УДК 338.244.4

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА, КАК ОСНОВА СТАБИЛЬНОСТИ ЦИФРОВОЙ ЭКОНОМИКИ

CRYPTOGRAPHIC PROTECTION AS A BASIS OF STABILITY DIGITAL ECONOMY

Р.М. АЛОЯН, В.В. ШУТЕНКО, О.И. НИКИТИНА, Л.С. МИЗГИРЕВ
R.M. ALOYAN, V.V. SHUTENKO, O.I. NIKITINA, L.S. MIZGIREV

(Ивановский государственный политехнический университет)
(Ivanovo State Polytechnical University)
E-mail: schutenkovv@gmail.com

В статье рассматривается вариант обеспечения криптографической защиты информации в условиях динамично развивающейся цифровой экономики с применением метода многоалфавитной подстановки шифра Виженера для симметричного шифрования информации с закрытым ключом. Целью исследований является создание шифровальщика Виженера на языке программирования Python для практического использования криптографических методов защиты экономической и финансовой информации.

The article considers the option of providing cryptographic protection of information in a dynamically developing digital economy, using the method of multi-alphanum substitution of Vigenère cipher, for symmetric encryption of information with a private key. The aim of the research is to create a cryptographer Vigenber in the Python programming language for practical use of cryptographic methods of information protection.

Ключевые слова: цифровая экономика, криптография, защита информации, шифрование, метод Виженера, Python.

Keywords: digital economy, cryptography, information protection, encryption, Vigenère method, Python.

В целях реализации Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы, утвержденной Указом Президента Российской Федерации от 09.05.2017 № 203 "О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы", распоряжением Правительства Российской Федерации от 28.07.2017 № 1632-р утверждена Программа "Цифровая экономика Российской Федерации", направленная на создание условий для развития общества знаний в Российской Федерации, повышение благосостояния и качества жизни граж-

дан нашей страны путем повышения доступности и качества товаров и услуг, произведенных в цифровой экономике с использованием современных цифровых технологий, повышения степени информированности и цифровой грамотности, улучшения доступности и качества государственных услуг для граждан, а также безопасности как внутри страны, так и за ее пределами.

Гарантия безопасности информационного потока обеспечивается криптографией путем защиты и сохранения тайны переданной информации, реализуемой различными способами: ограничить физический доступ к информационным потокам, скрыть каналы передачи, создать физические трудности подключения к линиям связи и т.д. Криптография обеспечивает целостную недоступность канала передачи для мошенников и гарантирует конфиденциальность и подлинность данных при помощи алгоритмов шифрования, ограничивающих доступность информации для доступа третьих лиц. Система современной криптографической защиты информации реализуется программно-аппаратным комплексом, гарантирующим защиту информации с позиции конфиденциальности, целостности, аутентификации, авторства [1].

В различные времена криптографией занимались Пифагор, Аристотель, Платон, Галилей, Д. Порта, Д. Кардано, Л. да Винчи, Ф. Виет, Д. Валлис, Б. Паскаль, И. Ньютон, Ф. Бекон, Х. Гольбах, Ф. Эпинус, Л. Эйлер, П.Ф. Шиллинг, Ч. Беббидж и другие.

Цель проведенного исследования в создании шифровальщика Виженера путем выбора алфавита для шифрования, языка программирования и написания на нем шифровальщика.

Метод Виженера относят к простейшим методам симметричного шифрования с закрытым ключом. В целях маскировки естественной частотной статистики исходного языка на практике применяется многоалфавитная подстановка, которая бывает нескольких видов. В многоалфавитных подстановках для замены символов исходного текста используется не один, а несколько алфавитов [2]. Обычно алфавиты для замены образованы из символов исходного алфавита, записанных в другом порядке.

Примером многоалфавитной подстановки может служить схема, основанная на использовании таблицы Виженера. Метод был описан французом Блезом Виженером в "Трактате о шифрах", вышедшем в 1585 г.

В созданном в рамках исследования шифровальщике Виженера используется русский алфавит и две цифры: АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ12. Дополнительно указанный шифровальщик, обрабатывая весь спектр заданных символов, кроме пробела, автоматически переводит строчные буквы в прописные.

