ВОПРОСЫ ПО КУРСУ “Криптография”

1. Односторонние функции.
2. Хеш-функции.
3. Гипотеза $P \neq NP$.
4. Симметричное шифрование.
5. Асимметричное шифрование.
6. Доказательства с нулевым разглашением.
7. Протоколы аутентификации и электронной подписи.
8. Неотслеживаемость. Электронная монета.
9. Протокол привязки к биту.
10. Протоколы электронного голосования.
11. Порождение простых чисел и проверка чисел на простоту. Сложность теоретико-числовых алгоритмов.
12. Протоколы разделения секрета.
13. Криптография на эллиптических кривых.