УДК 372.862

ПРИЕМЫ ОБУЧЕНИЯ СОТРУДНИКОВ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ ОСНОВАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

М. Н. Хуторова
УО «Могилевский институт Министерства внутренних дел Республики Беларусь»,
преподаватель кафедры оперативно-розыскной деятельности факультета милиции,
магистр педагогических наук

В современном обществе наивысшую ценность представляет информация, поэтому особое внимание при подготовке сотрудников правоохранительных органов следует уделять вопросам информационной безопасности [1].

В нашей статье был проанализирован базовый алгоритм симметричного шифрования — шифр Цезаря. Для изучения данного алгоритма предлагается построение модели шифра Цезаря в табличном процессоре средствами таблицы, а затем на основании полученной модели курсантам необходимо записать код алгоритмов шифрования и дешифрования шифра Цезаря на языке программирования Visual Basic.

Остановимся подробней на основных определениях. Симметричное шифрование до 1970 г. являлось единственным в своем роде криптографическим методом шифрования. Это алгоритм шифрования данных, который применяет один ключ для расшифровки и для дешифровки данных.

Шифр Цезаря — это, наверное, самый несложный и широко известный метод шифрования. Именно поэтому начинать изучать теорию шифрования рекомендуется с данного алгоритма, так как на базе шифра Цезаря мы получим четкое представление, как работают более сложные алгоритмы шифрования.

Шифр Цезаря, простыми словами, это вид шифра подстановки или сдвига, то есть каждый символ текста, который необходимо зашифровать, заменяется символом, который размещен на определенное количество позиций левее или правее него в алфавите. Так, например, если мы будем шифровать текст со сдвигом 5, буква А изменится на Е, Б изменится на Ё и так далее.

Хотя важно отметить, что шаг шифрования, который применяется шифром Цезаря, обычно входит в состав более сложных алгоритмов шифрования, таких как алгоритм Виженера, и имеет современное приложение в системе ROT13. Также следует знать, что шифр Цезаря легко поддается взламыванию и

не применяется в «чистом виде» в современных криптографических системах [2].

Курсантам можно предложить построить математическую модель шифра Цезаря средствами табличного процессора.

Пример задания:

Постройте таблицу, которая на основе введенного побуквенно исходного текста X и ключа K (сдвига) рассчитает зашифрованный Y по шифру Цезаря текст. В шифре Цезаря каждая буква зашифрованного текста Y получается путем сдвига буквы исходного текста в алфавите на K позиций вправо.

Математически для латинского алфавита с 26 буквами это может быть записано соответственно формуле 1:

$$y_i = (x_i + K) \bmod 26, \quad (1)$$

где mod 26 означает взятие остатка от деления суммы на 26.

Поэтому каждую букву исходного текста надо последовательно перевести с помощью функции «КОДСИМВ» в числовой код СР-1251, затем вычитанием 65 получить порядковый номер буквы в латинском алфавите, затем зашифровать, снова получить номер буквы в коде СР-1251, получить букву зашифрованного текста с помощью функции «СИМВОЛ».

Для построения математической модели шифра Цезаря вам необходимо построить таблицу, представленную на рисунке 1.

	A	B	C	D	E	F	G	H	I	J	K	L	M
1	Шифр Цезаря												
2													
3	X=	V	E	N	I	V	I	D	I	V	I	C	I
4	K=	10											
5	код буквы X в СР-1251	=КОДСИМВ(B3)											
6	номер буквы X в алфавите	=B5-65											
7	номер зашифрованной буквы	=ОСТАТ(B6+B4;26)											
8	код буквы СР-1251	=B7+65											
9	Y=	=СИМВОЛ(B8)											
10													

Рис. 1. Математическая модель шифра Цезаря

При верно введенных формулах вы получите таблицу, представленную на рисунке 2.

	A	B	C	D	E	F	G	H	I	J	K	L	M
1	Шифр Цезаря												
2													
3	X=	V	E	N	I	V	I	D	I	V	I	C	I
4	K=	10											
5	код буквы X в CP-1251	86	69	78	73	86	73	68	73	86	73	209	73
6	номер буквы X в алфавите	21	4	13	8	21	8	3	8	21	8	144	8
7	номер зашифрованной буквы	5	14	23	18	5	18	13	18	5	18	24	18
8	код буквы CP-1251	70	79	88	83	70	83	78	83	70	83	89	83
9	Y=	F	O	X	S	F	S	N	S	F	S	Y	S
10													

Рис. 2. Результат вычислений математической модели шифра Цезаря

После подробного разбора математической модели шифра Цезаря целесообразно рассмотреть построение данного алгоритма средствами языка программирования Visual Basic.

Алгоритм шифрования с применением шифра Цезаря на языке Visual Basic:

```
Sub Encrypt()
    Dim Pass$, Key$
    Dim charCode As Integer
     Dim newCharCode As Integer
     Dim newChar As String
    Pass = InputBox("Введите ключ для шифрования:")
    Key = WorksheetFunction.Rept(Pass, 100)
      ' Проходимся по каждому символу в листе
    For Each cell In ActiveSheet.UsedRange
       Txt = cell.Value
       For i = 1 To Len(Txt)
         ' Получаем код символа
         charCode = Asc(Mid(txt, i, 1))
            ' Сдвигаем символ по алфавиту на длину ключа, который ввели
            newCharCode = (charCode - 65 + Pass) Mod 26 + 65
            ' Преобразуем код символа обратно в символ
            newChar = Chr(newCharCode)
      Next i
      ' Выводим зашифрованные символы на лист
       cell.Value = newChar
```

```
    Next cell
End Sub
```

Алгоритм дешифрования на языке Visual Basic:

```
Sub Decrypt()
    Dim Pass$, Key$
    Dim charCode As Integer
    Dim newCharCode As Integer
    Dim newChar As String
    Pass = InputBox(«Введите ключ для расшифровки:»)
    Key = WorksheetFunction.Rept(Pass, 100)
    For Each cell In ActiveSheet.UsedRange
        Txt = cell.Value
        For i = 1 To Len(Txt)
          charCode = Asc(Mid(Txt, i, 1))
           newCharCode = (charCode - 65 - Pass + 26) Mod 26 + 65
             newChar = Chr(newCharCode)
        Next i
        cell.Formula = newChar
    Next cell
End Sub
```

Пояснение:

Функция CHR (код знака) возвращает значение «символ» для кода ASCII ().

Функция ASC (строка) возвращает код ASCII.

Функция MID (текст; начальная позиция; кол-во символов), где текст — текст, часть которого нужно вернуть; начальная позиция — отсчитываемый слева номер первого символа, который нужно вернуть; количество символов — общее количество символов, которое нужно получить, отсчитываемое слева от значения аргумента «начальная позиция».

Оператор mod делит два числа и возвращает только остаток.

Таким образом, отработав два данных примера, курсанты получают четкое представление о таких сложных понятиях, как шифрование и криптография, и готовы к усвоению и реализации более сложных видов алгоритмов шифрования, что способствует в будущем их эффективной служебной деятельности по противодействию киберпреступности.

1. Хуторова М. Н. Методика управляемого самообучения информатике курсантов учреждений образования Министерства внутренних дел // Вестн. БРГУ. Сер. 3. Философия. Педагогика. Психология. 2021. № 1. С. 161–167. Вернуться к статье

2. Эккель Б. Философия Java. 4-е полное изд. СПб. : Питер, 2018. 1168 с. Вернуться к статье