Методы многоалфавитной подстановки, в том числе и метод Виженера, фактически недоступны "ручному" криптоанализу. Для вскрытия методов многоалфавитной замены разработаны специальные, достаточно сложные алгоритмы. Машинные методы обработки позволяют реализовать вскрытие метода многоалфавитной подстановки быстро и оперативно благодаря высокой скорости проводимых операций и расчетов [3].

Поставленная в исследовании задача создания программы шифрования по методу Виженера может быть решена с использованием различных языков программирования. Для реализации выбран сравнительно новый язык программирования Python (пайтон), созданный Гвидо ванн Россумом (GuidovanRossum) в начале 90-х годов 20-го века. Он является интерпретируемым, изначально объектно-ориентированным языком программирования, он прост, содержит небольшое число ключевых слов, вместе с тем очень гибок и выразителен [4]. Это язык более высокого уровня по сравнению с Pascal, C, C++, что достигается, в первую очередь, за счет встроенных высокоуровневых структур данных (списки, словари, тьюплы).

Среди преимуществ языка Python, повлиявших на его выбор [5], выделим:

— открытая разработка;

— простота в изучении, особенно на начальном этапе;

— особенности синтаксиса, формирующие хорошо читаемый код;

— предоставляет средства быстрого прототипирования и динамической семантики;

— имеет большое сообщество, позитивно настроенное по отношению к новичкам;

— множество полезных библиотек и расширений языка можно легко использовать в своих проектах благодаря предельно унифицированному механизму импорта и программным интерфейсам;

— механизмы модульности хорошо продуманы и могут быть легко использованы;

— абсолютно все в Python является объектами в смысле ООП, но при этом объектный подход не навязывается программисту.

Листинг. *Фрагменты кода программы* (ссылка на шифровальщик Виженера: https://levchcode.github.io/vcipher/)

```
        functionsearchStringInArray (str, strArray)
        {
        for (var j=0; j<strArray.length; j++)
           {
        if (strArray[j].startsWith(str)) return j;
        }
        return -1;
        }

        //Отвечает за шифрование
        functioncipher(){

        //Получаем ключ, текст и алфавит из текстовых полей
        key = document.getElementById('key').value.toLocaleUpperCase()
        txt = document.getElementById('text').value.toLocaleUpperCase()

        var alphabets = []
        var result = ""
        init_alphabet = document.getElementById('alph').value.toLocaleUpperCase()

        if(init_alphabet === '')
        {
                for (vari = 1040; i< 1072; i++)
{
                        init_alphabet += String.fromCharCode(i);
                }
        }

        alphabets.push(init_alphabet)

        // Создаем алфавиты со сдвигом в соответствии с ключом
        for (i = 0; i<key.length; i++) {
                alphabets.push(key[i] + init_alphabet.split(key[i])[1] + init_alphabet.split(key[i])[0])
        }

        var aux = ""
        for (i = 0; i<txt.length; i = i + key.length) {
                aux += key;
        }

        aux = aux.substr(0, txt.length)

        //Шифруем
        for (i = 0; i<txt.length; i++) {

                varpos = alphabets[0].search(txt[i])
                varline_pos = searchStringInArray(aux[i], alphabets)
                result += alphabets[line_pos].charAt(pos)
        }

        document.getElementById('r').innerHTML = result
    }

    //Отвечает за расшифровку
    functiondecipher()
    {
        //Получаем ключ, текст и алфавит из текстовых полей
        key = document.getElementById('key').value.toLocaleUpperCase()
        txt = document.getElementById('text').value.toLocaleUpperCase()
```

```
        var alphabets = []
        varinit_alphabet = document.getEle-
mentById('alph').value.toLocaleUpperCase()
        var result = ""

        if(init_alphabet === '')
        {
                for (vari = 1040; i< 1072; i++)
{
                        init_alphabet +=
String.fromCharCode(i);
                }
        }

        alphabets.push(init_alphabet)

        // Создаем алфавиты со сдвигом в
соответствии с ключом
        for (i = 0; i<key.length; i++) {
                alphabets.push(key[i] +
init_alphabet.split(key[i])[1] + init_alpha-
bet.split(key[i])[0])
        }

        var aux = ""
        for (i = 0; i<txt.length; i = i +
key.length) {
                aux += key;
        }

        aux = aux.substr(0, txt.length)

        //Расшифровываем
        for (i = 0; i<txt.length; i++)
        {
                varline_pos = searchStringI-
nArray(aux[i], alphabets)
                varpos = alpha-
bets[line_pos].search(txt[i])
                result += alphabets[0].cha-
rAt(pos)
        }

        document.getElementById('r').in-
nerHTML = result
```

Рассмотрим примеры использования созданной программы шифровальщика Виженера.

