УДК 32.97

А.Г. Кику, К.С. Богомазов

РАЗРАБОТКА СИСТЕМЫ СИНТЕЗА КРИПТОГРАФИЧЕСКИХ МЕТОДОВ НА ОСНОВЕ ПРЕДВАРИТЕЛЬНОЙ ОБРАБОТКИ ИНФОРМАЦИИ

Аннотация: Предложена система синтеза криптографических методов обработки информации. Предложенная система иерархична по структуре и имеет открытый характер. Система позволяет потребителям синтезировать собственные методы шифрования информации, криптостойкость которых в общем случае выше криптостойкости существующих методов.

Ключевые слова: методы криптографии, криптостойкость

Введение

В современной криптографии разработано достаточно большое количество алгоритмов шифрования. Однако они имеют ряд недостатков.

В данной статье предлагается система, позволяющая самим потребителям синтезировать собственные методы шифрования информации с высокими криптографическими показателями качества.

Постановка задачи

Общая задача выполненных исследований в рамках данной статьи состоит в разработке системы синтеза криптографических методов, соответствующей следующим основным требованиям:

1. Система должна иметь отрытый структурный и параметрический характер;
2. Система должна обеспечивать возможность потребителям синтезировать собственные оригинальные методы шифровки информации, обеспечивающих высокий уровень показателей качества;
3. Система должна обеспечивать синтез методов криптографии, обеспечивающих более высокую вероятность не распознавания по сравнению с существующими методами.

Описание предложенной системы синтеза криптографических методов

Предложенная система синтеза криптографических методов построена на основе открытого иерархического принципа, позволяющего ее наращивать как структурно, так и параметрически. При этом:

1. Структурная открытость системы позволяет с одной стороны увеличивать число уровней предварительной обработки информации, а с другой увеличивать число методов предварительной обработки информации в каждом уровне.

2. Параметрическая открытость предложенной системы позволяет изменить как число параметров методов предварительной обработки информации, так и расширить множества значений упомянутых параметров.

Общая структурная схема предложенной системы синтеза методов криптографической обработки информации приведена на рис. 1.

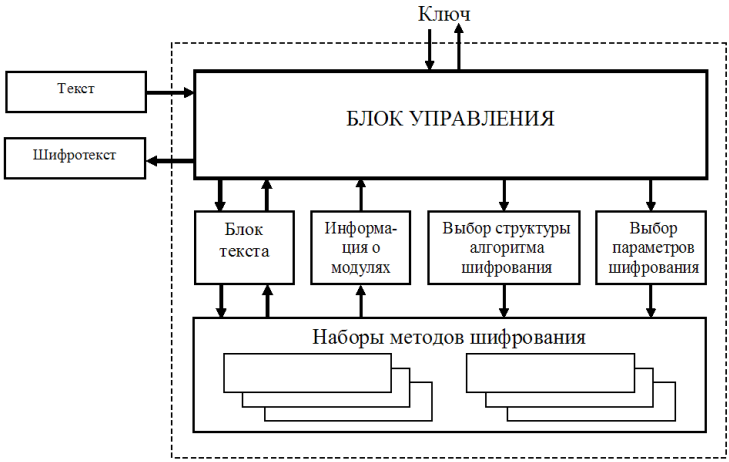

Рисунок 1. – Структура системы шифрования

Система синтеза криптографических методов содержит общий блок управления, общий блок формирования методов криптографической обработки информации и блок связи между ними.

Блок управления реализует следующие функции:
ввод-вывод обрабатываемой информации;
выбор стратегии разбиения текста на соответствующие блоки;
выбор количества и видов уровней криптографической обработки информации;

- выбор вида конфигурации отмеченных уровней криптографической обработки информации;
- выбор вида структур методов предварительной обработки информации в выбранных уровнях криптографической обработки информации;
- выбор параметров структур отмеченных методов предварительной обработки информации в выбранных уровнях системы криптографической обработки информации;
- выбор стратегий формирования ключа и его расположения;
- упаковка и распаковка служебной информации в шифруемых текстах.

 ISSN 1560-8956

Алгоритм шифрования построен как многоуровневая система (рис. 2), позволяющая формировать в зависимости от необходимой криптостойкости произвольное число уровней и произвольное количество методов шифрования на каждом уровне.

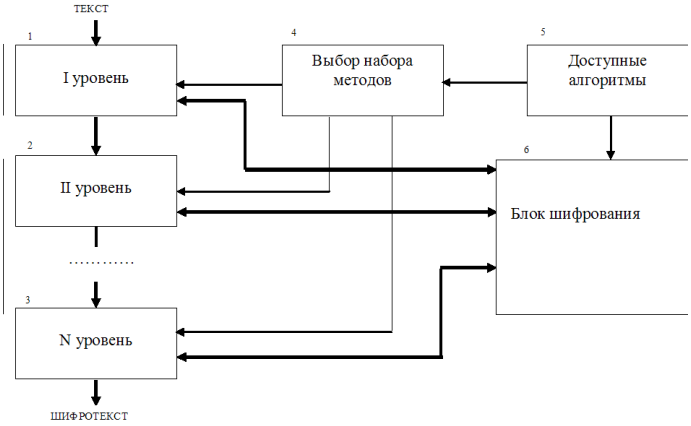

Рисунок. 2. – Структурная схема обобщенного алгоритма шифрования

В уровнях шифрования информации могут быть использованы различные методы предварительной обработки информации, например, алгебраические линейные и нелинейные операторы обработки информации, динамические операторы различного порядка, интегральные операторы различного типа, например, Z, Фурье, Радемахера, Уолша и другого вида интегральных преобразований, операторы зашумления информации и др. При этом кроме известных преобразований могут быть использованы и оригинальные преобразования, разработанные самими пользователями предлагаемой системы синтеза криптографических методов обработки информации.

