УДК 003.26:004.056.55

СПОСОБЫ ВСТАВКИ И ИЗВЛЕЧЕНИЯ ЭЛЕМЕНТОВ ТЕКСТОВОГО ОБЪЕКТА В ЯЧЕЙКИ КЛЮЧ-МАТРИЦ МАТРИЧНЫХ И ОПЕРАТОР-МАТРИЧНЫХ МЕТОДОВ

М.Х. Гафуров

Таджикский технический университет имени академика М.С. Осими

Для защиты и обеспечения сохранности информации в информационных системах (ИС) необходимо представить и использовать новые способы и методы шифрования текстовых объектов, отвечающие требованиям времени. Новые способы и методы шифровании текстовых объектов позволяют использовать структурам обеспечивающие государственную тайну и техническую защиту информации, с учетом увеличения переписки и оборота документов с использованием сведений, содержащих государственную тайну, развития науки и техники, а также новых инициатив на пути развития государственности, разработка и реализация которых реализуются посредством секретного режима. Передача и доступ к информации в ИС осуществляется с использованием открытых и закрытых (специальных) Интернет-соединений. Поэтому, необходимо принять меры для обеспечения сохранности и защиты открытого текстового объекта от киберпреступников и от несанкционированного (незаконного) доступа в сфере государственной тайны и защиты технической информации.

В данной статье предложены способы вставки (извлечения) элементов открытого текстового объекта в ячейках ключа матричных и оператор-матричных методов шифрования открытого текстового объекта, использование которых приводит к увеличению стабильности зашифрованного объекта. В результате чего лишает киберпреступников, добывающих необходимые материалы различными путями, возможности их знакомства и использования.

Ключевые слова: *метод, объект, шифрования, зашифрования, расшифрования, элемент, символ, ключ, вариант, матрица, оператор-матрица, стабильность, киберпреступность.*

ТАРЗҲОИ ДОХИЛКУНӢ ВА ХОРИҶКУНИИ ЭЛЕМЕНТҲОИ ОБЪЕКТИ МАТНӢ ДАР ЯЧЕЙКАҲОИ КАЛИД-МАТРИТСАҲОИ УСУЛҲОИ МАТРИТСАВӢ ВА ОПЕРАТОР-МАТРИТСАВӢ

М.Ҳ. Ғафуров

Барои ҳифз ва таъмини бехатарии иттилооти дар системаҳои иттилоотӣ (СИ), зарур аст ки тарзу усулҳои нави бадалсозии объектҳои матнии ба талаботи замон ҷавобгӯ пешниҳод карда шуда, мавриди истфода қарор дода шаванд. Тарзу усулҳои нави бадалсозӣ имкон медиҳанд, ки сохторҳои таъминкунандаи сирри давлатӣ ва ҳифзи техникии иттилоот бо назардошти зиёд гардидани мукотиба ва гардиши ҳуҷҷатҳо бо истифода аз маълумоти дорои сирри давлатӣ, рушди илму техника ва ташаббусҳои нав дар роҳи рушди давлатдорӣ, ки тарҳрезӣ ва амалигардонии онҳо тавассути реҷаи махфӣ амалӣ мегарданд, истифода кунанд. Иттилооти дар СИ буда бо истифода аз алоқаи кушодаю пушидаи (махсуси) шабакаҳои гуногуни интернетӣ интиқол ва дастрас карда мешаванд. Дар таъмини бехатарӣ ва ҳифз кардани объекти кушодаи матнӣ аз киберҷиноятқорон ва аз дастрасии беиҷозат (ғайриқонунӣ) дар самти сирри давлатӣ ва ҳифзи техникии иттилоот, чораҳои зарурӣ андешидан зарур мегардад.

Дар мақолаи мазкур тарзҳои дохилкунӣ (хориҷкунӣ)-и элементҳои объекти кушодаи матнӣ дар ячейкаҳои калид-матритсаи усулҳои матритсавӣ ва оператор-матритсавии бадалсозии объекти кушодаи матнӣ пешниҳод мегардад, ки истифодаи онҳо бо баланд гардидани объекти бадалшуда меоварад. Дар натиҷа киберҷиноятқоронро, ки беиҷозат маводи зарурирро бо роҳҳои гуногун ба даст меоранд, аз шинос гардидан ва истифодаи он маҳрум месозад.

