Вопросы к зачету
по дисциплине «криптографические протоколы»
для специальности «Компьютерная безопасность»
составил: д.ф-м.н., профессор Рацеев Сергей Михайлович
10-й семестр

Примерный перечень вопросов к зачету

1. Протоколы идентификации, использующие пароли (слабая аутентификация).
2. Протоколы идентификации, использующие технику «запрос–ответ»: «запрос–ответ» с использованием симметричных алгоритмов шифрования.
3. Протоколы идентификации, использующие технику «запрос–ответ»: «запрос–ответ» с использованием асимметричных алгоритмов шифрования.
4. Протокол идентификации Фиата-Шамира.
5. Протокол Фейга-Фиата-Шамира.
6. Итеративный протокол идентификации Фиата-Шамира без доверенного центра.
7. Трехпроходный протокол идентификации Фиата-Шамира без доверенного центра.
8. Итеративный протокол идентификации Шнорра.
9. Трехпроходный протокол идентификации Шнорра.
10. Протокол идентификации Окамото.
11. Протокол идентификации Гиллоу-Куискатр (GQ).
12. Протокол идентификации с нулевым разглашением на основе доказательства изоморфизма графов.
13. Протокол идентификации с нулевым разглашением на основе задачи о раскраске графа.
14. Протокол идентификации с нулевым разглашением на основе задачи о нахождении гамильтонова цикла в графе.
15. Протокол идентификации с нулевым разглашением на основе асимметричных шифров.
16. Передача ключей с использованием симметричного шифрования: двусторонние протоколы.
17. Передача ключей с использованием симметричного шифрования: трехсторонние протоколы. Протокол Kerberos.
18. Передача ключей с использованием асимметричного шифрования.
19. Открытое распределение ключей.
20. Предварительное распределение ключей. Схема Блома.