Текст, попадая в управляющий блок, по очереди подвергается шифрованию блоком шифрования, структура и параметры которого задаются блоком управления.

Упрощенная структурная схема алгоритма шифрования представлена на рис. 3.

Процесс шифрования можно разбить на 5 этапов. На первом этапе (блок 1) из исходного (открытого) текста выделяется блок текста, размер и расположение которого определяется модулем управления (блок 10) через модуль выбора длины и расположения блока текста (блок 6). На втором этапе (блок 2) к выделенному блоку добавляется информация о расположении параметров шифрования из предыдущего блока. Если данный блок является первым в процессе шифрования, т.е. последним при расшифровывании, то в параметрах расположения позиции указывается служебный код, указывающий на то, что данный блок последний и про-

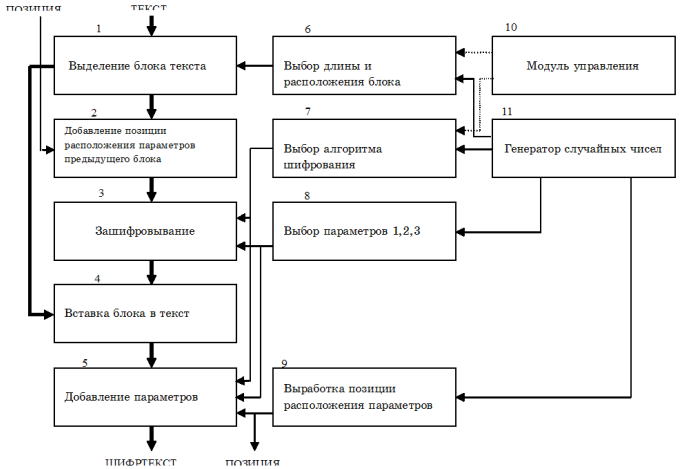

Рисунок. 3. – Упрощенная структура алгоритма шифрования.

цесс расшифровывания на нем должен будет завершиться. На третьем этапе (блок 3) происходит зашифровывание блока текста в соответствии с выбранным модулем управления через модуль выбора алгоритма шифрования (блок 7) алгоритмом и параметрами шифрования низшего уровня.

На четвертом этапе (блок 4) происходит вставка (возвращение) зашифрованного блока в текст в соответствии с его расположением до шифрования.

На пятом этапе (блок 4) в текст добавляется информация, необходимая для расшифровывания, содержащая номер метода и его параметры. Информация добавляется (вставляется) побайтно, в соответствии с позициями, выработанными блоком выработки позиций (блок 9) с использованием данных, полученных от генератора случайных чисел (блок 11).

Блок выбора длины и расположения блока текста производит разбиение текста на некоторое случайное число блоков приблизительно одинаковой длины. Длина блоков выбирается случайным образом, но с таким расчетом, чтобы общее количество блоков было достаточно большим для нахождения закономерности в пределах одного блока.

Подлежащий шифрованию текст подвергается разбиению на блоки для каждого уровня шифрования (рис. 4)

После этого информация подвергается криптографической обработке сформированным методом с соответствующим структурой и параметрами.

Зашифрованный текст представляет собой набор символов, среди которых случайным образом расположены служебные байты (рис. 5), содержащие информацию, необходимую для формирования алгоритма расшифровывания.

 ISSN 1560-8956

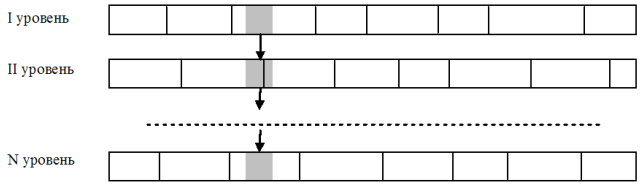

Рисунок 4. – Разбиение текста на блоки по уровням.

Рисунок 5. – Расположение служебной информации в зашифрованном тексте.

Набор позиций расположения служебной информации представляет собой ключ, передаваемый на приемную сторону. При расшифровывании участки со служебной информацией после ее извлечения удаляются.

Предложенная система синтеза алгоритмов криптографии позволяет синтезировать методы шифрования, вероятность взлома которых зависит от числа используемых уровней шифрования, от числа структур обработки информации в каждом уровне шифровки и от числа параметров используемых структур.

