УДК 621. 313

РЕАЛИЗАЦИЯ АЛГОРИТМА RIJNDAEL В КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЕ КОСМИЧЕСКИХ КАНАЛОВ СВЯЗИ

Сапабеков А., Беделханов Алмат., Брижанова С., Алимов Д.
ablai_sapabekov@mail.ru
Студенты 4-курса кафедры «Космическая техника и технологии» ЕНУ им. Л.Гумилева, Нур-Султан, Казахстан,
Научный руководитель – Молдамурат Х.

Цель работы исследование и разработка программно-аппаратной модели криптографической защиты информации при передаче ее по космическому каналу связей. Методы проведенных исследований и практическая реализация базируются на теории надежности систем информационной безопасности и криптосистем, криптографических методах защиты информации, теории нелинейных динамических систем (хаотических - реконструкция динамической системы по ее реализации).

Основные результаты научного исследование взаимосвязь криптографических алгоритмов и хаотических систем; разработана программная модель с использованием детерминированного хаоса для шифрования текстовых и графических данных.

Проблема защиты информации путем ее преобразования, исключающего ее прочтение посторонним лицом, волновала человеческий ум с давних времен. Среди всего спектра методов защиты данных от нежелательного доступа особое место занимают криптографические методы. История криптографии – ровесница истории человеческого языка. Более того, первоначально письменность сама по себе была криптографической системой, так как в древних обществах ею владели только избранные. С широким распространением письменности криптография стала формироваться как самостоятельная наука. Актуальность проблемы очевидна, т.к. информация в современном обществе – одна из самых ценных вещей в жизни, требующая защиты от несанкционированного проникновения лиц, не имеющих к ней доступа. Актуальной задачей была и продолжает оставаться, в частности, задача обеспечения конфиденциальности при передаче информации по космическим каналам.

Основными видами криптографического закрытия являются шифрование и кодирование защищаемых данных. При этом шифрование есть такой вид закрытия, при котором самостоятельному преобразованию подвергается каждый символ закрываемых данных; при кодировании защищаемые данные делятся на блоки, имеющие смысловое значение, и каждый такой блок заменяется цифровым, буквенным или комбинированным кодом. При этом используется несколько различных систем шифрования: замена, перестановка, гаммирование, аналитическое преобразование шифруемых данных. Широкое распространение получили комбинированные шифры, когда исходный текст последовательно преобразуется с использованием двух или даже трех различных шифров. В рамках выполнения научно-исследовательской работы были рассмотрены и изучены методы и алгоритмы шифрования информации. На сегодняшний день безопасность современных криптографических систем основана на вычислительной стойкости ключей.

В далеком 1998 году NIST объявил конкурс на создание алгоритма, удовлетворяющего выдвинутым институтом требованиям. Он опубликовал все несекретные данные о тестировании кандидатов и потребовал от авторов алгоритмов сообщить о базовых принципах построения используемых в них констант. В отличие от ситуации с DES, NIST при выборе (AES) RIJNDAEL не стал опираться на секретные и, как следствие, запрещенные к публикации данные об исследовании алгоритмов-кандидатов.

Чтобы быть утвержденным в качестве стандарта, алгоритм должен был:

– реализовать шифрование частным ключом;

– представлять собой блочный шифр;

– работать со 128-разрядными блоками данных и ключами трех размеров (128, 192 и 256 разрядов).

Перед первым туром конкурса в NIST поступило 21 предложение, 15 из которых соответствовали выдвинутым критериям. Затем были проведены исследования этих решений, в том числе связанные с дешифровкой и проверкой производительности, и получены экспертные оценки специалистов по криптографии. В августе 1999 года NIST объявил пять финалистов, которые получили право на участие во втором этапе обсуждений. 2 октября 2000 года NIST сообщил о своем выборе – победителем конкурса стал алгоритм RIJNDAEL (произносится как «райндол») бельгийских криптографов Винсента Раймана и Йоана Дамана, который зарегистрирован в качестве официального федерального стандарта как FIPS 197 (Federal Information Processing Standard).

