**Лабораторная работа № 10-11**

Тема: «Создание пользовательской формы, реализующей алгоритм шифра RSA».

Цель: разработать пользовательскую форму, реализующую алгоритм шифра RSA.

**Контрольные вопросы**

Идентификация — это определение пользователя в автоматизированной системе по уникальному признаку — идентификатору.

Аутентификация — это процедура проверки подлинности данных о пользователе.

Механизм идентификации применим к процессам для ограничения доступа случайных и незаконных субъектов (пользователи, процессы) информационных систем к ее объектам (аппаратные, программные и информационные ресурсы).

В качестве идентификаторов при реализации механизма идентификации обычно используют набор символов (пароль, секретный ключ, персональный идентификатор и т. п.), который пользователь запоминает или для их запоминания использует специальные средства хранения (электронные ключи).

В качестве идентификаторов при реализации механизма аутентификации обычно используют набор символов (пароль, секретный ключ, персональный идентификатор и т. п.), который пользователь запоминает или для их запоминания использует специальные средства хранения (электронные ключи).

Оба механизма, идентификация и аутентификация, важны для обеспечения безопасности. Однако, постоянная аутентификация, которая обеспечивает идентификацию каждого блока передаваемых данных, может быть считана более надежной, поскольку она предохраняет данные от несанкционированной модификации или вставки.

Динамическая аутентификация использует динамические данные аутентификации, меняющиеся с каждым сеансом работы. Это обеспечивает защиту от атак, где злоумышленник может перехватить аутентификационную информацию и использовать ее в следующих сеансах работы.

Механизм аутентификации пользователя включает в себя получение от пользователя информации, удостоверяющей его личность (например, ввод пароля или предоставление пальца для сканирования отпечатка), проверку ее подлинности и затем предоставление (или не предоставление) этому пользователю возможности работы с системой.

**Практическая часть**

1 Открыть документ Microsoft Excel.

Изображение выглядит как текст, снимок экрана, программное обеспечение, компьютер

Автоматически созданное описание

Рисунок 1 – Документ.

2 Выполнить команду Сервис/Макрос/Редактор Visual Basic.

