УДК 621.9-114

РАЗРАБОТКА И ОЦЕНКА РЕАЛИЗАЦИИ АЛГОРИТМА ШИФРОВАНИЯ RSA С ПРИМЕНЕНИЯ ЯЗЫКА VISUAL BASIC FOR APPLICATIONS

Д. С. Алексеева [1], **Н. А. Кононов** [2]

[1] ads.stat@mail.ru, [2] knnv.nkt@gmail.com

ФГБОУ ВО «Уфимский университет науки и технологий» (УУНиТ)

Аннотация. В статье рассматривается алгоритм шифрования *RSA* с открытым ключом. Описана реализация алгоритма в *MS Excel*, с применением языка *Visual Basic for Applications*. Проведена оценка применения офисного приложения в качестве криптографической системы.

Ключевые слова: криптография, шифрование, RSA, Excel

ВВЕДЕНИЕ

Одной из наук, тесно связанных с информационной безопасностью, является криптография.

Криптография решает многие вопросы, касающиеся контроля и целостности данных при взаимодействии сотрудников организации, а также конфиденциальности. Другими словами, криптография – это наука о шифровании данных.

Алгоритмов шифрования достаточно много, в статье рассматривается *RSA* с открытым ключом.

RSA - алгоритм, основанный на вычислительной сложности задачи факторизации больших целых чисел. Возник в 1977 году в США.

Его создатели Рональда Ривест, Ади Шамир и Леонард Адлеман, предложили всем желающим расшифровать некую фразу на английском языке. Для этого было необходимо факторизовать 129-значное десятичное число N, про которое было известно только то, что оно представляется в виде произведения двух простых сомножителей p и q, имеющих длину 65 и 64 десятичных знака.

РЕАЛИЗАЦИЯ АЛГОРИТМА В *MS EXCEL*

Для работы алгоритма необходима пара «открытый/закрытый ключ»:

1. Выбираются два простых числа p и q.

2. Вычисляется произведение $N = pq$. В реальных задачах длина N может достигать 2048 бит.

3. Вычисляется функция Эйлера $\varphi(N) = (p-1)(q-1)$.

4. Выбирается параметр e, входящий в открытый ключ RSA, равным произвольному числу, меньшему N, но взаимно простому с $\varphi(N)$.

5. Находится параметр d, по расширенному алгоритму Евклида, являющийся секретным параметром метода *RSA*, из условия $e \cdot d \mod \phi(N) = 1$.

На этом этапе пара (N, e) объявляется открытым ключом, а параметры $\phi(N)$ и d -закрытыми параметрами.

Для того, чтобы зашифровать текст по методу *RSA* необходимо разбить текст на отдельные символы. Каждому символу присваивается код c. Его шифрование производится возведением в степень: $r = enc(c) = c^e \mod N$, где пара (N, e) взяты из открытого ключа *RSA*.

Для расшифровки выполняется возведение шифра r в степень d, где d – секретный параметр *RSA*: $c=dec(r)=r^d \bmod N$.

Так как *RSA* широко используемый алгоритм его реализация подручными средствами достаточно распространенная задача.

В качестве такого подручного средства был рассмотрен *MS Excel*.

Реализация *RSA* в *Excel* начинается с реализации алгоритма Евклида.

Алгоритм Евклида используются для нахождения по заданным целым числам A и B их наибольшего общего делителя C.

Расширенный алгоритм Евклида, применяемый в *RSA*, используется также для нахождения целых чисел (x, y) таких, что выполняется условие $x \cdot A + y \cdot B = C$.

Дальнейшая реализация производится с помощью *Visual Basic for Applications*:

```
'Проверка на простоту
Function Check_prime(T As Integer) As Boolean
    Dim k As Integer
    Dim i As Integer
    Dim B As Boolean

    B = 1
    k = Int(Sqr(T))

    For i = 2 To k
        If T Mod i = 0 Then
                B = 0
                Exit For
        End If
    Next i
    Check_prime = B
End Function
```