Для меня остается загадкой, зачем в российском вузе преподают стандарты иностранных государств. Видимо, исходят из принципа, что врага надо знать в лицо:). Ладно, в общем-то, это не наше дело. Нам надо просто программно реализовать основу национальной безопасности США.

Методы защиты информации, передаваемой покосмическим каналам связи.Для передачи сообщения от одной стороны к другой через сеть, обе стороны, являющиеся инициаторами транзакции, должны вступить во взаимодействие. С этой целью создается логический информационный канал, для чего определяется маршрут прохождения данных от источника к адресату в сети и согласованно обоими инициаторами выбирается для использования коммуникационный протокол (например, TCP/IP).

Вопросы безопасности возникают в тех случаях, когда необходимо обеспечить защиту передаваемой информации от некоторого злоумышленника, который может угрожать целостности, конфиденциальности и т.п. В этом случае любая технология защиты должна включать в себя следующие две составляющие:

1. Преобразование передаваемой информации (шифрование, добавление зависящего от сообщения кода, по которому адресат сможет идентифицировать отправителя).

2. Использование некоторой общей для обоих инициаторов транзакции секретной информации (ключ шифра, применяемый для кодирования сообщения соответствующим преобразованием перед отправкой и для последующего декодирования после получения).

Для обеспечения защиты может понадобиться участие третьей стороны, заслуживающей доверия обоих инициаторов транзакции, которая осуществляет доставку секретной информации и гарантирует аутентичность передаваемого сообщения [1].

Из приведенной общей модели следует, что при разработке конкретного средства защиты необходимо решить следующие четыре основные задачи.

1. Разработать алгоритм преобразования информации для обеспечения защиты.
2. Создать секретную информацию, которая будет использоваться с алгоритмом.

Разработать методы доставки и совместного использования этой секретной информации.

Шифрование

(AES) RIJNDAEL является стандартом, основанным на алгоритме Rijndael. Для (AES) RIJNDAEL длина input (блока входных данных) и State(состояния) постоянна и равна 128 бит, а длина шифроключа K составляет 128, 192, или 256 бит. При этом, исходный алгоритм Rijndael допускает длину ключа и размер блока от 128 до 256 бит с шагом в 32 бита. Для обозначения выбранных длин input, State и Cipher Key в байтах используется нотация Nb = 4 для input и State, Nk = 4, 6, 8 для Cipher Key соответственно для разных длин ключей.

В начале шифрования input копируется в массив State по правилу s [r, c] = in [r + 4c], для и. После этого к State применяется процедура AddRoundKey() и затем State проходит через процедуру трансформации (раунд) 10, 12, или 14 раз (в зависимости от длины ключа), при этом надо учесть, что последний раунд несколько отличается от предыдущих. В итоге, после завершения последнего раунда трансформации, State копируется в output по правилу out [r + 4c] = s [r, c], для и.

Отдельные трансформации SubBytes(), ShiftRows(), MixColumns(), и AddRoundKey() – обрабатывают State. Массив w[] – содержит key schedule.

```
Cipher (byte in [4*Nb], byte out [4*Nb], word w [Nb*(Nr+1)])
begin
byte state [4, Nb]
state = in
AddRoundKey (state, w [0, Nb-1])
for round = 1 step 1 to Nr-1
SubBytes(state)
ShiftRows(state)
MixColumns(state)
AddRoundKey (state, w [round*Nb, (round+1)*Nb-1])
end for
SubBytes(state)
ShiftRows(state)
AddRoundKey (state, w [Nr*Nb, (Nr+1)*Nb-1])
out = state
end
SubBytes()
```

В процедуре SubBytes, каждый байт в state заменяется соответствующим элементом в фиксированной 8-битной таблице поиска, S; bij = S(aij).

Процедура SubBytes() обрабатывает каждый байт состояния, независимо производя нелинейную замену байтов используя таблицу замен (S-box). Такая операция обеспечивает нелинейность алгоритма шифрования. Построение S-box состоит из двух шагов. Во-первых, производится взятие обратного числа в поле Галуа. Во-вторых, к каждому байту b из которых состоит S-box применяется следующая операция:

$$b'_i = b_i \oplus b_{(i+4) \bmod 8} \oplus b_{(i+5) \bmod 8} \oplus b_{(i+6) \bmod 8} \oplus b_{(i+7) \bmod 8} \oplus c_i \qquad (1)$$

где, и где bi есть i-ый бит b, а ci – i-ый бит константы c = 6316 = 9910 = 011000112. Таким образом, обеспечивается защита от атак, основанных на простых алгебраических свойствах.