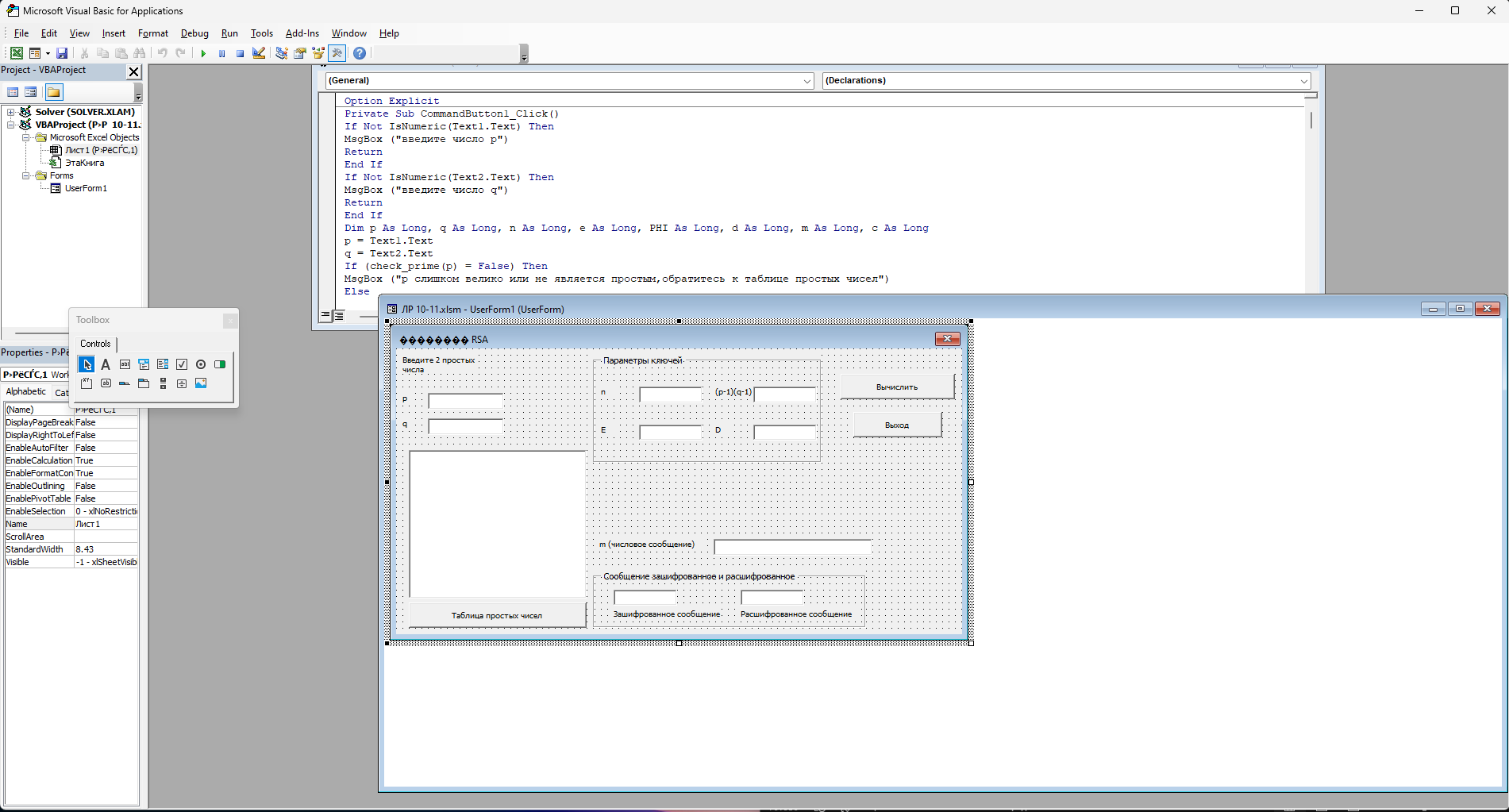


Рисунок 2 – Visual Basic.

3 Выберать команду Insert/UserForm. В редакторе Visual Basic появятся: окно пользовательской формы и панель инструментов Панель элементов.

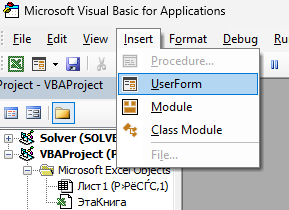


Рисунок 3 – Вставка пользовательской формы.

4 Используя диалоговое окно Свойства (для вызова этого окна, если оно отсутствует, выполните команду View/Properties Windows) и Панель элементов, простым перетаскиванием элементов управления на форму, создайте пользовательскую форму.

Изображение выглядит как текст, снимок экрана, программное обеспечение, число

Автоматически созданное описание

Рисунок 4 – Заполнение формы.

5 С созданной формой свяжите следующий программный код, обеспечивающий выполнение операций, реализуемых при нажатии на кнопках формы:

Option Explicit

Private Sub CommandButton1\_Click()

If Not IsNumeric(Text1.Text) Then

MsgBox ("введите число p")

Return

End If

If Not IsNumeric(Text2.Text) Then

MsgBox ("введите число q")

Return

End If

Dim p As Long, q As Long, n As Long, e As Long, PHI As Long, d As Long, m As Long, c As Long

p = Text1.Text

q = Text2.Text

If (check\_prime(p) = False) Then

MsgBox ("p слишком велико или не является простым,обратитесь к таблице простых чисел")

Else

If (check\_prime(q) = False) Then

MsgBox ("q слишком велико или не является простым,обратитесь к таблице простых чисел")

Else

n = p \* q

Text3.Text = n

PHI = (p - 1) \* (q - 1)

e = getE((PHI))

d = getD((e), (PHI))

Text4.Text = PHI

Text5.Text = d

Text6.Text = e

m = Text7.Text

If m > n - 1 Then MsgBox ("число m не может быть зашифровано "): GoTo 1

If m ^ e > 2147483647 Then MsgBox ("число m не может быть зашифровано, в данной программе"): GoTo 1

c = (m ^ e) Mod n

Text8.Text = c

m = decrypt(c, n, d)

Text9.Text = m

Label12.Caption = "Ключ дешифрования =<" + Str(d) + "," + Str(n) + ">"

Label13.Caption = "Ключ шифрования =<" + Str(e) + "," + Str(n) + ">"

End If

End If

1:

End Sub

Private Function check\_prime(ByVal val As Long) As Boolean

Dim primes, i As Integer, prime As Boolean

primes = Array(1, 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199, 211, 223, 227, 229, 233, 239, 241, 251, 257, 263, 269, 271, 277, 281, 283, 293, 307, 311, 313, 317, 331, 337, 347, 349, 353, 359, 367, 373, 379, 383, 389, 397)

check\_prime = False

For i = 0 To 78

If (val = primes(i)) Then

prime = True

End If

Next i

check\_prime = prime

End Function

Private Function decrypt(ByVal c As Long, ByVal n As Long, ByVal d As Long) As Long

Dim i As Long

Dim g As Long

Dim f As Long

On Error GoTo errorhandler

If (d Mod 2 = 0) Then

g = 1

Else: g = c

End If

For i = 1 To Int(d / 2)

f = c \* c Mod n

g = f \* g Mod n

Next i

decrypt = g

Exit Function

errorhandler:

Select Case Err.Number

Case 6

Status.Text = "Переполнение, задайте меньшие значения"

Case Else

Status.Text = "Ошибка вычисления"

