УДК 681.3.06

Использование простого алгоритма ROT13

Камбур О. М., Рожин О.В.
Белорусский национальный технический университет

Один из самых простых методов кодирования – ROT 13 (англ. rotate, «сдвинуть на 13 позиций»). Он заключается в том, что каждой букве английского алфавита присваивается число, например A–1, B–2 и т.д. ROT13 является обратным алгоритмом, одни и те же действия могут быть использованы для кодирования и декодирования [(ROT13(ROT13(x)) = =ROT26(x) = x для любого текста x]. Если вы пишете слово, то присваиваете число каждой букве, затем к каждому из них прибавляете 13, после чего полученные числа снова заменяются буквами. Если это число больше 26, то из него следует вычесть 26, чтобы не превысить количество букв в алфавите (латинский).

Алгоритм не дает никакой реальной криптографической безопасности и никогда не должен использоваться для этого. ROT13 использовался в новостном форуме net.jokes в начале 1980-х.,чтобы скрыть потенциально оскорбительные шутки или ответ на головоломку или спойлер. ROT13 представляет собой частный случай алгоритма шифрования, известного как шифр Цезаря, приписываемый Юлию Цезарю в I веке до нашей эры. Netscape Communicator использовал ROT-13 в рамках небезопасной схемы для хранения паролей электронной почты.

ROT13 предоставляет возможность для «игр в слова». Компьютерная программа Westley может корректно компилировать как простые, так и кодированные алгоритмом ROT13 исходные файлы. Варианты алгоритма(Rot47). В 2001 году русский программист Дмитрий Скляров продемонстрировал, что поставщик eBook, компания New Paradigm Research Group (NPRG), использовала ROT13 для шифрования своих документов. Адреса электронной почты также иногда кодируют алгоритмом ROT13, чтобы скрыть их от не самых продвинутых спам-ботов. Трансформированные алгоритмом ROT13 слова , производят другое известное слово. ROT13 стал жаргонным словом для обозначения какой-либо явно слабой схемы шифрования. Благодаря алгоритму ROT13 легко научиться шифровать данные.