Калидвожаҳо: *усул, объект, бадалсозӣ, бадалкунӣ, аксбадалкунӣ, элемент, аломат, калид, вариант, матритса, оператор-матритса, устуворӣ, киберҷиноят.*

METHODS OF INSERTING AND EXTRACTING TEXT OBJECT ELEMENTS INTO KEY-MATRIX CELLS OF MATRIX AND OPERATOR-MATRIX METHODS

M.Kh. Gafurov

To protect and ensure the safety of information in information systems (IS), it is necessary to introduce and use new methods and techniques for encrypting text objects that meet the requirements of the time. New methods and techniques for encrypting text objects allow the use of structures that provide state secrets and technical protection of information, taking into account the increase in correspondence and circulation of documents using information containing state secrets, the development of science and technology, as well as new initiatives towards the development of statehood, the development and implementation of which are carried out through a secret regime. Transfer and access to information in the IS is carried out using open and closed (special) Internet connections. Therefore, it is necessary to take measures to ensure the safety and protection of an open text object from cybercriminals and from unauthorized (illegal) access in the field of state secrets and the protection of technical information.

This article proposes methods for inserting (extracting) elements of an open text object in the key cells of matrix and operator-matrix methods for encrypting an open text object, the use of which leads to increased stability of the encrypted object. As a result, it deprives cybercriminals who obtain the necessary materials in various ways from the opportunity to be acquainted with and use them.

Keywords: *method, object, encryption, decryption, element, symbol, key, option, matrix, matrix operator, stability, cybercrime.*

Введение

Способы определения корневых слов, слогов, приставок, суффиксов, аффиксов, биграмм, триграмм и морфологического анализа слов, на основе которых были разработаны компьютерные программы, представлены и обсуждаются в работах [1,2]. Способ выбора или создания алфавита шифрования (частного, расширенного и общего), способы разработки ключа шифрования и метод шифрования с использованием символов и знаков открытого объекта представлены в работе [3]. В [4] был представлен и рассмотрен метод шифровании с использованием элементов заданного открытого текста, в котором создается множество текстовых элементов - корневых слов, префиксов и суффиксов, слогов, орфографических и специальных символов, цифр и с их помощью разрабатывается

произвольный ключ шифрования данного текстового объекта. Шифрование открытого текстового объекта на основе текстовых элементов - биграмм и триграмм, применяемое с помощью метода Полибея, рассмотрено в [5]. Применение шифровании открытого текстового объекта на основе текстовых элементов - корневых слов, префиксов и суффиксов, слогов, орфографических и специальных символов и цифр с использованием метода Полибея представлено в [6]. В [7] рассмотрено применение шифровании открытого текстового объекта с помощью триграмм в квадрате Полибея и двойного ключа. В работе [8] представлено и обсуждено применение оператор-матричного метода шифровании с указанием способов вставки и извлечения символов и знаков в ячейках произвольного ключа, присутствующие в данном открытом текстовом объекте. В работе [9] представлены методы матричного и оператор-матричного шифрования с использованием текстовых элементов. В [10] представлен матричный метод шифровании с помощью текстовых символов и знаков, и способы их вставки и извлечения в (от) ячейки ключ-матрицы.

При выполнении операции зашифрования данного открытого текстового объекта на произвольном языке в первую очередь учитываются особенности языка текста, так как объект разбивается на элементы. С другой стороны, способ вставки и извлечения текстовых элементов - корневых слов, префиксов и суффиксов, слогов, орфографических и специальных знаков, цифр, биграмм и триграмм в ячейках ключ-матрицы не зависит от языка текста.

Алгоритм решения задач

На примере текстового объекта произвольного языка можно применять способы вставки и извлечения текстовых элементов в ячейках ключ-матрицы (корневых слов, префиксов и суффиксов, слогов, орфографических и специальных знаков, чисел, биграмм и триграмм). Предлагаем алгоритм решения задач:

Пусть текст данного открытого объекта ***W*** написан или представлен на произвольном языке.

Данный текстовый объект могут быт разделена на следующие группы элементов:

- коренные слова, префиксы и суффиксы, орфографические и специальные знаки, цифры;
- слоги;
- униграммы (символы), биграммы и триграммы.