1 случай: шифрование. Ключ: ДЕНЬ
Текст: МОЙДЯДЯСАМЫХЧЕСТНЫХПРАВИЛ
Шифр: РУЧ1АИЙКДСЁОЫЙЯЛС1АИФЕПВП

2 случай: дешифрование. Ключ: УТРО
Шифр: П3ЯЫ2НЕ3Ч1ЯУ1ХЮЭХЧЮЗШ
Текст: ЯПОМНЮЧУДНОЕМГНОВЕННЬЕ

ВЫВОДЫ

Результаты проведенных исследований свидетельствуют о возможности использования шифровальщика Виженера как для шифрования, так и для дешифрования информационного потока экономического и финансового содержания простейшим методом симметричного шифрования с закрытым ключом с многоалфавитной подстановкой.

ЛИТЕРАТУРА

1. *Алоян Р.М., Филимонова Н.М., Петрухин А.Б., Капустина Н.В.* Управление логистическими факторами риска в процессе организации производства // Изв. вузов. Технология текстильной промышленности. – 2017, № 4. С. 94...97.

2. *Алоян Р.М., Шутенко В.В.* Разработка информационного сопровождения оценки качества государственных образовательных услуг, предоставляемых вузом // Изв. вузов. Технология текстильной промышленности. – 2016, № 5. С. 5...10.

3. *Алоян Р.М., Татиевский П.Б., Федосеев В.Н.* Практика использования информационно-аналитических технологий (ИАТ) для принятия управленческих решений в режиме "On-Line" // Интеграл – М.: ООО НПЦ "Энергоинвест", 2013, № 1-2. С. 56...58.

4. *Андреева О.Р., Зайцева И.А., Шутенко В.В.* Выбор приоритетных направлений инновационного развития социальной сферы на основе использования метода анализа иерархий // Современные наукоемкие технологии. Региональное приложение. – Иваново: ИГХТУ, 2013, № 4 (36). С. 16...23.

5. *Андреева О.Р., Зайцева И.А., Шутенко В.В.* Оценка качества подачи тепловой энергии на основе метода анализа иерархий в программной системе "Mpriority" // Современные наукоемкие технологии. Региональное приложение. – Иваново: ИГХТУ, 2014, № 1. С. 30...37.

R E F E R E N C E S

1. Alojan R.M., Filimonova N.M., Petruhin A.B., Kapustina N.V. Upravlenie logisticheskimi faktorami riska v processe organizacii proizvodstva // Izv. vuzov. Tehnologija tekstil'noj promyshlennosti. – 2017, № 4. S.94...97.

2. Alojan R.M., Shutenko V.V. Razrabotka informacionnogo soprovozhdenija ocenki kachestva gosudarstvennyh obrazovatel'nyh uslug, predos-tavljaemyh vuzom // Izv. vuzov. Tehnologija tekstil'noj promyshlennosti. – 2016, № 5. S. 5...10.

3. Alojan R.M., Tatievskij P.B., Fedoseev V.N. Praktika ispol'zovanija informacionno-analiticheskih tehnologij (IAT) dlja prinjatija upravlencheskih reshenij v rezhime "On-Line" // Integral – M.: OOO NPC "Jenergoinvest", 2013, № 1-2. S. 56...58.

4. Andreeva O.R., Zajceva I.A., Shutenko V.V. Vybor prioritetnyh napravlenij innovacionnogo razvitija social'noj sfery na osnove ispol'zovanija metoda analiza ierarhij // Sovremennye naukoemkie tehnologii. Regional'noe prilozhenie. – Ivanovo: IGHTU, 2013, № 4 (36). S. 16...23.

5. Andreeva O.R., Zajceva I.A., Shutenko V.V. Ocenka kachestva podachi teplovoj jenergii na osnove metoda analiza ierarhij v programmnoj sisteme "Mpriority" // Sovremennye naukoemkie tehnologii. Regional'noe prilozhenie. – Ivanovo: IGHTU, 2014, № 1. S.30...37.

Рекомендована кафедрой информационных систем и технологий. Поступила 25.10.17.