Детальная схема алгоритма шифрования представлена на рисунке 1.

Листинг программы

```
unit Main;
interface
uses
Windows, Messages, SysUtils, Classes, Graphics, Controls, Forms, Dialogs,
StdCtrls, Math, Buttons, ExtCtrls, Menus, jpeg, pngimage;
type
E(AES) RIJNDAELError = class(Exception);
PInteger = ^Integer;
T(AES) RIJNDAELBuffer = array [0..15] of byte;
T(AES) RIJNDAELKey128 = array [0..15] of byte;
T(AES) RIJNDAELExpandedKey128 = array [0..43] of longword;
P(AES) RIJNDAELBuffer =^T(AES) RIJNDAELBuffer;
P(AES) RIJNDAELKey128 =^T(AES) RIJNDAELKey128;
P(AES) RIJNDAELExpandedKey128 =^T(AES) RIJNDAELExpandedKey128;
TForm1 = class(TForm)
```

```
Label1: TLabel;
Edit1: TEdit;
OpenDialog1: TOpenDialog;
Button1: TButton;
Button2: TButton;
Label2: TLabel;
Label3: TLabel;
Label4: TLabel;
Label5: TLabel;
Edit2: TEdit;
Label_Time: TLabel;
Label9: TLabel;
Label_Status: TLabel;
MemoOut: TMemo;
ButtonStop: TButton;
Panel1: TPanel;
MemoIn: TMemo;
EditDelay: TEdit;
RadioGroup1: TRadioGroup;
CBOpt: TComboBox;
Label6: TLabel;
LName: TLabel;
LPath: TLabel;
Label10: TLabel;
MainMenu1: TMainMenu;
MFile: TMenuItem;
MFChoose: TMenuItem;
MHelp: TMenuItem;
MHHelp: TMenuItem;
MFExit: TMenuItem;
Label7: TLabel;
Label8: TLabel;
Image1: TImage;
Label11: TLabel;
procedure Button1Click (Sender: TObject);
procedure Button2Click (Sender: TObject);
procedure ButtonStopClick (Sender: TObject);
procedure CBOptChange (Sender: TObject);
procedure FormActivate (Sender: TObject);
procedure RadioGroup1Click (Sender: TObject);
procedure MFExitClick (Sender: TObject);
procedure MFChooseClick (Sender: TObject);
procedure FormCreate (Sender: TObject);
procedure MHHelpClick (Sender: TObject);
private
{Private declarations}
public
{Public declarations}
end;
var
Form1: TForm1;
EncryptedText, Fpath: string;
```

flag: boolean;

Расшифровка производиться аналогично, но в обратном порядке. Соответственно шифротексту аттрактором генерируются числа. Основная сложность заключается в начальных параметрах и выбранном аттракторе. Если начальные параметры отличаются хоть на сотую долю, то зашифрованное сообщение не будет расшифровано. Поэтому важно точно и безопасно передать параметры шифрования. Итак, полученные числа преобразовываются в двоичный вид и, используя метод Вернама, получаем двоичные значения символов. Эти значения преобразовываются в десятичный вид, они же в свою очередь, сверяясь по таблице ASCII, превращаются в символы, образуя исходный текст [4].

Шифрование самого изображения достаточно распространено, однако это сложно реализовать, т.к. необходимо обеспечить должный уровень шифрования и одновременно сохранить целостность изображения при дешифровании.

На подготовительном этапе, перед шифрованием, изображение преобразовывается в битовую маску, в так называемую Bitmap. Откуда считываются пиксели и информация об их цвете. Данная информация хранится в виде числового значения относительно цветовой схеме RGB. Т.к. программа разрабатывалась в среде Delphi, при обработке изображении имеются ограничения, т.е. возможно лишь использование цветовой схемы RGB. После чтения цвета пикселя, информация о цвете разделяется на три ветви, это соответственно Red, Green и Blue [5].