При шифровании данного открытого текстового объекта матричным методом выбирается ключ шифровании - матрица который имеет произвольный размер и некоторые его ячеек могут быть неактивными (закрытыми). В оператор-матричном методе выбираются ключ шифровании состоящей из не менее двух матриц произвольного размеров, в каждой матрице некоторые их ячейки могут быть неактивными.

Чтобы показать процесс вставки и извлечения текстовых элементов в (от) ячейки матрицы - произвольного выбранного ключа, рассмотрим это действие в произвольной по размеру матрице.

Пусть задан произвольная матрица ***A(4,5)***. Элементы данного текстового объекта обозначено как a_{ij}, где $i = \overline{1,4}$ и $j = \overline{1,5}$ тогда, реализуем способы вставки и извлечения в (от) ячейки матрицы следующим образом (рис. 1).

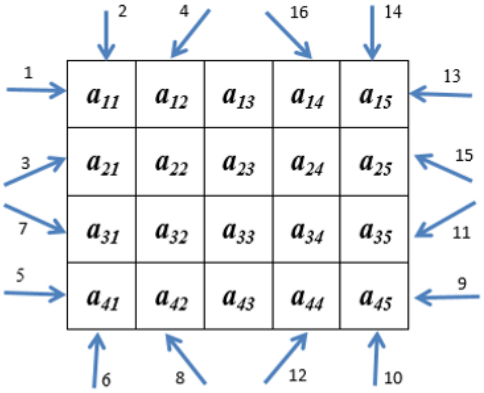

Рисунок 1 – Варианты вставки и извлечения элементов текстового объекта в (от) ячеек ключ-матрицы произвольного размера

В1. Последовательные способы вставки (извлечения) текстовых элементов в ячейки матрицы – в виде строк, столбец и диагональ (по левой и правой стороне):

1.1. a_{11} a_{12} a_{13} a_{14} a_{15} a_{21} a_{22} a_{23} a_{24} a_{25} a_{31} a_{32} a_{33} a_{34} a_{35} a_{41} a_{42} a_{43} a_{44} a_{45} - по строкам, вверху слева, слева направо;

1.2. a_{11} a_{21} a_{31} a_{41} a_{12} a_{22} a_{32} a_{42} a_{13} a_{23} a_{33} a_{43} a_{14} a_{24} a_{34} a_{44} a_{15} a_{25} a_{35} a_{45} - по столбцам, сверху слева, сверху вниз;

1.3. a_{11} a_{21} a_{12} a_{31} a_{22} a_{13} a_{41} a_{32} a_{23} a_{14} a_{42} a_{33} a_{24} a_{15} a_{43} a_{34} a_{25} a_{44} a_{35} a_{45} - по диагонали, сверху слева, снизу-вверх;

1.4. $a_{11}\ a_{12}\ a_{21}\ a_{13}\ a_{22}\ a_{31}\ a_{14}\ a_{23}\ a_{32}\ a_{41}\ a_{15}\ a_{24}\ a_{33}\ a_{42}\ a_{25}\ a_{34}\ a_{43}\ a_{35}\ a_{44}\ a_{45}$ - по диагонали, сверху слева, сверху вниз:

1.5. $a_{41}\ a_{42}\ a_{43}\ a_{44}\ a_{45}\ a_{31}\ a_{32}\ a_{33}\ a_{34}\ a_{35}\ a_{21}\ a_{22}\ a_{23}\ a_{24}\ a_{25}\ a_{11}\ a_{12}\ a_{13}\ a_{14}\ a_{15}$ - по строкам, снизу слева, слева направо;

1.6. $a_{41}\ a_{31}\ a_{21}\ a_{11}\ a_{42}\ a_{32}\ a_{22}\ a_{12}\ a_{43}\ a_{33}\ a_{23}\ a_{13}\ a_{44}\ a_{34}\ a_{24}\ a_{14}\ a_{45}\ a_{35}\ a_{25}\ a_{15}$ - по столбцам, снизу слева, снизу-вверх;

