Я.В. Березинец
Научный руководитель: к.т.н., доцент А.А. Быков
Муромский институт (филиал) Владимирского государственного университета
602264, г. Муром, Владимирская обл., ул. Орловская, д. 23
E-mail: berezinec.yaroslav@mail.ru

Сравнение стандартов шифрования AES и ГОСТ 28147-89

Шифрование – это способ сокрытия исходного смысла сообщения или другого документа, обеспечивающий искажение его первоначального содержимого.

Шифрование применяется для хранения важной информации в ненадёжных источниках и передачи её по незащищённым каналам связи. Такая передача данных представляет из себя два взаимно обратных процесса: шифрования и дешифрация.

Надежность хранения информации особенно важна для государственных структур. Поэтому именно государственные стандарты шифрования обладают одними из самых высоких показателей криптографической стойкости. Таковыми же являются и два следующих стандарта шифрования – стандарт США AES и стандарт СССР и РФ ГОСТ 28147-89.

Стандарт ГОСТ 28147-89

ГОСТ 28147-89 — советский и российский стандарт симметричного шифрования, введённый в 1990 году, также является стандартом СНГ. Полное название — «ГОСТ 28147-89 Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования». Блочный шифроалгоритм. При использовании метода шифрования с гаммированием может выполнять функции поточного шифроалгоритма.

С момента опубликования ГОСТа на нём стоял ограничительный гриф «Для служебного пользования», и формально шифр был объявлен «полностью открытым» только в мае 1994 года. История создания шифра и критерии разработчиков по состоянию на 2015 год не обнародованы.

Основа алгоритма шифра — сеть Фейстеля. Выделяют четыре режима работы ГОСТ 28147-89:

- простой замены
- гаммирование
- гаммирование с обратной связью
- режим выработки имитовставки.

Алгоритм ГОСТ 28147-89 считается очень сильным алгоритмом - в настоящее время для его раскрытия не предложено более эффективных методов, чем упомянутый выше метод "грубой силы". Его высокая стойкость достигается в первую очередь за счет большой длины ключа - 256 бит. При использовании секретной синхропосылки эффективная длина ключа увеличивается до 320 бит, а засекречивание таблицы замен прибавляет дополнительные биты. Кроме того, криптостойкость зависит от количества раундов преобразований, которых по ГОСТ 28147-89 должно быть 32 (полный эффект рассеивания входных данных достигается уже после 8 раундов).

Основные проблемы ГОСТа связаны с неполнотой стандарта в части генерации ключей и таблиц замен. Считается, что у ГОСТа существуют «слабые» ключи и таблицы замен, но в стандарте не описываются критерии выбора и отсева «слабых».

Возможные применения:

- Использование в S/MIME (PKCS#7, Cryptographic Message Syntax).
- Использование для защиты соединений в TLS (SSL, HTTPS, WEB).
- Использование для защиты сообщений в XML Encryption.

По результатам открытых работ можно сделать вывод о достаточно высокой криптостойкости отечественного стандарта шифрования.

Стандарт AES

Advanced Encryption Standard (AES), также известный как Rijndael (произносится [rɛinda:l] (Рэндал)) — симметричный алгоритм блочного шифрования (размер блока 128 бит, ключ 128/192/256 бит), принятый в качестве стандарташифрования правительством США по результатам конкурса AES. Этот алгоритм хорошо проанализирован и сейчас широко используется, как это было с его предшественником DES. Национальный институт стандартов и технологий США (англ. *National Institute of Standards and Technology*, NIST) опубликовал спецификацию AES 26 ноября 2001 года после

пятилетнего периода, в ходе которого были созданы и оценены 15 кандидатур. 26 мая 2002 года AES был объявлен стандартом шифрования. По состоянию на 2009 год AES является одним из самых распространённых алгоритмов симметричного шифрования. Поддержка AES (и только его) введена фирмой Intel в семейство процессоров x86начиная с Intel Core i7-980X Extreme Edition, а затем на процессорах Sandy Bridge.

В отличие от алгоритма ГОСТ 28147-89, который долгое время оставался секретным, американский стандарт шифрования AES, призванный заменить DES, выбирался на открытом конкурсе, где все заинтересованные организации и частные лица могли изучать и комментировать алгоритмы-претенденты.

В отличие от отечественного стандарта шифрования, алгоритм Rijndael представляет блок данных в виде двухмерного байтового массива размером 4X4, 4X6 или 4X8 (допускается использование нескольких фиксированных размеров шифруемого блока информации). Все операции выполняются с отдельными байтами массива, а также с независимыми столбцами и строками

Алгоритм Rijndael выполняет четыре преобразования: BS (ByteSub) - табличная замена каждого байта массива; SR (ShiftRow) - сдвиг строк массива. При этой операции первая строка остается без изменений, а остальные циклически побайтно сдвигаются влево на фиксированное число байт, зависящее от размера массива.

Rijndael стал новым стандартом шифрования данных благодаря целому ряду преимуществ перед другими алгоритмами. Прежде всего он обеспечивает высокую скорость шифрования на всех платформах: как при программной, так и при аппаратной реализации. Кроме того, требования к ресурсам для его работы минимальны, что важно при его использовании в устройствах, обладающих ограниченными вычислительными возможностями.

Недостатком же алгоритма можно считать лишь свойственную ему нетрадиционную схему. Дело в том, что свойства алгоритмов, основанных на сети Фейстеля, хорошо исследованы, а Rijndael, в отличие от них, может содержать скрытые уязвимости, которые могут обнаружиться только по прошествии какого-то времени с момента начала его широкого распространения.

Несмотря на существенные различия в архитектурных принципах шифров AES и ГОСТ 28147-89, их основные рабочие параметры сопоставимы. В отличие от ГОСТа, размер шифруемого блока и размер ключа в алгоритме Rijndael могут изменяться, что допускается использованной в нем архитектурой «квадрат». Данное свойство позволяет варьировать стойкость и быстродействие алгоритма в зависимости от внешних требований к реализации в некоторых пределах, –однако, не очень широких, – число раундов, а вместе с ним и быстродействие, в крайних случаях различаются в 1.4 раза. Однако AES имеет преимущество в быстродействии перед ГОСТом при аппаратной реализации на базе одной и той же технологии. По ключевым для алгоритмов такого рода параметрам криптостойкости ни один из алгоритмов не обладает существенным преимуществом, также примерно одинаковы скорости оптимальной программной реализации. Из сказанного можно сделать вывод, что отечественный стандарт шифрования соответствует требованиям, предъявляемым к современным шифрам, и может оставаться стандартом еще достаточно долгое время