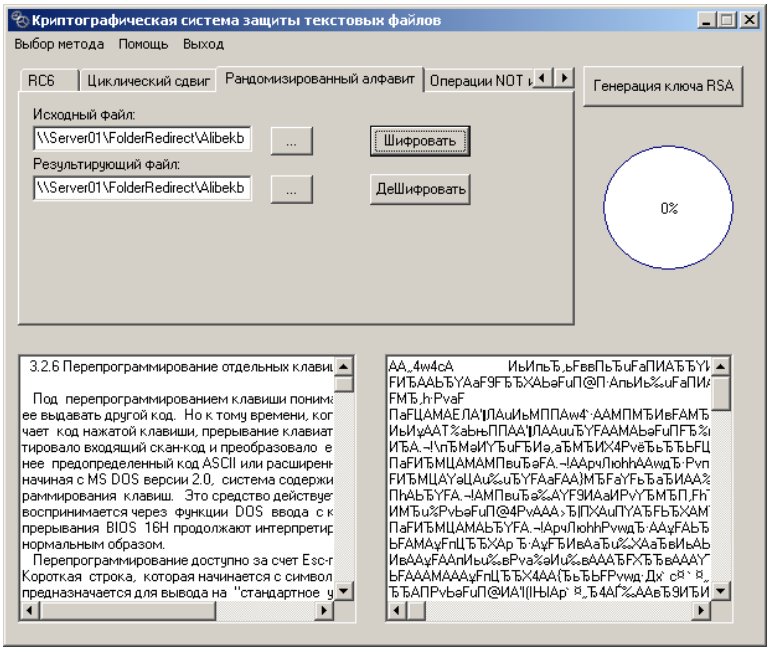

Рис. 1. Главная форма

Для дешифрования текста необходимо сначала выбрать зашифрованный файл, затем файл сохранения результата и нажать кнопку «Дешифровать». Если используются ключи, то необходимо также указать и исходный ключ.

Для просмотра сведений о программе достаточно нажать соответствующий пункт меню «Помощь». Для выхода из программы надо нажать меню «Выход».

В настоящее время криптография успешно используется почти во всех информационных системах – от Internet до баз данных. Без нее обеспечить требуемую степень конфиденциальности в современном, до предела компьютеризированном мире уже не представляется возможным. Кроме того, с помощью криптографии предотвращаются попытки мошенничества в системах электронной коммерции и обеспечивается законность финансовых сделок. Со временем значение криптографии, по всей вероятности, возрастет. Для этого предположения имеются веские основания [3].

Однако с огорчением приходится признать, что подавляющее большинство криптографических систем не обеспечивает того высокого уровня защиты, о котором с восторгом обычно говорится в их рекламе. Многие из них до сих пор не были взломаны по той простой причине, что пока не нашли широкого распространения. Как только эти системы начнут повсеместно применяться на практике, они, словно магнит, станут привлекать пристальное внимание злоумышленников, которых сегодня развелось великое множество.

При этом удача и везение будут явно на стороне последних. Ведь для достижения своих целей им достаточно найти в защитных механизмах всего лишь одну брешь, а обороняющимся придется укреплять все без исключения уязвимые места.

Понятно, что никто не в состоянии предоставить стопроцентную гарантию безопасности. Тем не менее криптографическую защиту без особых усилий можно спроектировать так, чтобы она противостояла атакам злоумышленников вплоть до того момента, когда им станет проще добыть желаемую информацию другим путем (например, с помощью подкупа персонала или внедрения программ-шпионов). Ведь криптография действительно хороша именно тем, что для нее уже давно придуманы эффективные алгоритмы и протоколы, которые необходимы, чтобы надежно защитить компьютеры и компьютерные сети от электронного взлома и проявлений вандализма [4].

Вот почему в реальной жизни криптографические системы редко взламываются чисто математическими методами. Ведь криптографический алгоритм или протокол от его практической реализации в виде работающей программы, как правило, отделяет зияющая пропасть. Даже доказанный по всем правилам формальной логики факт, что криптографическая зашита совершенна с математической точки зрения, совсем не означает, что она останется таковой после того, как над ее внедрением поработают программисты.

Немало проблем, связанных с использованием криптографических средств, создают сами пользователи. Безопасность заботит их меньше всего. В первую очередь им требуются простота, удобство и совместимость с уже существующими (как правило, недостаточно защищенными) программными продуктами. Они выбирают легко запоминающиеся криптографические ключи, записывают их где попало, запросто делятся ими с друзьями и знакомыми. Поэтому грамотно спроектированная криптографическая система обязательно должна принимать во внимание специфические особенности поведения людей.

Еще труднее убедить людей в необходимости строго и неукоснительно применять криптографическую защиту данных. Пользователи с готовностью приносят в жертву собственную безопасность, если средства ее обеспечения мешают им поскорее сделать свою работу. Поэтому только в том случае, если при проектировании криптографической системы были учтены реальные потребности пользователей, она действительно в состоянии защитить их компьютеры и компьютерные сети.

Данный программный продукт можно использовать для защиты данных текстовых файлов путем шифрования различными методами.

СПИСОК ЛИТЕРАТУРЫ

1 Герасименко В.А., Размахнин М.К. Криптографические методы в автоматизированных системах // Зарубежная радиоэлектроника. – 1982. – № 8.

2 Сяо Д., Керр Д.С. Мэдник. Защита ЭВМ. – М.: Мир, 1982.

3 Хоффман Л.Дж. Современные методы защиты информации. – М.: Сов.радио, 1980.

4 Джефф П.Р. Электроника. 1973. Т. 46. №1.

Түйін

Бұл мақалада мәтіндік файлдарды шифрлаудың криптографиялық жүйесінің әртүрлі әдістері суреттелген. Бағдарлама Borland Delphi 7.0 құралдармен іске асырылған.

Conclusion

This article describes how cryptographic encryption of text files in different ways. The program is implemented by means of Borland Delphi 7.0