Лабораторная работа №2

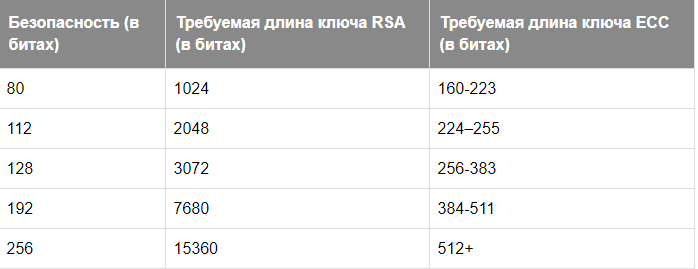
Дворяков Максим

12 группа кафедра ИСУ

Вариант 3

Сравним RSA и ECDSA

**Уровень безопасности** является метрикой в ​​криптографии, относящейся к силе  
криптографического примитива или функции, который измеряется в «битах»,  
обозначает количество операций, которые злоумышленник должен выполнить, чтобы скомпрометировать его  
безопасность.

По сравнению с RSA, ECDSA оказался более защищенным от существующих методов взлома благодаря своей сложности. ECDSA обеспечивает тот же уровень безопасности, что и RSA, но при этом использует гораздо более короткие ключи. Следовательно, для более длинных ключей ECDSA потребуется значительно больше времени для взлома с помощью брутфорсинга.

В принципе этим всё сказано. Наверное, только с приходом квантовых вычислений, эти алгоритмы станут бесполезными, а пока они являются очень безопасными.

Самая затратная часть ECDSA это алгоритм Шуфа, сложность которого равна

Остальные части не являются настолько затратными.

В основу криптографической системы с открытым ключом RSA положена сложность задачи факторизации произведения двух больших простых чисел