Российская криптография

Как перестать беспокоиться и начать жить

Disclaimer

Почему важно

- Масса недостоверных слухов в Интернете
- Закон Яровой
- Предубеждения
- Необходимость вовлечения инженерного сообщества

Отечественные стандарты

- Не являются секретными
- Разрабатываются с участием сообщества
- Полностью открыты и доступны для скачивания на сайте ТК26: https://www.tc26.ru/
- Реализуют большинство основных криптографических функций, необходимых в ежедневной работе

ГОСТ Р 34.10-2012: Электронная подпись

- Процессы генерации и проверки подписи с использованием асимметричной криптографии на эллиптических кривых с ключами длиной до 512 бит
- Использует хэш-функцию из ГОСТ Р 34.11-2012 (“Стрибог”)
- Приводит примеры параметров для задания конкретных кривых, но не закрепляет их нормативно (существуют отдельные методические рекомендации)
- Позволяет (совместно с некоторыми другими алгоритмами) реализовать все необходимые приложения электронной подписи и обмена ключами: S/MIME, TLS полностью аналогично ECDSA
- На сегодняшний день нет открытых и свободных реализаций (только для предыдущего стандарта ГОСТ Р 34.10-2001), необходима доработка имеющихся патчей к OpenSSL

ГОСТ Р 34.11-2012: Хэш-функция

- Современный быстрый хэш с 512-битными блоками
- Размер хэша 256 или 512 бит
- Возможность эффективной реализации на большинстве архитектур
- Конкурс по поиску уязвимостей, 2013-2015 год
- Может полностью заменить SHA-256/SHA-512
- Открытая реализация на https://www.streebog.net/

ГОСТ Р 34.12-2015: Блочные шифры

- Симметричный алгоритм блочного шифрования
- Размеры блоков 64 бита (“Магма”), 128 бит (“Кузнечик”)
- Поддерживает все основные режимы: ECB, CTR, CFB, MAC (отдельный важный документ по режимам!)
- Создан с прицелом на устойчивость относительно известных видов атак
- Может быть использован для замены AES256
- Модельная реализация TK26
- Реализации для OpenSSL, libgcrypt, десятки реализаций на GitHub, включая оптимизированные

Мифы

- Российские алгоритмы секретные
- Российские алгоритмы содержат закладки ФСБ
- Российские алгоритмы давно взломаны
- Российские алгоритмы медленные
- Российские алгоритмы не работают в современных приложениях
- Российские алгоритмы можно использовать только если купить сертифицированное решение за 100500 миллионов, а если взять какое-то другое, то отправят на Колыму

Что нужно

- Разработчики :)
- Создание полных реализаций во free software библиотеках и импорт в апстрим
    - Обновление OpenSSL engine
    - Порт на BoringSSL (для Chromium)
    - Поддержка в почтовых клиентах
    - WolfSSL и embedded
    - libgnutls
    - ..
- Исследование возможностей применения российской криптографии в IoT (lightweight crypto)