К ВОПРОСУ МУТАЦИИ КЛЮЧЕЙ КРИПТОГРАФИЧЕСКИХ ПРЕОБРАЗОВАНИЙ

канд. экон. наук, доц. М.И. Главчев, магистр Я.О. Сахно,
Национальный технический университет "Харьковский политехнический институт", г. Харьков.

Большинство современных симметричных алгоритмов шифрования построены в соответствии с архитектурой сети Фейстеля. Сеть представляет собой определённую многократно повторяющуюся итерированную структуру, называющуюся ячейкой Фейстеля или раундом шифрования. При переходе от одной ячейки к другой меняется ключ, причём выбор ключа зависит от конкретного алгоритма. Операции шифрования и расшифровывания на каждом этапе очень просты, и при определённой доработке совпадают, требуя только обратного порядка используемых ключей. Шифрование при помощи данной конструкции легко реализуется как на программном уровне, так и на аппаратном, что обеспечивает широкие возможности применения.

Ключи раунда получаются из ключа шифрования с помощью преобразования, состоящего из двух компонентов: расширение ключа и выбор ключа раунда. Основной принцип состоит в следующем: общее число битов ключа раунда равно длине блока, умноженной на количество раундов плюс 1. Для длины блока 512 бит и 10 раундов необходимо 5632 битов ключа раунда. Ключи раунда получаются следующим способом: первый ключ раунда состоит из первых Nb слов, второй состоит из следующих Nb слов и т.д. и в результате создается таблица перемутации.

Ключевое расписание использует таблицы пермутации, каждая пермутация содержит значения от 0 до 255. Каждый цикл шифрования состоит из 4 операций: Операций XOR с таблицей пермутации, измельчение или пермутирование отдельных бит в блоке, безключевой диффузии и распространения, именуемых англ. raking (сгребание), и этапа подстановки с использованием таблиц подстановки, именуемых S-box. Этап измельчения может так же пермутировать все 8-битные массивы независимо, или в группе из четырех в зависимости от 3-го котрольного бита. Таблицы пермутации могут оставаться неизменными в течении всего процесса шифрования, либо, если установлен 5-й контрольный бит, таблицы пермутации генерируются отдельно для каждого блока.

Создание мутирующей ключевой последовательности есть один из основных элементов проводимого исследования.