ЧАСТОТНЫЙ АНАЛИЗ КАК СРЕДСТВО МАТЕМАТИЧЕСКОЙ АТАКИ НА АСИММЕТРИЧНЫЙ АЛГОРИТМ RSA

А.В.Бозняков

Научный руководитель: доцент, к.ф.-м.н. М.Е. Семенов

Национальный исследовательский Томский политехнический университет,

Россия, г.Томск, пр. Ленина, 30, 634050

E-mail: anton1993-08@mail.ru

FREQUENCY ANALYSIS AS A MEAN OF MATHEMATICAL ATTACK ON ASYMMETRIC ALGORITHM RSA

A.V. Boznyakov

Scientific Supervisor: PhD, Associate prof. M.E. Semenov

Tomsk Polytechnic University, Russia, Tomsk, Lenin str., 30, 634050

E-mail: anton1993-08@mail.ru

Abstract. *In this paper we describe a method of mathematical attack on the RSA cipher, which is called the method of frequency analysis of the encrypted message. The main idea of this method is comparison a frequency of encrypted text elements and a frequency distribution of the English alphabet. The frequency distribution of the letters of the English alphabet on different original texts and the frequency distribution of the encrypted message elements were calculated. The minimum length of the encrypted message have been determined that can be decrypted without the key. This result was confirmed with statistical hypothesis testing using the chi-square test.*

Криптографическая система с открытым ключом – это система шифрования данных, при которой открытый ключ передаётся по открытому каналу и используется для шифрования сообщения. Для расшифровки сообщения используется закрытый ключ [1].

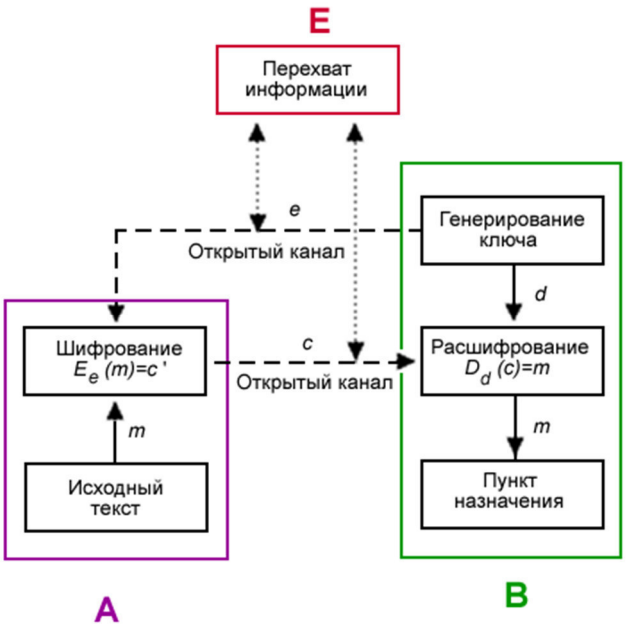

Рис.1. Схема асимметричного алгоритма шифрования

Криптосистема с открытым ключом определяется тремя алгоритмами: генерации ключей, шифрования и дешифрования. Алгоритм генерации ключей открыт, всякий может подать ему на вход случайную строку r надлежащей длины и получить пару ключей ($k1$, $k2$). Один из ключей (например, $k1$) публикуется, он называется *открытым*, а второй, называемый *секретным*, хранится в тайне. Алгоритмы шифрования E_{k1} и дешифрования D_{k2} таковы, что для любого открытого текста m справедливо [2, 3]:

$$D_{k2}(E_{k1}(m)) = m\,. \qquad (1)$$

Стойкость алгоритма базируется на сложности факторизации больших простых чисел [1]. В данном методе применяются следующие формулы для преобразования информации:

Формула шифрования: $C = M^e \bmod(n)$. (2)

Формула дешифрования: $M = E^e \bmod(n)$. (3)

В данной работе был проведен частотный анализ сообщения, зашифрованного методом RSA [2, 4]. Для начала был зашифрован текст длиной 400 знаков, затем длина текста уменьшалась. Это проводится для того, чтобы определить минимальную длину шифрованного сообщения, которую можно расшифровать без использования ключа. Была определена частота каждого элемента в шифрованном тексте, за тем полученные частоты были отсортированы по убыванию и сравнивались с эталонной частотой для установки соответствия шифрованного элемента и буквы алфавита.

