Автор: Узаков О.Ш.
09.04.2018 13:29 -

ОЦЕНКА ЭКСПОНЕНЦИАЛЬНОЙ СЛОЖНОСТИ СТАНДАРТА АЛГОРИТМА ШИФРОВАНИЯ AES-FIPS-197

Узаков О. Ш.

Каршинский филиал ташкентского университета информационных технологий имени Мухаммада аль-Хоразмий, Кафедра «Информационных технологии», ассистент

Оценка экспоненциальной сложности дешифрования шифр текстов позволит дать ответ на вопрос, “каким должен быть крипто стойкий алгоритм шифрования”, чтобы дешифрование шифр текста не было практически возможным без исходного ключа шифрования.

В 2001 году стандартом шифрования данных был принять AES (Advanced Encryption Sta ndard
) (
FIPS
-197) за основу которого был взять алгоритм шифрования
RIJNDAEL
, разработанный Бельгийскими специалистами Йон Дэмен (
Joan
Daemen
) и Винсент Рюмен (
Vincent
Rijmen
), начальные буквы фамилий которых и образуют название алгоритма –

RIJNDAEL

.

RIJNDAEL

–

это итерационный блочный алгоритм шифрования, имеющий архитектуру "Квадрат". Алгоритм шифрования имеет переменную длину блоков и раз
личные длины ключей. Длина ключа и длина блока могут быть равными независимо друг от друга 128, 192 или 256 битам. В стандарте
AES
определена длина блока данных, равная 128 битам.

...

Полный текст во вложении