1.7. $a_{41}\ a_{31}\ a_{42}\ a_{21}\ a_{32}\ a_{43}\ a_{11}\ a_{22}\ a_{33}\ a_{44}\ a_{12}\ a_{23}\ a_{34}\ a_{45}\ a_{13}\ a_{24}\ a_{35}\ a_{14}\ a_{25}\ a_{15}$ - по диагонали, снизу слева, сверху вниз;

1.8. $a_{41}\ a_{42}\ a_{31}\ a_{43}\ a_{32}\ a_{21}\ a_{44}\ a_{33}\ a_{22}\ a_{11}\ a_{45}\ a_{34}\ a_{23}\ a_{12}\ a_{35}\ a_{24}\ a_{13}\ a_{25}\ a_{14}\ a_{15}$ - по диагонали, снизу слева, снизу-вверх:

1.9. $a_{45}\ a_{44}\ a_{43}\ a_{42}\ a_{41}\ a_{35}\ a_{34}\ a_{33}\ a_{32}\ a_{31}\ a_{25}\ a_{24}\ a_{23}\ a_{22}\ a_{21}\ a_{15}\ a_{14}\ a_{13}\ a_{12}\ a_{11}$ - по строкам, снизу справа, справа налево;

1.10. $a_{45}\ a_{35}\ a_{25}\ a_{15}\ a_{44}\ a_{34}\ a_{24}\ a_{14}\ a_{43}\ a_{33}\ a_{23}\ a_{13}\ a_{42}\ a_{32}\ a_{22}\ a_{12}\ a_{41}\ a_{31}\ a_{21}\ a_{11}$ - по столбцам, снизу справа, снизу вверх;

1.11. $a_{45}\ a_{35}\ a_{44}\ a_{25}\ a_{34}\ a_{43}\ a_{15}\ a_{24}\ a_{33}\ a_{42}\ a_{14}\ a_{23}\ a_{32}\ a_{41}\ a_{13}\ a_{22}\ a_{31}\ a_{12}\ a_{21}\ a_{11}$ - по диагонали, снизу справа, сверху вниз;

1.12. $a_{45}\ a_{44}\ a_{35}\ a_{43}\ a_{34}\ a_{25}\ a_{42}\ a_{33}\ a_{24}\ a_{15}\ a_{41}\ a_{32}\ a_{23}\ a_{14}\ a_{31}\ a_{22}\ a_{13}\ a_{21}\ a_{12}\ a_{11}$ - по диагонали, снизу справа, снизу вверх;

1.13. $a_{15}\ a_{14}\ a_{13}\ a_{12}\ a_{11}\ a_{25}\ a_{24}\ a_{23}\ a_{22}\ a_{21}\ a_{35}\ a_{34}\ a_{33}\ a_{32}\ a_{31}\ a_{45}\ a_{44}\ a_{43}\ a_{42}\ a_{41}$ - по строкам, сверху справа, справа налево;

1.14. $a_{15}\ a_{25}\ a_{35}\ a_{45}\ a_{14}\ a_{24}\ a_{34}\ a_{44}\ a_{13}\ a_{23}\ a_{33}\ a_{43}\ a_{12}\ a_{22}\ a_{32}\ a_{42}\ a_{11}\ a_{21}\ a_{31}\ a_{41}$ - по столбцам, сверху справа, сверху вниз;

1.15. $a_{15}\ a_{25}\ a_{14}\ a_{35}\ a_{24}\ a_{13}\ a_{45}\ a_{34}\ a_{23}\ a_{12}\ a_{44}\ a_{33}\ a_{22}\ a_{11}\ a_{43}\ a_{32}\ a_{21}\ a_{42}\ a_{31}\ a_{41}$ - по диагонали, сверху справа, снизу-вверх;

1.16. $a_{15}\ a_{14}\ a_{25}\ a_{13}\ a_{24}\ a_{35}\ a_{12}\ a_{23}\ a_{34}\ a_{45}\ a_{11}\ a_{22}\ a_{33}\ a_{44}\ a_{21}\ a_{32}\ a_{43}\ a_{31}\ a_{42}\ a_{41}$ - по диагонали, сверху справа, сверху вниз.

