УДК 004.056

АНАЛИЗ ЭФФЕКТИВНОСТИ ЧАСТОТНОГО МЕТОДА КРИПТОАНАЛИЗА В СРЕДЕ ПРОГРАММИРОВАНИЯ DELPHI

Студентки гр. 113458 ПСФ Глухова Е.А., Тиханович Н.Э.
кандидат физ.-мат. наук, доцент Буснюк Н.Н.
Белорусский национальный технический университет

Условие совершенной криптостойкости симметричной криптосистемы заключается в том, что количество информации, содержащейся в шифртексте У об исходном сообщении Х, равно нулю. Если условие совершенной криптостойкости не выполнено, то криптоаналитик может обнаружить закономерности и расшифровать сообщение. Наиболее известными методами расшифровывания без знания ключа, не применяющими полный перебор всех возможных вариантов, являются методы статистического анализа, и среди них – «частотный метод». Однако не известно математических формул, устанавливающих форму зависимости между минимальной длиной текста Х и вероятностью его расшифрования путем подбора ключа. Т.е считается, что криптоаналитик может расшифровать шифртекст У быстрее чем полным перебором, если последний содержит в себе некоторую информацию об исходном тексте Х, но насколько быстрее – строго не описано.

Метод частотного анализа (по-другому называемый метод максимального правдоподобия) основан на том модельном предположении, что исходный текст Х представляет собой случайную последовательность с некоторым заданным распределением вероятностей.

Целью настоящего исследования являлось изучение зависимости между длиной текста Х и вероятностью расшифровывания текста У частотным методом. Исследование проводилось с помощью компьютерной программы, составленной в интегрированной среде Delphi. В качестве алфавита исходного текста был взят русский алфавит с известными вероятностными характеристиками алфавита. Знаки препинания, пробелы и другие символы в исходном тексте не применялись. После подсчета частот встречаемости символов в наблюдаемом шифртексте и вычисления функции правдоподобия вариант расшифрованного текста выводился на печать и визуально оценивался на правдоподобность. В случае неправдоподобности выбиралось очередное максимальное значение функции и новый полученный вариант расшифрованного текста оценивался. Такая процедура выполнялась 5 раз. В случае правдоподобности длина исходного текста варьировалась в меньшую сторону, в случае невозможности расшифровывания за 5 итераций, длина исходного текста увеличивалась. Исходный текст выбирался из литературного источника, а ключ генерировался с помощью датчика случайных чисел.