УДК 681.3.07

СЕМЕЙСТВО СИММЕТРИЧНЫХ БЛОЧНЫХ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ ЗАЩИТЫ ИНФОРМАЦИИ С ДИНАМИЧЕСКИ УПРАВЛЯЕМЫМИ ПАРАМЕТРАМИ ШИФРОВАНИЯ

Белецкий А.Я., д-р техн. наук, профессор,
Белецкий А.А., мл. научный сотр., Национальный авиационный университет (E-mail: abel@nau.edu.ua)
А.А.Кузнецов, канд.техн.наук, ст. научный сотр.
Харьковский университет воздушных сил
(E-mail: kuznetsov_alex@rambler.ru)

В данном докладе предлагается достаточно гибкая к изменению параметров шифрования симметричная блочная криптосистема, названная системой ***RSB* - 32.**. Аббревиатура ***RSB*** происходит от ключевых слов ***R****ound,* ***S****tep,* ***B****lock* – подчеркивая тем самым, что основными для криптоалгоритма являются раундовые преобразования (***R***), разбитые на определенное число шагов (***S***), а действие алгоритма осуществляется над блоками (***B***) открытого или закрытого текстов, причем размер раундового ключа (как элемента общего ключа) составляет 32 бита. ***RSB*** – это итерационный блочный шифр, который доставляет уникальную возможностью по изменению как размеров секретных ключей, так и числа шагов (раундов) шифрования.

Отличительная особенность ***RSB*** алгоритма состоит в том, что в нем используется оригинальная функция шифрования типа *скользящего кодирования* (свертки), которая обеспечивает не только глубокое перемешивание открытого текста, но и участвует в формировании *блочного раундового ключа* для очередного шифруемого блока. Общий ключ в ***RSB*** шифре образуется конкатенацией (объединением) ***r*** 32–разрядных раундовых ключей, являющихся *базовыми раундовыми ключами.*

Основные параметры ***RSB*** шифра:

- Длина раундового ключа - 32 бита.
- Длина общего (шагового) ключа: $r * 32$, $r = 1, 2, \ldots$
- Число шагов шифрования: $s = 1, 2, \ldots$
- Общее число раундов шифрования: $r * s$.
- Размер блока: 256 бит.

- Размер элементов скользящего кодирования - 32 бита.
- Размер элементов нелинейной замены: 8 бит.

Основная идея составных, или композиционных, блочных шифров состоит в построении криптостойкой системы путем многократного применения относительно простых криптографических преобразований, которые называются *криптографическими примитивами* (функциями шифрования). В качестве криптографических примитивов в ***RSB*** алгоритме используются:

- стохастическая круговая прокрутка шифруемого блока;
- скользящее кодирование 32-разрядных элементов блока;
- стохастическая нелинейная замена байтов блока;
- стохастическая перестановка байтов в пределах блока.

Перечисленные криптографические примитивы обеспечивают в ***RSB*** шифре стохастические операции циклических сдвигов блоков, свертки, а также нелинейных замен и перестановок байтов в пределах блока, причем указанные преобразования выполняются в каждом блоке под управлением индивидуальных блочных раундовых ключей, зависящих не только от значения секретного базового раундового ключа, но и всего шифруемого текста, предшествующего преобразуемому блоку. Применение оригинальных примитивов типа лево- и правостороннего скользящего кодирования в ***RSB*** алгоритме позволило устранить один из серьезных недостатков классических блочных шифров, который проявляется в том, что одинаковым блокам открытого текста соответствуют одинаковые блоки шифротекста. В ***RSB*** шифре указанный недостаток устраняется как операциями скользящего кодирования (свертки 32-разрядного базового ключа с соответствующими по размеру элементами текста), так и за счет различия в двух любых блочных раундовых ключах, управляющих криптопреобразованиями соответствующих блоков шифруемого текста.

Как показали результаты статистических испытаний ***RSB*** криптосистемы, эффективность алгоритма зашифрования, оцениваемая количеством тестов в пакете ***NIST STS***, в котором тестирование успешно прошло больше 99% и соответственно 96 % последовательностей, оказалось на уровне не ниже российского алгоритма ***ГОСТ*** 28147-89 и превосходит в отдельных случаях эффективность широко используемых зарубежных стандартов криптографической защиты, таких как ***DES***, ***IDEA*** и ***AES*** (*Rijndael*).