B2. Вставка (извлечение) текстовых элементов в ячейки матрицы – в виде строк, столбец и диагональ (по левой и правой стороне) по спирали:

2.1. $a_{11}\ a_{12}\ a_{13}\ a_{14}\ a_{15}\ a_{25}\ a_{24}\ a_{23}\ a_{22}\ a_{21}\ a_{31}\ a_{32}\ a_{33}\ a_{34}\ a_{35}\ a_{45}\ a_{44}\ a_{43}\ a_{42}\ a_{41}$ - по строкам, сверху слева, слева направо и по спирали;

2.2. $a_{11}\ a_{21}\ a_{31}\ a_{41}\ a_{42}\ a_{32}\ a_{22}\ a_{12}\ a_{13}\ a_{23}\ a_{33}\ a_{43}\ a_{44}\ a_{34}\ a_{24}\ a_{14}\ a_{15}\ a_{25}\ a_{35}\ a_{45}$ - по столбцам, сверху слева, сверху вниз и по спирали;

2.3. $a_{11}\ a_{12}\ a_{21}\ a_{31}\ a_{22}\ a_{13}\ a_{14}\ a_{23}\ a_{32}\ a_{41}\ a_{42}\ a_{33}\ a_{24}\ a_{15}\ a_{25}\ a_{34}\ a_{43}\ a_{44}\ a_{35}\ a_{45}$ - по диагонали, сверху слева, снизу-вверх и по спирали;

2.4. $a_{11}\ a_{21}\ a_{12}\ a_{13}\ a_{22}\ a_{31}\ a_{41}\ a_{32}\ a_{23}\ a_{14}\ a_{15}\ a_{24}\ a_{33}\ a_{42}\ a_{43}\ a_{34}\ a_{25}\ a_{35}\ a_{44}\ a_{45}$ - по диагонали, сверху слева, сверху вниз и по спирали;

2.5. $a_{41}\ a_{42}\ a_{43}\ a_{44}\ a_{45}\ a_{35}\ a_{34}\ a_{33}\ a_{32}\ a_{31}\ a_{21}\ a_{22}\ a_{23}\ a_{24}\ a_{25}\ a_{15}\ a_{14}\ a_{13}\ a_{12}\ a_{11}$ - по строкам, снизу слева, слева направо и по спирали:

2.6. $a_{41}\ a_{31}\ a_{21}\ a_{11}\ a_{12}\ a_{22}\ a_{32}\ a_{42}\ a_{43}\ a_{33}\ a_{23}\ a_{13}\ a_{14}\ a_{24}\ a_{34}\ a_{44}\ a_{45}\ a_{35}\ a_{25}\ a_{15}$ - по столбцам, снизу слева, снизу-вверх и по спирали;

2.7. $a_{41}\ a_{42}\ a_{31}\ a_{21}\ a_{32}\ a_{43}\ a_{44}\ a_{33}\ a_{22}\ a_{11}\ a_{12}\ a_{23}\ a_{34}\ a_{45}\ a_{35}\ a_{24}\ a_{13}\ a_{14}\ a_{25}\ a_{15}$ - по диагонали, снизу слева, сверху вниз и по спирали;

2.8. $a_{41}\ a_{31}\ a_{42}\ a_{43}\ a_{32}\ a_{21}\ a_{11}\ a_{22}\ a_{33}\ a_{44}\ a_{45}\ a_{34}\ a_{23}\ a_{12}\ a_{13}\ a_{24}\ a_{35}\ a_{25}\ a_{14}\ a_{15}$ - по диагонали, снизу слева, снизу-вверх и по спирали;

2.9. $a_{45}\ a_{44}\ a_{43}\ a_{42}\ a_{41}\ a_{31}\ a_{32}\ a_{33}\ a_{34}\ a_{25}\ a_{24}\ a_{23}\ a_{22}\ a_{21}\ a_{11}\ a_{12}\ a_{13}\ a_{14}\ a_{15}$ - по строкам, снизу справа, справа налево и по спирали;

2.10. $a_{45}\ a_{35}\ a_{25}\ a_{15}\ a_{14}\ a_{24}\ a_{34}\ a_{44}\ a_{43}\ a_{33}\ a_{23}\ a_{13}\ a_{12}\ a_{22}\ a_{32}\ a_{42}\ a_{41}\ a_{31}\ a_{21}\ a_{11}$ - по столбцам, снизу справа, снизу вверх и по спирали;

