РАЗРАБОТКА АЛГОРИТМА ШИФРОВАНИЯ НА ОСНОВЕ ДИНАМИЧЕСКОГО ХАОСА И ЭЛЕМЕНТЫ ЕГО ЛИНЕЙНОГО КРИПТОАНАЛИЗА

Сидоренко А. В., Жуковец Д. А.

Белорусский государственный университет, Минск, Беларусь,
e-mail: sidorenkoa@yandex.ru

В современном мире информационный ресурс стал одним из наиболее мощных рычагов экономического развития.

Наряду с традиционными алгоритмами шифрования, которые постоянно разрабатываются и совершенствуются, все большую популярность в криптографическом сообществе приобретают алгоритмы шифрования на основе систем динамического хаоса.

Системами динамического хаоса называются динамические системы с экспоненциальной зависимостью состояния от начальных условий, т.е. небольшое изменение начального состояния системы приводит к существенному изменению всей траектории системы на фазовой плоскости. Изменение в начальных условиях экспоненциально усиливается во времени.

Блочный шифр способен зашифровать одним ключом одно или несколько сообщений суммарной длиной, превышающей длину ключа. Передача малого по сравнению с сообщением ключа по зашифрованному каналу — задача значительно более простая и быстрая, чем передача самого сообщения или ключа такой же длины, что делает возможным его практическое использование. Однако, при этом, шифр перестает быть не вскрываемым.

Линейный метод криптоанализа предполагает, что криптоаналитик знает открытые и соответствующие зашифрованные тексты. Обычно при шифровании используется сложение по модулю 2 текста с ключом и операции рассеивания и перемешивания. Задача криптоаналитика – найти наилучшую линейную аппроксимацию (после всех циклов шифрования) выражения

$$P_{i1} \oplus ... \oplus P_{il} \oplus C_{j1} \oplus ... \oplus C_{jm} = K_{k1} \oplus ... \oplus K_{kn}. \qquad (1)$$

Пусть P_L вероятность того, что это равенство выполняется, при этом необходимо, чтобы величина $|P_L–1/2|$ была максимальна. Если $|P_L–1/2|$ достаточно велико, и криптоаналитику известно достаточное число пар открытых и соответствующих зашифрованных текстов, то сумма по модулю 2 бит ключа на соответствующей позиции в правой части равенства равна наиболее вероятному значению суммы по модулю 2 соответствующих бит открытых и зашифрованных текстов в левой части.

Требуемое для раскрытия ключа количество N пар открытых и зашифрованных текстов (блоков) оценивается выражением

$$N \approx \left| P_L - \frac{1}{2} \right|^{-2} \qquad (2)$$

Литература