В общем случае эта гипотеза до сих пор не доказана и не опровергнута, хотя существует много работ, ей посвященных. Такое положение дел свидетельствует о том, что, с одной стороны, рассматриваемая гипотеза интересна специалистам в области графов, а с другой стороны, достаточно сложна, чтобы оставаться недоказанной вот уже более тридцати лет.

В 2015-2016 годах, начав с некоторых идей из работы [2] и продолжая постепенное их обобщение, D. Cranston совместно с китайскими математиками Y.-C. Liang, X. Zhu, F. Chang, Z. Pan [3, 4, 5] получили, пожалуй, наиболее красивый и существенный результат по гипотезе Хартсфилд-Рингеля на сегодняшний момент:

Все регулярные графы – антимагические.

В 2014 году автором настоящего доклада была доказана [6] *антимагичность унографов*, обладающих, помимо прочего, интересной особенностью: они либо регулярны, либо “почти” регулярны, т.е. имеют одну вершину, степень которой отлична от остальных. В сочетании с вышеупомянутыми работами по антимагичности всех регулярных графов вообще, это подсказывает, что можно искать удобные для исследования классы среди “почти” регулярных графов. И, в то время как общая задача доказательства гипотезы для таких графов представляется непростой (равно как и точное определение, что же именно считать “почти” регулярными графами), автором был найден пример содержательного антимагического класса подобных графов, а именно *fork-join графы* [7].

Доказана антимагичность fork-join графов. В рамках доказательства приведены алгоритмы, строящие для fork-join графов антимагическую нумерацию в зависимости от их структуры.

Список цитируемых источников

1. Hartsfield, N. Pearls in Graph Theory: A Comprehensive Introduction / N. Hartsfield, G. Ringel. – Academic Press, Inc., Boston, 1990. – 246 p.

2. Dense graphs are antimagic / N. Alon [et al.] // J. Graph Theory. – 2004. – Vol. 47. – P. 297–309.

3. Cranston, D. W. Regular bipartite graphs are antimagic/ D. W. Cranston // J. Graph Theory. – 2009. – Vol. 60. – P. 173–182.

4. Cranston, D. W. Odd degree regular bipartite graphs are anti-magic / D. W. Cranston, Y. Liang, X. Zhu // J. Graph Theory. – 2015. – Vol. 80(1). – P. 28–33.

5. Antimagic labeling of regular graphs / F. Chang [et al.] // J. Graph Theory. – 2016. – Vol. 82. – P. 339–349.

6. Калачев, В. Н. К гипотезе Хартсфилда-Рингеля: связные унографы / В. Н. Калачев // Труды института математики. – 2014. – Т. 22, № 2. – С. 46–52.

7. Калачев, В. Н. Fork-join графы антимагические / В. Н. Калачев // Труды института математики. – 2017. – Т. 25, № 2. – С. 21–28.

УДК 004.056.5

МОНОФОНИЧЕСКАЯ ЗАМЕНА КАК ЧАСТНЫЙ СЛУЧАЙ ПОЛИАЛФАВИТНОЙ ЗАМЕНЫ И ЕЁ ОСОБЕННОСТИ

А.И. Калько
Барановичский государственный университет, Барановичи, Беларусь

MONOALPHABETIC SUBSTITUTION AS A SPECIAL CASE OF POLYALPHABETIC SUBSTITUTION AND ITS FEATURES

A.I. Kalko
Baranovichi State University, Baranovichi, Belarus

Аннотация. Статья рассматривает монофоническую замену как частный случай полиалфавитной замены и её особенности, включая выравнивание частот появления символов для усложнения криптоанализа.

Ключевые слова: монофоническая замена, шифрование, криптоанализ, частотный анализ, оптимизация.

Annotation. The article examines monoalphabetic substitution as a special case of polyalphabetic substitution and its features, including equalizing the frequencies of character appearances to enhance cryptographic security.

Keywords: monoalphabetic substitution, encryption, cryptanalysis, frequency analysis, optimization.

Монофоническая замена, как частный случай полиалфавитной замены, имеет свои особенности. В этом методе количество и состав алфавитов подбираются таким образом, чтобы частоты появления символов в зашифрованном тексте были одинаковыми. Это делает криптоанализ зашифрованного текста сложным, так как статистическая обработка текста не дает явных результатов. Для достижения равномерной частоты появления символов используется разное количество заменяющих элементов для часто и редко встречающихся символов исходного текста.

Процесс шифрования подобен простой замене, за исключением того, что после шифрования каждого символа соответствующий ему столбец алфавитов сдвигается циклически вверх на одну позицию. Таким образом, столбцы алфавита формируют независимые друг от друга кольца, которые поворачиваются вверх на один знак после каждого шифрования.

Зашифруем монофоническим шифром следующий текст большей длинны:

«Проснувшись однажды утром после беспокойного сна, Грегор Замза обнаружил,что он у себя в постели превратился в страшное насекомое.Лежа на панцирнотвердой спине, он видел, стоило ему приподнять голову, свой коричневый, выпуклый,разделенный дугообразными чешуйками живот, на верхушке которого еле держалось готовое вот-вот окончательно сползти одеяло. Его многочисленные, убого тонкие по сравнению с остальным телом ножки беспомощно копошились у него перед глазами.»

Анализ частот последующего текста, представленный в виде графика на рисунке 1.