2.11. $a_{45}\ a_{44}\ a_{35}\ a_{25}\ a_{34}\ a_{43}\ a_{42}\ a_{33}\ a_{24}\ a_{15}\ a_{14}\ a_{23}\ a_{32}\ a_{41}\ a_{31}\ a_{22}\ a_{13}\ a_{12}\ a_{21}\ a_{11}$ - по диагонали, снизу справа, сверху вниз и по спирали;

2.12. $a_{45}\ a_{35}\ a_{44}\ a_{43}\ a_{34}\ a_{25}\ a_{15}\ a_{24}\ a_{33}\ a_{42}\ a_{41}\ a_{32}\ a_{23}\ a_{14}\ a_{13}\ a_{22}\ a_{31}\ a_{21}\ a_{12}\ a_{11}$ - по диагонали, снизу справа, снизу вверх и по спирали;

2.13. $a_{15}\ a_{14}\ a_{13}\ a_{12}\ a_{11}\ a_{21}\ a_{22}\ a_{23}\ a_{24}\ a_{25}\ a_{35}\ a_{34}\ a_{33}\ a_{32}\ a_{31}\ a_{41}\ a_{42}\ a_{43}\ a_{44}\ a_{45}$ - по строкам, сверху справа, справа налево по спирали;

2.14. $a_{15}\ a_{25}\ a_{35}\ a_{45}\ a_{44}\ a_{34}\ a_{24}\ a_{14}\ a_{13}\ a_{23}\ a_{33}\ a_{43}\ a_{42}\ a_{32}\ a_{22}\ a_{12}\ a_{11}\ a_{21}\ a_{31}\ a_{41}$ - по столбцам, сверху справа, сверху вниз и по спирали;

2.15. $a_{15}\ a_{14}\ a_{25}\ a_{35}\ a_{24}\ a_{13}\ a_{12}\ a_{23}\ a_{34}\ a_{45}\ a_{44}\ a_{33}\ a_{22}\ a_{11}\ a_{21}\ a_{32}\ a_{43}\ a_{42}\ a_{31}\ a_{41}$ - по диагонали, сверху справа, снизу вверх и по спирали;

2.16. $a_{15}\ a_{25}\ a_{14}\ a_{13}\ a_{24}\ a_{35}\ a_{45}\ a_{34}\ a_{23}\ a_{12}\ a_{11}\ a_{22}\ a_{33}\ a_{44}\ a_{43}\ a_{32}\ a_{21}\ a_{31}\ a_{42}\ a_{41}$ - по диагонали, сверху справа, сверху вниз и по спирали.

Из последовательной вставки (извлечения) текстовых элементов в (от) ячейки матрицы в случаях пунктов В1 и В2 видно, что для одного (16) способа вставки существует пятнадцать (15) произвольных способов извлечения. То есть для каждого случая вставки (извлечения) элементов имеется 240 вариантов, а всего для обоих случаев (пунктов В1 и В2) — для одного (из 32) способа вставки существует тридцать один (31) произвольных способов извлечения, всего имеются 992 вариантов вставки (извлечения) текстовых элементов в (от) ячейки матрицы.

Решение задачи на примерах

Реализуем способы вставки и извлечения текстовых элементов в оператор-матричном методе шифрования с использованием биграмм в ячейках произвольного ключа.

Пусть текст открытого объекта ***W*** имеет следующий вид (Лоик Шерали):

$$\boldsymbol{W} = \begin{Bmatrix} \text{Зарафшон меравад сӯи Бухоро,} \\ \text{Зи кӯҳи Панҷрӯд, аз чашмасорон.} \\ \text{Ба роҳаш ёдгорӣ монда ҷорист,} \\ \text{Ба нафъи халқ зар афшонда ҷорист.} \end{Bmatrix} \quad (1)$$

Чтобы разбить на левосторонние биграммы и сохранить структуру исходного объекта при выполнении расшифрования, создадим следующий вспомогательный ключ, который заменяет орфографические знаки и при необходимости знак пустоты на буквенными символами, отсутствующими в объекте. Пусть одним из вариантов вспомогательного ключа имеет следующий вид:

$$\boldsymbol{K^h} = \{\text{’} \rightarrow \boldsymbol{k}, \text{·} \rightarrow \boldsymbol{f}, \text{ˬ} \rightarrow \boldsymbol{v}, \text{↵} \rightarrow \mathbf{t}, \varnothing \rightarrow \boldsymbol{q}\} \quad (2)$$

