О КРИПТОАНАЛИЗЕ ШИФРОВ ПРОСТОЙ ЗАМЕНЫ С ИСПОЛЬЗОВАНИЕМ СЛОВАРЯ

М.Б. Абросимов, А.Д. Коннова, Д.А. Томилов

В работе рассматривается криптоанализ моноалфавитного шифра замены, то есть шифра, в котором каждой букве открытого текста сопоставляется единственная буква шифр-текста. Хорошо известным методом криптоанализа шифра простой замены является алгоритм [1] на основе частотного анализа, который состоит в итерационном процессе минимизации разницы частот. В зашифрованном сообщении вычисляются частоты символов и сравниваются с эталонными значениями. В таком случае можно сопоставить частоты символов шифроалфавита с исходными и восстановить исходный текст. Однако на практике одних лишь частот символов оказывается недостаточно. Текст может быть слишком короткий, чтобы в нем оказались эталонные или близкие к ним частоты. Как отмечает автор, для достаточно больших текстов количество ошибок может быть незначительным, и текст может быть прочитан, хотя и с некоторыми ошибками.

Предлагается добавить в алгоритм на основе частотного анализа дополнительный слой на основе словаря. Получив достаточное приближение к эталонным частотам, переходим к следующему этапу – проверке частично дешифрованных слов по словарю. При выборе определенного слова из словаря пробуем совершить замену ошибочной буквы и подсчитать коэффициент похожести слов. Коэффициент похожести слов – сумма минимальных ошибок в словах расшифрованной с помощью предположительной перестановки криптограммы со словами из словаря. Алгоритм заканчивает работу, когда не остается слов с ошибкой для исправления.

Была разработана программа, реализующая предлагаемый алгоритм. На вход подавались зашифрованные шифром простой замены тексты и анализировалось качество автоматической дешифровки. Если в работе [1] у автора были ошибки на тексте длиной 1000 символов, то описываемый метод полностью справился со всеми текстами длины более 800 символов.

Литература

1. Jakobsen T.P. A Fast Method for Cryptanalysis of Substitution Ciphers // Cryptologia. 1995. Vol. 19. P. 265–274.