Необходимо отметить, что один лишь уровень зашумления может обеспечить практически бесконечно малую вероятность $P_{Ш}$ дешифровки текста. Действительно, на основе даже одного известного генератора псевдослучайных последовательностей могут быть выбраны “рабочие” последовательности, структуры и параметры которых могут принадлежать множествам с практически бесконечно большой мощностью. Тем более может быть обеспечена практически бесконечно малую вероятность дешифровки текста, если уровень зашумления будет содержать несколько различных генераторов псевдослучайных последовательностей.

Кроме указанного уменьшение вероятности дешифровки обеспечивается использованием “достаточно большого” числа уровней предварительной обработки информации, в каждом из которых содержится “достаточно большое” число методов обработки информации, каждый из которых определяется соответствующим числом параметров.

Так, например, если система содержит N уровней шифровки информации, то на их основе в общем случае вероятность $P_{Ш}$ может быть уменьшена в $N!$ раз.

Если допустим, что в каждом уровне содержится даже одинаковое число N_M методов предварительной обработки информации, вероятность дешифровки уменьшится еще в N_M раз.

Допустим, что каждый метод предварительной обработки информации “фиксируется” $N_П$ параметрами, каждый из которых имеет, напри-

мер, по $N_З$ значений, то вероятность дешифровки может быть уменьшена еще в $N_П N_З$ раз.

Таким образом, даже вышеописанный возможный вариант криптографического метода будет обеспечивать вероятность $P_{НД}$ дешифровки шифрованного текста, равной

$$P_{НД} = P_{Ш}(N!N_M N_П N_З)^{=1} \quad (1)$$

Если допустить, что система содержит хотя бы один из известных криптографических методов с уровнем криптостойкости, равным $P_И$, то общая вероятность дешифровки будет равна

$$P = P_И P_{Ш}(N!N_M N_П N_З)^{=1} \quad (2)$$

При желании или необходимости вероятность не дешифровки текстов для синтезированных методов может быть точно определена.

Из приведенного очевидно вытекает, что на основе предложенной иерархической системы синтеза криптографических методов могут быть разработаны методы шифровки, которые обеспечивают практически бесконечно малую вероятность распознавания шифрованных текстов.

Экспериментальное исследование предложенного подхода синтеза методов криптографической обработки информации осуществлено путем его компьютерной реализации в среде Delphi.

На рис.6 приведен зашифрованный текст, а на рис.7- дешифрованный текст, который полностью совпадает с исходным текстом, который подлежал шифрованию.

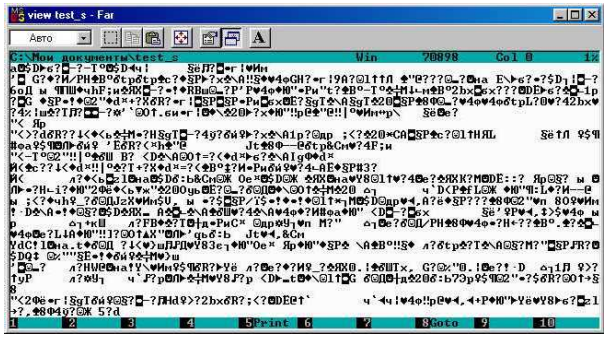

Рисунок. 6. – Зашифрованный текст

Выводы

В качестве основных выводов к работе можно отметить следующее:

1. Предложенная система синтеза криптографических методов позволяет потребителям синтезировать оригинальные методы шифровки информации с требуемой вероятностью не дешифровки зашифрованных текстов;

 ISSN 1560-8956

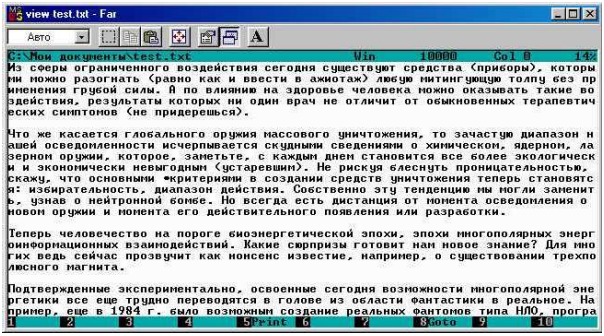

Рисунок 7. – Исходный текст

2. Предложенная система в комбинации с существующими методами шифровки позволяет синтезировать методы улучшения характеристик существующих;
3. Предлагаемая система синтеза криптографических методов обработки информации позволяет синтезировать методы, которые обеспечивают “очень высокую” вероятность не дешифровки зашифрованных текстов.
4. Дешифровка какого нибудь экземпляра зашифрованного текста не обеспечивает облегчение процесса обучения дешифровки других.
5. Открытый структурный и параметрический характер системы повышает интерес исследователей (в частности, моего руководителя) к разработке собственных методов предварительной обработки информации, например, оригинальных генераторов псевдослучайных последовательностей.

Литература

1. Каппелинин В. и др., Цифровые фильтры и их применение, М.:Энергоатомиздат,1983.
2. Шрюфер Е., Обработка дискретизированных сигналов Киев: Либідь, 1992.
3. Молдован А.А. , Молдован Н.А., Б.Я.Советов, Криптография, Санкт-Петербург: Лань 2000

Отримано 08.12.2010 р.