Используя вспомогательный ключ $\boldsymbol{K^h}$, получаем данный открытый объект (1) в следующей (канонической) последовательности символов:

$$\boldsymbol{W^h} = \begin{Bmatrix} \text{ЗарафшонvмеравадvсӯиvБухороktЗиvкӯҳиvПанҷ} \\ \text{рӯдkvазvчашмасоронftБаvроҳашvёдгорӣvмондаv} \\ \text{ҷористktБаvнафъиvхалқvзарvафшондаvҷористf} \end{Bmatrix} \quad (3)$$

Теперь разделим объект (3) на левосторонние биграммы и получим следующий объект ***W1***, разделенный на биграммы:

$$\boldsymbol{W1} = \begin{Bmatrix} \text{За, ра, фш, он, vм, ер, ав, ад, vс, ӯи, vБ, ух, ор, ok, t3,} \\ \text{иv, кӯ, ҳи, vП, ан, ҷр, ӯд, kv, аз, vч, аш, ма, со, ро, нf,} \\ \text{tБ, av, ро, ҳа, шv, ёд, го, рӣ, vм, он, да, vҷ, ор, ис, тk, tБ,} \\ \text{av, на, фъ, иv, ха, лқ, vз, ар, vа, фш, он, да, vҷ, ор, ис, тf} \end{Bmatrix} \quad (4)$$

Для зашифровании открытого объекта, заданного в (1), выбираем произвольный ключ состоящей как минимум из двух матриц разных размерностей, в каждой из которых произвольные ячейки могут быть неактивными. Пусть она состоит из следующих двух матриц разной размерности ***B1(5,4)*** и ***B2(4,4)***, в которых следующие ячейки ***b1(2,3)***, ***b1(4,2)***, ***b1(5,3)*** и ***b2(2,2)***, ***b2(3,4)*** неактивны, то есть произвольно выбранный ключ шифрования объекта имеет следующий вид:

$$\boldsymbol{K1 = B1(5,4) \cup B2(4,4) - \{b1(2,3), b1(4,2), b1(5,3), b2(2,2), b2(3,4)\}} \quad (5)$$

Используя произвольный ключ (5), зашифруем данный открытый объект. Последовательно разложим биграммы, заданные в (4), приведенные в 1.5-м способом (по строкам, нижний левый, слева направо) в ячейках матрицы ***B1(5,4)*** и 2.11-м способом (по диагонали, снизу справа, сверху вниз и по спирали) в ячейках матрицы ***B2(4,4)*** и получим:

ok	tЗ	иv	кӯ
vБ	ух		ор
ав	ад	vс	ӯи
он		vм	ер
За	ра		фш

U

tБ	нf	ма	аш
ро		vч	ан
со	аз	ҷр	
kv	ӯд	vП	ҳи

тk	tБ	av	на
vҷ	ор		ис
рӣ	vм	он	да
шv		ёд	го
av	ро		ҳа

U

тf	ис	да	он
ор		фш	ха
vҷ	va	лқ	
ар	vз	иv	фъ

Теперь, способом приведенные в 1.3 (по диагонали, сверху слева, снизу-вверх) из ячеек матрицы ***B1(4,5)*** и способом 2.13 (по строкам, сверху справа, справа налево по спирали) из ячеек матрицы ***B2(4,4)*** извлечем биграммы, создав зашифрованный объект ***W2***, который имеет следующий вид:

$$\boldsymbol{W2} = \begin{Bmatrix} \text{okvБtЗавухиvонадкӯЗаvсоррavмӯиерфшашманf} \\ \text{tБроvчанҷразсokvӯдvПҳиtkvҷtБрӣоravшvvмнаav} \\ \text{онисроёддагоҳаондаистfорфшхалқvavҷарvзиvфъ} \end{Bmatrix} \quad (6)$$

Для реализации процесса расшифровании зашифрованного объекта, достаточно получить ключ шифровании (5) и зашиврованный объект (6). После зашиврованный объект (6) разделим на левосторонние биграммы, и при использовании ключа меняем операции извлечения на вставку и операции вставки на извлечения биграмм, получим объект состоящей из последовательности символов вида (3). Применяя к полученному объекту (3) вспомогательный ключ (2), в результате получим исходный открытый объект.