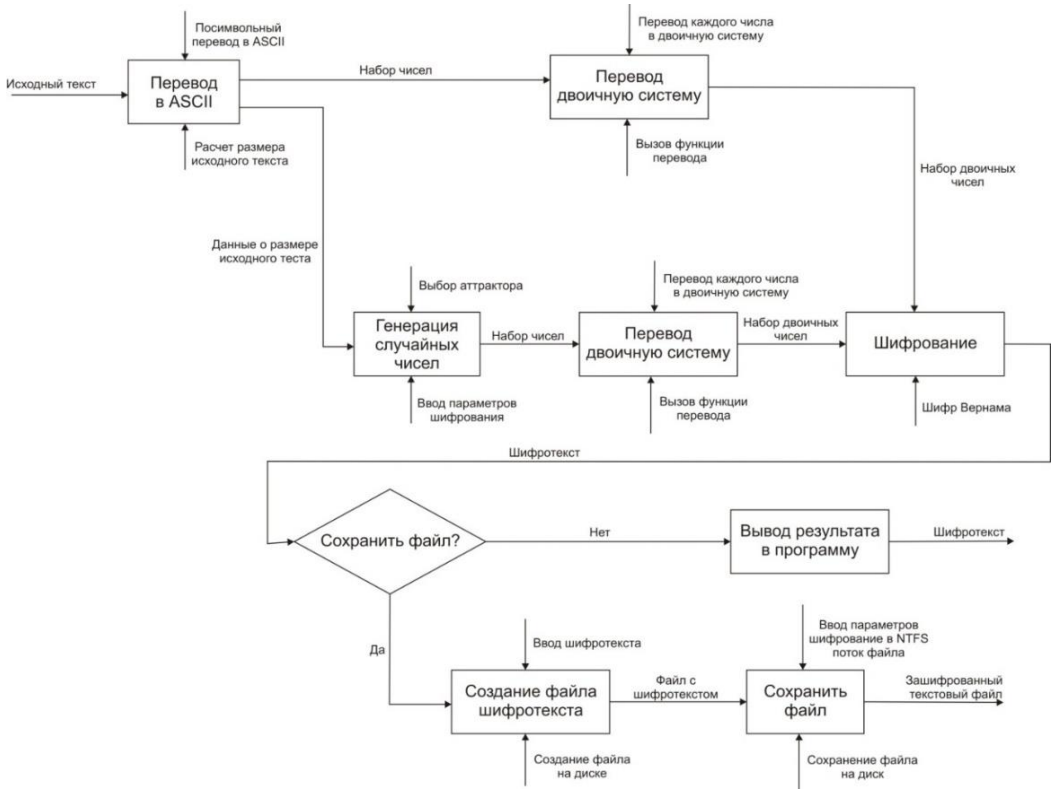

Рисунок 1 – Модель шифрования текстового файла

Заключение.В этой работе исследована возможность представления, передачи и извлечения информации с помощью траекторий динамических систем с хаосом; изучена взаимосвязь детерминированного хаоса и криптографии, как одной из самых распространенных и хорошо зарекомендовавших себя технологий защиты информации при передаче ее по космическим каналам; разработаны цифровые модели программной защиты передачи данных по космическому каналу связи с использованием криптографических методов.

Список использованных источников

1. Архангельская А.В., Запечников С.В. Характеристика и области эффективного применения методов поточного шифрования для защиты трафика в телекоммуникационных системах. //Информационное противодействие угрозам терроризма. Научно-практический журнал. - №4, – 2005. – С. 196-199.
2. Корт С.С. Теоретические основы защиты информации//– М.: Гелиос АРВ, 2014.
3. Молдовян А.А., Молдовян Н.А. и др. Криптография. Скоростные шифры. – С.Пб: БХВ-Петербург, – 2009. – 493 с.
4. Асосков А.В. Поточные шифры// – М.: Кудиц-Образ, – 2003. – 334 с.
5. Столлингс В. Криптография и защита сетей//- М.:Вильямс, – 2001.- 669 с.
6. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. Технические средства и методы защиты информации//Учебное пособие для вузов,– 4-е изд., испр. И доп. – М., – 2009.