End Select

End Function

Private Function getD(ByVal e As Long, ByVal PHI As Long) As Long

Dim u(3) As Long

Dim v(3) As Long

Dim q As Long

Dim temp1 As Long

Dim temp2 As Long

Dim temp3 As Long

u(0) = 1: u(1) = 0: u(2) = PHI: v(0) = 0: v(1) = 1: v(2) = e

While (v(2) <> 0)

q = Int(u(2) / v(2))

temp1 = u(0) - q \* v(0)

temp2 = u(1) - q \* v(1)

temp3 = u(2) - q \* v(2)

u(0) = v(0)

u(1) = v(1)

u(2) = v(2)

v(0) = temp1

v(1) = temp2

v(2) = temp3

Wend

If (u(1) < 0) Then

getD = (u(1) + PHI)

Else

getD = u(1)

End If

End Function

Private Function getE(ByVal PHI As Long) As Long

Dim great As Long

Dim e As Long

great = 0

e = 2

While (great <> 1)

e = e + 1

great = get\_common\_denom(e, PHI)

Wend

getE = e

End Function

Private Function get\_common\_denom(ByVal e As Long, ByVal PHI As Long) As Long

Dim great As Long, temp As Long, a As Long

If (e > PHI) Then

While (e Mod PHI <> 0)

temp = e Mod PHI

e = PHI

PHI = temp

Wend

great = PHI

Else

While (PHI Mod e <> 0)

a = PHI Mod e

PHI = e

e = a

Wend

great = e

End If

get\_common\_denom = great

End Function

Private Sub show\_primes()

Dim no\_primes As Long, i As Long, prime As Boolean, j As Long

Status.Text = "1"

no\_primes = 1

For i = 2 To 400

prime = True

For j = 2 To (i / 2)

If ((i Mod j) = 0) Then

prime = False

End If

Next j

If (prime = True) Then

no\_primes = no\_primes + 1

Status.Text = Status.Text + ", " + Str(i)

End If

Next i

Status.Text = Status.Text + vbCrLf + "Количество первых простых чисел:" + Str(no\_primes)

End Sub

Private Sub CommandButton2\_Click()

Unload Me

'при закрытии формы очищаем текстовые поля

Text1.Text = ""

Text2.Text = ""

Text3.Text = ""

Text4.Text = ""

Text5.Text = ""

Text6.Text = ""

Text7.Text = ""

Text8.Text = ""

Text9.Text = ""

End Sub

Private Sub CommandButton4\_Click() 'обращение к процедуре вывода простых чисел в поле формы

Call show\_primes

End Sub

6 В результате нажатия кнопки «Таблица простых чисел» диалоговое окно примет вид.

Изображение выглядит как текст, снимок экрана, дисплей, диаграмма

Автоматически созданное описаниеРисунок 5 – Результат выполнения.

7 В итоге введения исходного текста сообщения и двух простых чисел p, q после нажатия кнопки «Вычислить» диалоговое окно примет вид.

Буква З:

Изображение выглядит как текст, снимок экрана, дисплей, программное обеспечение

Автоматически созданное описание

Рисунок 6 – Буква «З».

Буква У:

Изображение выглядит как текст, снимок экрана, дисплей, диаграмма

Автоматически созданное описание

Рисунок 7 – Буква «У».

Буква Б:

Изображение выглядит как текст, снимок экрана, дисплей, программное обеспечение

Автоматически созданное описание

Рисунок 8 – Буква «Б».

8 Нажатие кнопки «Выход» приведет к закрытию формы.

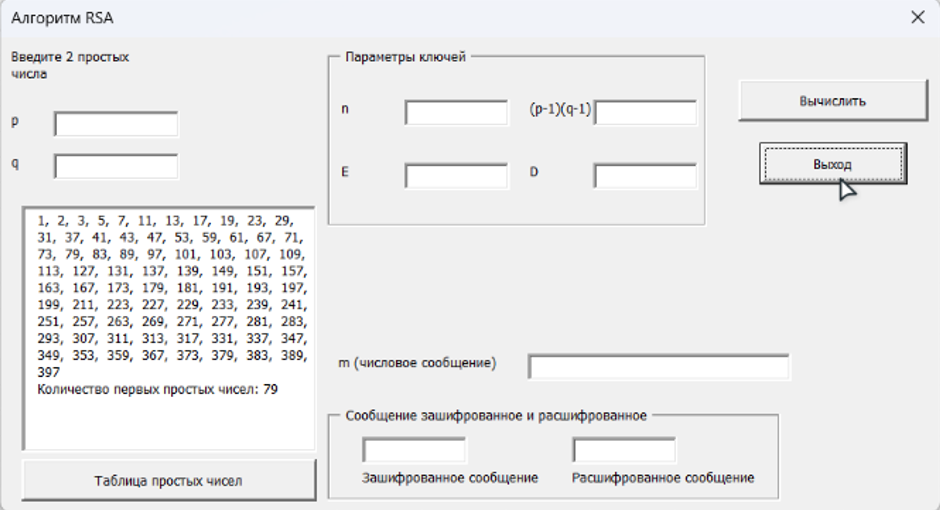


Рисунок 9 – Выход из формы.