Вывод

1. Данные способы вставки (извлечения) текстовых символов или элементов в ячейки матрицы позволяют взломщикам не иметь возможности выполнить расшифровании зашифрованного объекта в случае определения способа использования шифрования. Возможно применение данного метода и способов создания ключей шифрования для текстового объекта произвольного языка.
2. Данные способы вставки (извлечения) текстовых символов или элементов в (из) ячеек матрицы позволяют реализовать ее для заданных текстовых элементов - корневых слов, префиксов и суффиксов, слогов, орфографических и специальных символов, чисел, биграмм и триграмм.
3. Так как в оператор-матричном методе выбираются ключ шифровании состоящей из не менее двух матриц произвольного размеров, в каждой матрице возможно произвольного выбора вариантов вставки (извлечения) текстовых символов или элементов.
4. Указанные способы вставки (извлечения) текстовых символов или элементов (992 вариантов) в (из) ячеек матриц позволяют повысить стабильность зашифрованного объекта.

Рецензент: Мирзоев С.Х. – д.т.н., профессор кафедры информатики Таджикского национального университета.

Литература

1. Усманов З.Д. Морфологический анализ словоформ таджикского языка: монография. / З.Д. Усманов, Г.М. Довудов / Душанбе: «Дониш», 2015. – 130 с.
2. Усманов, З.Д. Частотность биграмм таджикской литературы / З.Д. Усманов, А.А. Косимов // Доклады Академии наук Республики Таджикистан. - 2016. -т.59. -№1-2. -С.28-32.
3. Гафуров М.Х. Шифрование текстового объекта при использовании языковых символов (на тадж. яз.) / М.Х. Гафуров // Политехнический вестник. Серия: Интеллект. Инновации. Инвестиции. 2020. № 4 (52). С.31-35.
4. Гафуров М.Х. Об одном способе шифрования объекта с использованием элементов языка / М.Х. Гафуров // Политехнический вестник. Серия: Интеллект. Инновации. Инвестиции. 2023. №2 (62). С.22-29.
5. Гафуров М.Х. Применение биграмм и триграмм при шифровании объекта с использованием квадрата Полибея / М. Х. Гафуров // Политехнический вестник. Серия: Интеллект. Инновации. Инвестиции. 2024. № 1 (65). С. 72-75.
6. Гафуров М.Х. Операторное применение шифрования элементов языка с квадратом Полибея / М.Х. Гафуров // Вестник Технологического университета Таджикистана. 2024. № 1 (56). С.159-164.

7. Gafurov, M. Application of trigrams in encryption of objects using the Polybius square and a double key / M. Gafurov, A. Radjabova, R. Giyosov // Вестник Таджикского национального университета. Серия социально-экономических и общественных наук. 2024. Vol. 2024, № 3. - DOI 10.62965/tnu.sns.2024.3.16.

8. Гафуров М.Х. Шифрование объекта оператор-матричным методом / М. Х. Гафуров // Общественная безопасность, законность и правопорядок в III тысячелетии. 2018. № 4-2. С. 14-21.

9. Гафуров М.Х. Шифрование элементов текста матричным и оператор - матричным методами / М. Х. Гафуров // Политехнический вестник. Серия: Интеллект. Инновации. Инвестиции. 2024. № 4 (68). С. 30-35.

10. https://www.cyberforum.ru/php-beginners/thread1879116.html - электронный ресурс. (дата обращения 07.02.2025).

МАЪЛУМОТ ДАР БОРАИ МУАЛЛИФ - СВЕДЕНИЯ ОБ АВТОРЕ – INFORMATION ABOUT THE AUTHOR

TJ	RU	EN
Ғафуров Миршафи Ҳамитович	Гафуров Миршафи Хамитович	Gafurov Mirshafi Khamitovich
н.и.т., дотсент	к.т.н., доцент	Candidate of technical sciences, associate professor
Донишгоҳи техникии Тоҷикистон ба номи академик М.С. Осимӣ	Таджикский технический университет имени академика М.С. Осими	Tajik technical university named after academician M.S. Osimi
E-mail: mirugaf56@gmail.com		