Лопатина Алина Алексеевна
студентка
Еременко Марина Петровна
преподаватель общетехнических
и специальных дисциплин
ГБПОУ «Ставропольский колледж
связи им. В.А. Петрова»
г. Ставрополь, Ставропольский край

КОДИРОВАНИЕ ИНФОРМАЦИИ МЕТОДОМ RSA

Аннотация: *в данной статье рассматривается проблема кодирования информации методом RSA. Информация в наше время является не только объектом передачи, хранения и использования. Не секрет, что информация стала ценностью, материалом для работы и досуга. Активный обмен информацией, например, в глобальной сети Интернет, требует ее сохранения и защиты. В настоящее время существует множество различных технологий защиты информации. Они направлены на защиту носителей информации, каналы передачи данных. Второе направление составляют технологии защиты от незаконного использования чужой информации. Третье направление – это защита от изменения и кражи данных. Если в первых двух случаях можно добиться цели путем усовершенствования носителей, линий связи, схем размещения, устройств и оборудования, то защита информации от изменения является самой уязвимой. Всегда есть опасения, что данные станут доступны посторонним, которые могут ей воспользоваться или обратить во вред законному пользователю.*

Ключевые слова: *защита информации, методы кодирования, ассиметричные системы защиты, программирование.*

Информация, представленная в цифровом виде, т.е. в виде нулей и единиц, может стать доступной на любом этапе ее использования. Поэтому все чаще в настоящее время используются различные методы криптологии, науки о защите информации. Раньше приемы криптологии применялись в военных ведомствах,

служили государственным интересам. Сейчас существует множество программных продуктов, которые кодируют данные в разных сферах нашей жизни, например, защита данных клиентов банков, кодирование данных на дисках, использование электронной подписи и т. д.

Методы криптографии направлены на то, чтобы сделать данные бесполезными для посторонних. Такие изменения позволяют лишить возможности извлечения информации, а значит сохранения ее целостности.

Принципы, по которым информация может быть преобразована (закодирована), называют методами кодирования. Некоторые правила кодирования основаны на том, что сам алгоритм преобразования является секретным. Но этот трудоемкий подход в настоящее время почти не используется. Современные способы кодирования используют ключи, которые необходимы при кодировании и декодировании. Если это один и тот же ключ, то кодирование называют симметричным. Если ключ для кодирования не совпадает с ключом для дешифровки, то алгоритм называют ассиметричным. Как правило, ключи никак не связаны друг с другом. Одним из наиболее криптостойких асимметричных алгоритмов является RSA [2, с. 75].

Ассиметричные системы защиты называют криптосистемами с открытым ключом. Первый ключ может быть опубликован для всех пользователей системы. Он используется для кодирования. Другой ключ является секретным, со значением первого он никак не связан.

Алгоритм RSA предложили в 1978 г. три автора: Р. Райвест (Rivest), А. Шамир (Shamir) и А. Адлеман (Adleman). Алгоритм получил свое название по первым буквам фамилий его авторов. Алгоритм RSA стал первым полноценным алгоритмом с открытым ключом, который может работать как в режиме шифрования данных, так и в режиме электронной цифровой подписи [1, с. 127].

Алгоритм актуален тем, что опирается на использовании больших чисел, на трудности подбора чисел и выполнения вычислений. В качестве открытого ключа используется целое число К, секретным ключом является целое значение k. Отправитель, зная открытый ключ, может закодировать сообщение.

Получатель, используя закрытый ключ, выполнит декодирование. Если сообщение будет перехвачено, раскодировать его невозможно без секретного ключа k.

Для проведения кодирования задаются два произвольных взаимно простых числа P и Q, находится N – модуль: N = P*Q.

Открытый ключ K выбирают так, чтобы выполнялись условия:

$$1 < K <= F(N), \text{НОД}(K, F(N)) = 1, F(N) = (P-1)(Q-1), \quad (1)$$

где: F(N) – функция Эйлера, НОД – наибольший общий делитель. Из условия видно, что число K и функция Эйлера F(N) взаимно простые числа, а функция Эйлера F(N) указывает количество положительных целых чисел в интервале от 1 до N, которые взаимно просты с N.

Секретный ключ k подбирают таким образом, чтобы произведение чисел K*k было взаимно простым с функцией Эйлера F(N), т.е.:

$$(k*K) \bmod F(N) = 1 \quad (2)$$

Кодирование каждого символа выполняется по формуле:

$$C = M^K \bmod N, \quad (3)$$

где M – каждый символ исходного сообщения, C – результат кодирования этого символа, mod N – остаток от деления на N. Из формулы (3) видно, что если постороннему лицу известны значения C (символ закодированного сообщения), K и N, то определить M (исходный символ сообщения) практически невозможно.

Процесс декодирования выполняется по формуле:

$$M = C^k \bmod N, \quad (4)$$

где k – секретный ключ.

