СИММЕТРИЧНЫЙ КРИПТОАЛГОРИТМ ENIGMA-R10

Рябченко Д.В., Губенко Н.Е.
Донецкий национальный технический университет

В настоящее время существует множество разновидностей криптоалгоритмов, которые условно можно разделить на симметричные и асимметричные. Симметричные алгоритмы используют один и тот же ключ для прямого и обратного преобразований и требуют защищенный канал, для передачи ключа от отправителя шифрованной информации к получателю. Асимметричные алгоритмы (т.н. алгоритмы с открытым ключом) оперируют двумя однозначно взаимосвязанными ключами, один из которых используется для прямого преобразования информации (открытый ключ), а второй -для обратного (закрытый ключ). При этом задача нахождения закрытого ключа из открытого до сих пор не решена математически. Данный тип алгоритмов выгодно отличается от симметричных отсутствием необходимости защищенной пересылки ключа получателю, но значительно более трудоемкий. Асимметричные алгоритмы целесообразно применять при передаче данных от одного лица - другому. Если же, необходимо шифровать данные, не предназначенные для передачи другим лицам (например, личную или финансовую информацию), то целесообразно использовать симметричный алгоритм (т.к. отпадает необходимость передачи ключа). Более того, в связи с математической и, соответственно, аппаратной трудоемкостью шифрования с открытым ключом, для шифрования сообщений, имеет смысл использовать симметричный шифр со случайным ключом, а относительно короткий ключ шифровать, используя ассиметричный алгоритм. Именно так работает популярная криптосистема для защиты электронной почты PGP (Pretty good privacy). Алгоритм Enigma-R10 представляет собой симметричный криптоалгоритм, оперирующий с блоками данных размером 2^{10} байт = 1 килобайт. Данный алгоритм назван в память о первой шифровальной машине "Enigma", разработанной и использовавшейся в Германии, во время Второй Мировой Войны. Данные шифруются 1-килобайтные блоками с использованием одного, или двух ключей, произвольной длины, вводимых пользователем. Тот же алгоритм с теми же ключами служит для обратного преобразования шифрованного текста в открытый. Ключи, вводимые пользователем преобразуются, таким образом, что их длина и содержимое меняются, в зависимости от первоначальных значений. На первом шаге данные преобразуются посредством циклического сдвига битов блока. Оба ключа представляются в виде массивов цифр, определяющих величину сдвига. Элементы первого массива циклически распределяются последовательно от начала блока к его концу. Элементы второго массива распределяются циклически, но скачкообразно, от начала к концу и обратно (метод "краевой атаки"), приближаясь к середине блока. Таким образом посредством сочетания двух методов распределения элементов образуется неповторяющийся результирующий ключ, длиной равный блоку. Этот принцип повышает криптоустойчивость закрытого текста, т. к. из него нельзя определить длину исходных ключей. Затем биты каждого байта блока сдвигаются на величину, определяемую соответствующим элементом результирующего ключа. Направление сдвига зависит от того, в каком направлении работает алгоритм (шифрования или дешифрования блока). На втором шаге к каждому байту блока применяется побитовая операция исключающего ИЛИ с каждым элементов массива первого ключа. Таким образом достигается т. н. лавинный эффект, повышающий криптоустойчивость шифрованного

текста. Лавинный эффект - высокая чувствительность результата к изменению начальных данных - любые малые изменения ключа приводят к значительным изменениям в результирующем тексте. В частности, изменения значения всего одного бита ключа отражается в изменении значений многих битов в шифрованном тексте. Для определения эффективности алгоритма Enigma-R10, было проведено сравнение с известным алгоритмом DES (Data Encryption Standard) с длиной блока 64 бит и длиной ключа 56 бит. В результате изменения одного бита ключа, после 16 раундов DES выдает блок, отличающийся на 35 бит от первоначального, т.е. результат на 45,31 % совпадает с оригиналом (смотри источник [2], стр. 109, таблица 3.5(б)). В аналогичной ситуации Enigma-R10 выдает результат, совпадающий с оригиналом на 0 % - 12,2 %. Таким образом, лавинный эффект Enigma-R10 почти в 4 раза больше чем лавинный эффект DES. Результаты дешифрования файла размером 254 075 байт, зашифрованного с ключом "aq123" представлены в таблице 1.

Таблица 1

Лавинный эффект Enigma-R10

Ключ	*Идентичность*	*Ключ*	*Идентичность*	*Ключ*	*Идентичность*
aq120	0.00 %	aq12l	0.00 %	aq12G	0.00 %
aq121	0.00 %	aq12m	0.00 %	aq12H	0.33 %
aq122	0.00 %	aq12n	0.00 %	aq12I	0.00 %
aq123	100.00 %	aq12o	0.00 %	aq12J	0.00 %
aq124	0.31 %	aq12p	0.37 %	aq12K	0.00 %
aq125	0.00 %	aq12q	0.00 %	aq12L	0.00 %
aq126	0.00 %	aq12r	0.00 %	aq12M	0.27 %
aq127	0.00 %	aq12s	0.00 %	aq12N	0.00 %
aq128	0.00 %	aq12t	0.34 %	aq12O	0.00 %
aq129	0.25 %	aq12u	0.34 %	aq12P	0.00 %
aq12a	0.28 %	aq12v	0.00 %	aq12Q	0.01 %
aq12b	0.00 %	aq12w	0.00 %	aq12R	0.33 %
aq12c	0.00 %	aq12x	0.00 %	aq12S	0.00 %
aq12d	0.00 %	aq12y	12.20 %	aq12T	0.00 %
aq12e	0.15 %	aq12z	0.29 %	aq12U	0.00 %
aq12f	0.34 %	aq12A	0.00 %	aq12V	0.00 %
aq12g	0.00 %	aq12B	0.00 %	aq12W	0.29 %
aq12h	0.00 %	aq12C	0.30 %	aq12X	0.00 %
aq12i	0.00 %	aq12D	0.00 %	aq12Y	0.00 %
aq12j	0.00 %	aq12E	0.00 %	aq12Z	0.00 %
aq12k	0.32 %	aq12F	0.00 %	-	-

В связи с тем, что алгоритм DES использует 16 раундов, а Enigma-R10 - 2 раунда, время преобразования данных алгоритмом Enigma-R10 в 3-5 раз меньше, по сравнению с DES. Например, для ЭВМ с 256 Мб ОЗУ и ЦП Athlon XP 2600 + Enigma-R10 преобразует 2000 килобайт в секунду, а DES - 480 килобайт в секунду. Для алгоритма DES, при длине ключа 56 бит имеется 2^{56} вариантов различных ключей, что приблизительно равно 7,2 x 10^{16}. Для алгоритма Enigma-R10 с пользовательским ключом "aq123" - преобразованный ключ имеет длину 15 байт = 96 бит. Соответственно существует 2^{96} вариантов различных ключей, что приблизительно равно 7,9 x 10^{28}. Соответственно алгоритм Enigma-R10 менее уязвим к методу перебора ключей, чем DES.

Литература

[1] М.Н. Аршинов, Л.Е. Садовский, *Коды и математика* - М. Наука. 1983. - 144 с.

[2] Вильям Столлингс, *Криптография и защита сетей: принципы и практика, 2-е изд.* Пер. с англ. - М.: Издательский дом "Вильямс", 2001. - 672 с.