Рис. 1 Листинг, фрагмент 1.

```
'Вычисление методом Эвклида
Function calcEvclid(numA As Integer, numB As Integer, isCheckXY As Boolean, isCheckNOD As Boolean)
    Dim modAB As Integer
    Dim divAB As Integer
    Dim ROW As Integer
    Dim maxROW As Integer
    Dim NOD As Integer
    Dim x As Integer
    Dim y As Integer

    Module1.clearEvclid

    modAB = 1
    ROW = 3
    x = 0
    y = 1

    Do While modAB > 0
        modAB = numA Mod numB
        divAB = numA \ numB
        Cells(ROW, 1).Value = numA
        Cells(ROW, 2).Value = numB
        Cells(ROW, 3).Value = modAB
        Cells(ROW, 4).Value = divAB
        numA = numB
        numB = modAB
        ROW = ROW + 1
    Loop

    ROW = ROW - 1
    Cells(ROW, 5).Value = x
    Cells(ROW, 6).Value = y

    'Покажем где НОД
    Cells(ROW + 1, 2).Value = "(НОД)"
    'Сохраним НОД, что бы потом проверить
    NOD = Cells(ROW, 2).Value
    'Сохраним номер максимальной строчки
    maxROW = ROW + 1


    ROW = ROW - 1

    Do While ROW > 2
        Cells(ROW, 5).Value = Cells(ROW + 1, 6).Value
        Cells(ROW, 6).Value = Cells(ROW + 1, 5).Value - Cells(ROW + 1, 6).Value * Cells(ROW, 4).Value
        ROW = ROW - 1
    Loop

    UserForm1.Hide

    'Если необходимо проверить XY
    If (isCheckXY = True) Then
        Cells(maxROW + 2, 2).Value = "Проверка X и Y"
        Cells(maxROW + 2, 5).Value = "=E3*L3+F3*N3"
    End If
```

Рис. 2 Листинг, фрагмент 2.

```
'Шифрование
Public Function encode(key As Integer, N As Integer) As Integer

    Dim ROW As Integer
    ROW = 3
    Do While Not IsEmpty(Cells(ROW, 18))
        Cells(ROW, 19) = AscW(Cells(ROW, 18))
        Cells(ROW, 20) = Module1.mod_exp(Cells(ROW, 19), CLng(key), CLng(N))
        ROW = ROW + 1
    Loop

    encode = 1
End Function
'ДеШифрование
Public Function decode(key As Integer, N As Integer) As Integer

    Dim ROW As Integer
    ROW = 3
    Do While Not IsEmpty(Cells(ROW, 20))
        Cells(ROW, 21) = Module1.mod_exp(Cells(ROW, 20), CLng(key), CLng(N))
        Cells(ROW, 22) = ChrW(Cells(ROW, 21))
        ROW = ROW + 1
    Loop
End Function
```

Рис. 3 Листинг, фрагмент 3.

Данный фрагмент программного код позволяет произвести шифрование слов (Рис. 4,5).

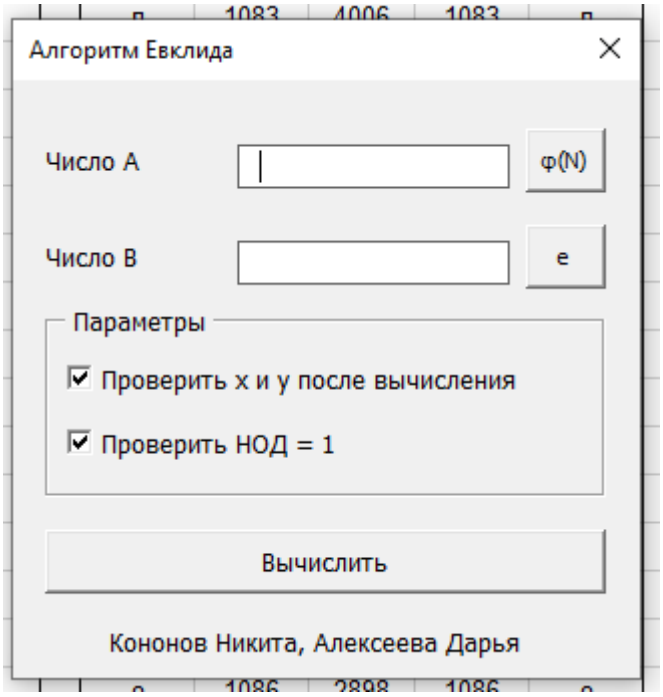

Рис. 4 Экранная форма «Алгоритм Евклида»