Зашифруем и расшифруем сообщение «привет» по алгоритму RSA. Для простоты будут использованы маленькие числа. На практике применяются очень большие числа.

1. Выберем P = 6 и Q = 5.

2. Определим N = P * Q = 6 * 5 = 30.

3. Найдем F(N) = (P – 1) * (Q – 1) = (6 – 1) * (5 – 1) = 20.

Выбираем случайным образом значение числа k. Это число должно быть взаимно простым с функцией Эйлера (т.е. k не должно иметь с числом 20 общих делителей кроме 1). Пусть k = 3 (секретный ключ).

4. Выберем число K по формуле: (k * K) mod 20 = 1, т. е. произведение k * K при целочисленном делении на F(N) = 20 должно в остатке давать 1. Пусть K = 7, т.к.: 3 * 7 = 21 и (21 mod 20) = 1 (т.е. 21:20 = 1 (ост. 1))

5. Представим шифруемое сообщение как последовательность чисел в диапазоне от 0 до 29 (кончается на N–1). Буквы в алфавитном порядке: В = 1, Е = 2, И = 3, П = 4, Р = 5, Т = 6. Исходное сообщение: М = 04 05 03 01 02 06.

6. Зашифруем сообщение, используя открытый ключ (K = 7, N = 30):

C1 = 4^7 mod 30 = 16384 mod 30 = 4 (16384: 30 = 546(ост. 4)

C2 = 5^7 mod 30 = 78125 mod 30 = 5; (78125: 30 = 2604 (ост. 5)

C3 = 3^7 mod 30 = 2187 mod 30 = 27; (2187: 30 = 72 (ост. 27)

C4 = 1^7 mod 30 = 1 mod 30 = 1; (1: 30 = 0 (ост. 1)

C5 = 2^7 mod 30 = 128 mod 30 = 8; (128: 30 = 4 (ост. 8)

C6 = 6^7 mod 30 = 279936 mod 30 = 6; (279936: 30 = 9331 (ост. 6)

Т.е. криптограмма представляет собой вид: С = 04 05 27 01 08 06

7. Расшифруем эти данные, используя закрытый ключ (k = 3, N = 30).

M1=4^3 mod 30 =64 mod 30 = 4 (П); (64: 30 = 2 (ост. 4)

M2=5^3 mod 30 =125 mod 30 = 5 (Р); (125: 30 = 4 (ост. 5)

M3=27^3 mod 30 =27 mod 30 = 3 (И); (19683: 30 = 656 (ост. 3)

M4=1^3 mod 30 =1 mod 30 = 1 (В); (1: 30 = 0 (ост. 1)

M5=8^3 mod 30 = 512 mod 30 = 2 (Е); (512: 30 = 17 (ост. 2)

M6=6^3 mod 30 = 216 mod 30 = 6 (Т); (216: 30 = 7 (ост. 6)

Сообщение расшифровано: М = 04 05 03 01 02 06.

Данный алгоритм шифрования RSA интересен тем, что может быть легко автоматизирован с помощью любого языка программирования высокого уровня, например, C++.

Далее приведен пример программного кода, который автоматизирует шифрование и дешифровку слова из шести букв. В качестве исходных данных

вводятся числа, соответствующие буквам исходного сообщения. В результате получаем номера букв, заданных при запуске кода:

```
#include <iostream>
#include <cmath>
#include <locale>
using namespace std;
int main ()
{
setlocale (LC_ALL, «Rus»);
double P, Q, N, F, k, K, A [6], C [6], M [6];
P = 6, Q = 5; // пусть P и Q произвольные
N = P * Q; F = (P – 1) * (Q – 1); k = 3; // пусть к = 3, вз простое с F
K = 7; // пусть К = 7 произвольно (К, к) mod 20 = 1
cout << «Введите слово по номерам букв» << endl;
for (int i = 0;i < 6;i ++)
{ cin >> A[i];}
cout << «Кодирование» << endl; // шифруем К = 7, N = 30
for (int i = 0; i < 6; i ++)
{ C[i] = pow(A[i],K); C[i]= (int)C[i]% (int)N; cout << «C = « << C[i] << endl;}
cout << «Декодирование» << endl; // расшифровываем к = 3, N = 30
for (int i = 0; i < 6; i++)
{M[i] = pow(C[i],k);
M[i] = (int)M[i]% (int)N; cout <<«M= « << M[i] << endl;}
return 0;}.
```

Программный код можно модернизировать, добавив функцию определения взаимно простых чисел, а также произвольного введения ключей. Необходимо также учесть использование больших чисел при объявлении переменных.

Список литературы

1. Макаренко С.И. Информационная безопасность: Учебное пособие. – Ставрополь: СФ МГГУ им. М.А. Шолохова, 2009. – 372 с.

2. Мещеряков Р.В. Информационная безопасность: Учебное пособие / Р.В. Мещеряков, Н.Ю. Хабибулина. – Томск: Изд-во Томского политехнического университета, 2015. – 134 с.