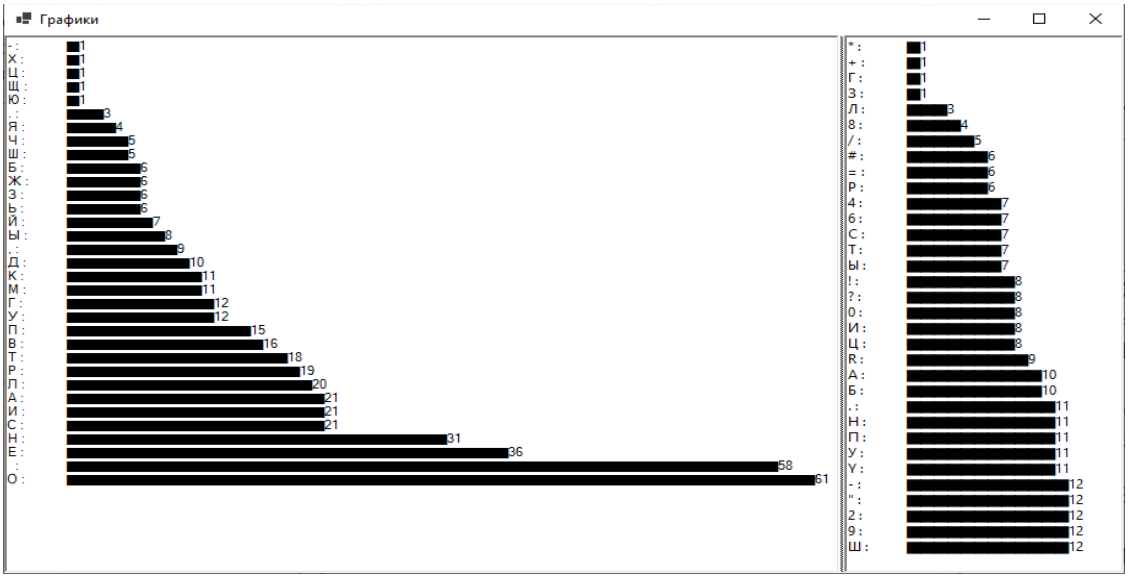

Рисунок 1 – Частота символов в тексте

График построен в виде столбиковой диаграммы с помощью символов. От частоты встречаемости символа зависит длина столбца. Столбцы сформированы с помощью символа "". Число в конце столбца показывает сколько раз символ встречается в тексте.

Для оптимизации программы при шифровании длинного текста была сформирована функция сглаживания для частоты встречаемости символа в тексте [1]. Функция представляет собой модифицированную сигмоидальную функцию:

$$\frac{4}{1+e^{-\left(\frac{n}{m}-0.5\right)\cdot 8}}+1,$$

где n – сколько раз символ встречается в тексте, m – наибольшее число повторений одного символа в тексте.

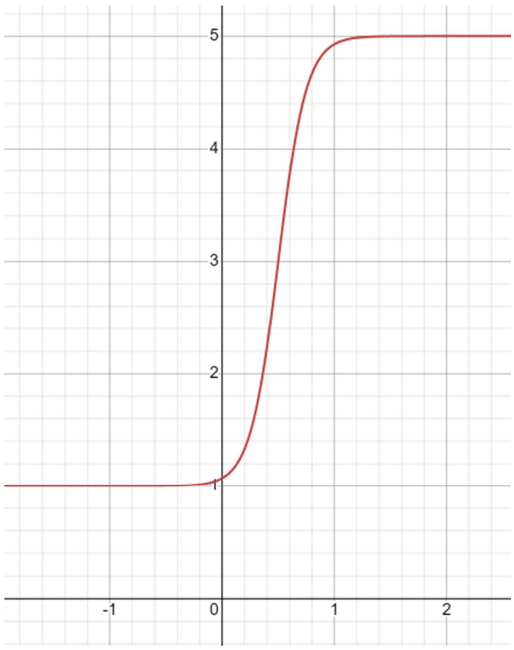

Рисунок 2 – График оптимизации

Таким образом максимальное количество заменяющих символов равно пяти, а минимальное одному. Чем чаще символ встречается относительно других, тем ближе число заменяющих символов будет к максимальному.

Для увеличения максимального количества заменяющих символов достаточно увеличить числитель. Для увеличения чувствительности функции можно заменить число восемь на большее.

Список цитируемых источников

1. Сандруцкий, Д. И. Применение криптографических систем при создании мессенджера / Д. И. Сандруцкий, С. Д. Колдушко, А. И. Калько // Студенческий. – 2017. – № 16(16). – С. 14–16. – EDN KFGYYP.

УДК 004.42

МАНИФЕСТ РЕАКТИВОГО ПРОГРАММИРОВАНИЯ

В.А. Литвинова
Белорусский государственный университет информатики и радиоэлектроники,
г. Минск, Беларусь

THE REACTIVE MANIFESTO

V.A. Litvinava
Belarusian State University of Informatics and Radioelectronics, Minsk, Belarus

Аннотация. В данной работе рассмотрено понятие реактивного программирования. Рассмотрен манифест реактивных систем и представлена его схема. Рассмотрена полезность реактивных системы, методы и средства ее достижения. Рассмотрена формулировка закона Д. Амдала 1967 г.

Ключевые слова: реактивность, реактивное программирование, манифест реактивных систем, отзывчивость, эластичность, отказоустойчивость, обмен сообщениям, событийно-ориентированный подход закон Джина Амдала.