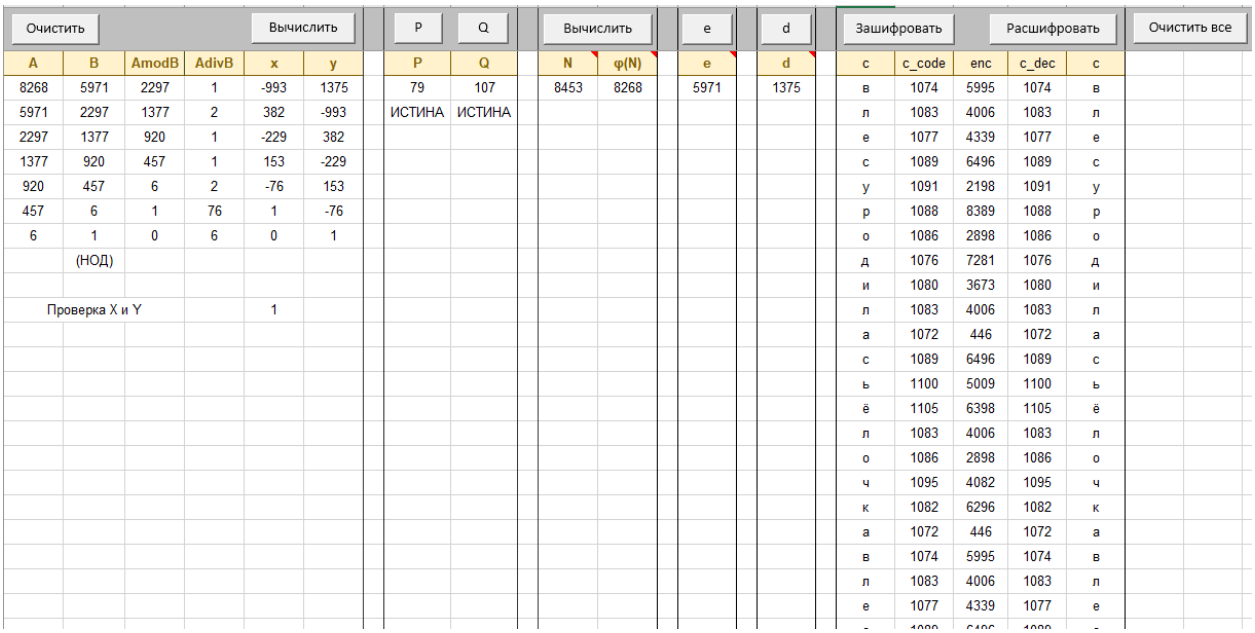

Рис. 5 Экранная форма *«RSA»*.

Как видно из выше представленного примера реализация *RSA* пакетом офисных приложений возможна и с учетом навыков программирования отнимает небольшое количество времени.

ЗАКЛЮЧЕНИЕ

Если оценивать стойкость *MS Excel*, как криптографического средства, то его можно классифицировать, как практически нестойкую криптосистему.

Плюсом является возможность работы в операционной системе *Windows*, а также минимальная сложность реализации некоторых алгоритмов шифрования. Однако это офисное приложение не обладает должным быстродействием кодирования большого объема данных и не имеет должных показателей экономической эффективности, так как вероятность взлома достаточно высока.

С момента создания алгоритма *RSA* достигнут значительный прогресс. Число, предложенное Ривестом, Шамиром и Адлеманом, разложили в 1994 году с помощью метода квадратичного решета, разработанного Карлом Померанцем и реализованного Аткинсом, Граффом, Ленстрой и Лейлендом. В работе над этим проектом участвовали около 600 добровольцев, которые работали на протяжении 7 месяцев, а также было задействовано 1700 компьютеров.

Параллельно с этим, Джоном Поллардом, был разработае «метод решета числового поля, который является наиболее быстрым на сегодняшний день. Текущий рекод составляет 1000-бит. Это делает небезопасным ключи *RSA* длиной 1024, которые являются самыми распространёнными на сегодняшний день.

Соответственно затраты, произведенные на разработку кода на основе алгоритмов шифрования и на сам лицензированный *MS Excel*, не оправдывают себя.

СПИСОК ЛИТЕРАТУРЫ

1. Антонов В.В. Методические указания по лабораторным работам «Реализация в среде Excel алгоритма RSA шифрования с открытым ключом».

2. Беляев А.В. "Методы и средства защиты информации" (курс лекций). http://www.citforum.ru/internet/infsecure/index.shtml.

3. Болотов А.А., Гашков С.Б, Фролов А.Б., Часовских А.А. «Алгоритмические основы эллиптической криптографии».

4. Учебное пособие. М.: Изд-во МЭИ. 2000 г., 100 с. Фомичев В.М. Дискретная математика и криптология, Диалог-МИФИ, 2003, 399 с.

ОБ АВТОРАХ

АЛЕКСЕЕВА Дарья Сергеевна, магистрантка 1-го курса ФИРТ.
КОНОНОВ Никита Алексеевич, магистрант 1-го курса ФИРТ.

METADATA

Title: Cryptography with excel tools at hand. Evaluation of implementation**.**

Affiliation: Ufa University of Science and Technology (UUST), Russia.

Email: [1] ads.stat@mail.ru, [2] knnv.nkt@gmail.com.

Language: Russian.

Source: Molodezhnyj Vestnik UGATU (scientific journal of Ufa University of Science and Technology), no. 1 (27), pp. 10-14, 2023. ISSN 2225-9309 (Print).

Abstract: The article discusses the RSA encryption algorithm with a public key. The implementation of the algorithm in MS Excel, using the Visual Basic for Applications language, is described. The evaluation of the use of an office application as a cryptographic system was carried.

Key words: cryptography, encryption, RSA, Excel.

About authors:

ALEKSEEVA Darya Sergeevna, postgraduate student 1 year, Ufa state aviation technical University.

KONONOV Nikita Alekseevich, postgraduate student 1 year, Ufa state aviation technical University.