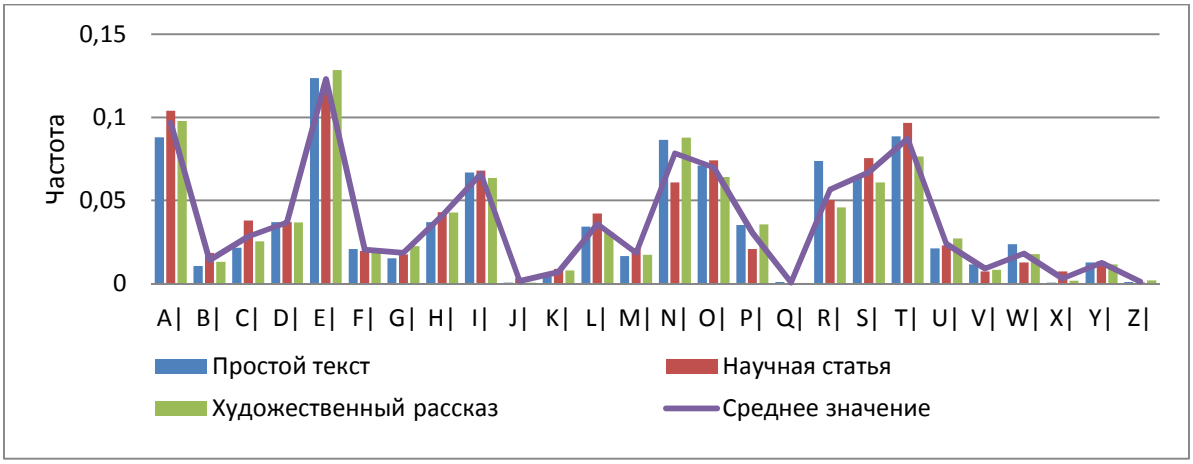

Рис.2. Распределение частот букв английского алфавита

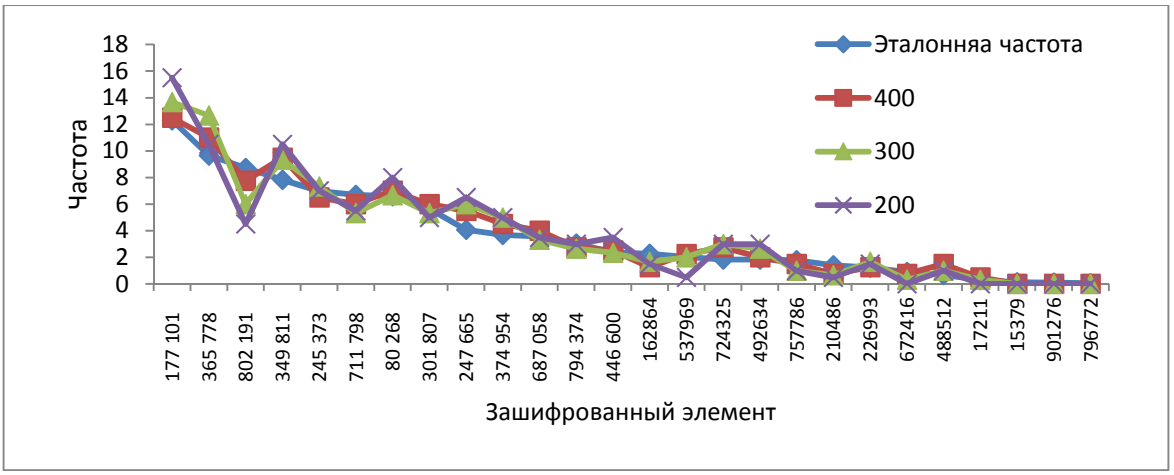

Рис.3. График распределения частот шифрованных элементов

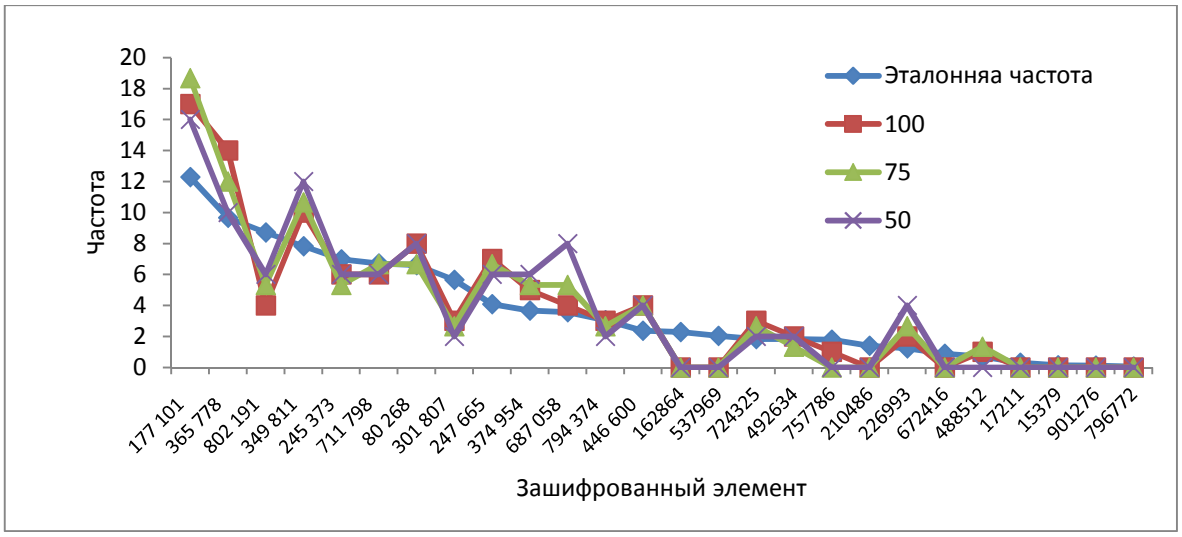

Рис. 4. График распределения частот шифрованных элементов

Как можно заметить, при достаточной длине шифрованного текста, частота шифрованных элементов достаточно близка к эталонной частоте букв алфавита, но с уменьшением длины текста проявляется существенное отклонение. Воспользуемся критерием χ-квадрат, который устанавливает, подчиняется ли некоторое экспериментально распределение теоретическому закону. Для этого было рассчитано значение статистки χ-квадрат для распределения частот и критическое значение, критическое значение статистики равно 16,611, число степеней свободы равно 25, доверительная вероятность 0,95 (табл. 1).

Таблица 1

Расчет статистики χ-квадрат

Длина сообщения	Значение статистики	Длина сообщения	Значение статистики
400	6,580	100	23,319
300	11,046	75	23,620
200	16,195	50	30,575

Таким образом, приходим к выводу, что методом частотного анализа можно расшифровать текст, длиной не менее 300 знаков.

СПИСОК ЛИТЕРАТУРЫ

1. Саломаа А. Криптография с открытым ключом. – М.: Мир, 1995. – 318 с.
2. Яковлев А.В. Криптографическая защита информации: учебное пособие/ Яковлев А.В., Безбогов А.А., Родин В.В., Шамкин В.Н. – Тамбов: Изд-во Тамб. гос. техн. ун-та, 2006. – 140 с.
3. Онацкий А.В., Йона Л.Г. Асимметричные методы шифрования. – Модуль 2 Криптографические методы защиты информации в телекоммуникационных системах и сетях: учеб. Пособие/ Под ред. Н.В. Захарченко – Одесса: ОНАС им. А.С Попова, 2010 – 148с.
4. Авдошин С.М. Криптографические методы защиты информационных систем // Бизнес-информатика. – 2006. – №17.