



NOXCrypt v2.3.0 — Публичная спецификация

Автор: NOX

1. Название

NOXCrypt v2.3.0 — проприетарный криптоалгоритм, разработанный специально для системы NOX. Его назначение — обеспечивать шифрование, которое невозможно распознать как шифрование, включая маскировку под различные медиаформаты и случайные двоичные потоки.

2. Цели и особенности

- Скрытие не только содержимого данных, но и самого факта их существования.
- Выходные данные могут имитировать изображения, аудио, видео или произвольные бинарные данные.
- Маскировка под популярные форматы (например, JPEG, MP3, PNG).
- Применение исключительно внутри экосистемы NOX.
- Ключ динамичный, с уникальной генерацией для каждой сессии.

3. Архитектура

Архитектура использует каскадные этапы преобразования данных, включая подстановки, смешивание и добавление контролируемого шума. Дополнительно алгоритм встроен в общий механизм глубокого

инкриптования NOX, обеспечивающий не только защиту содержимого, но и невидимость самой коммуникации. Конкретные математические схемы и внутренние таблицы являются конфиденциальной информацией и не раскрываются в публичной версии спецификации.

4. Ключ и сессии

Ключ шифрования имеет высокую длину и формируется динамически с использованием случайных и сеансовых параметров. Для каждой сессии создаются уникальные таблицы и правила преобразований, исключающие повторное использование ключей и шаблонов шифрования.

5. Маскировка

Алгоритм способен преобразовывать зашифрованный поток в вид, соответствующий различным типам медиафайлов или сетевого трафика, что существенно затрудняет определение факта передачи зашифрованной информации.

6. Безопасность

Каждая сессия использует уникальные ключи и наборы правил шифрования. Даже при перехвате трафика без доступа к ключу расшифровка невозможна. В алгоритм встроены механизмы предотвращения криптоанализа и маскировки структуры данных.

7. Применение

NOXCrypt может шифровать текст, голосовые данные и произвольные бинарные потоки, преобразуя их в вид, не вызывающий подозрений. Алгоритм оптимизирован для высокой скорости и низкой задержки при передаче данных.

8. Заключение

NOXCrypt — это криптосистема нового поколения, ориентированная на обеспечение максимальной конфиденциальности и анонимности, а также на устойчивость к обнаружению и анализу. Она является частью более широкого механизма глубокого инкриптования NOX, формирующего

базовый уровень защиты экосистемы. Данная спецификация представляет собой обзор технологии и не раскрывает внутренних алгоритмических деталей.