Оценочный материал для промежуточной аттестации по дисциплине «Криптографические методы защиты информации» 5 семестр

Код, направление подготовки	**09.03.02 Информационные системы и технологии**
Направленность (профиль)	Безопасность информационных систем и технологий
Форма обучения	Очная
Кафедра-разработчик	Информатики и вычислительной техники
Выпускающая кафедра	Информатики и вычислительной техники

Типовые задания для контрольной работы:

Практическое задание № 1. Реализация алгоритма шифрования RSA

В результате выполнения данной лабораторной работы будет изучен и реализован алгоритм шифрования RSA, оценена его эффективность и безопасность, что сделан вывод о его применимости для защиты информации.

Цель работы – *изучить и применить алгоритм шифрования RSA для защиты информации*.

Оборудование: Компьютер с установленными программами для разработки и выполнения кода (например, Python).

Шаги выполнения:

- Изучить принципы работы алгоритма шифрования RSA.
- Написать программу на выбранном языке программирования, реализующую шифрование и дешифрование сообщений с использованием алгоритма RSA.
- Протестировать программу на различных входных данных.
- Оценить эффективность и безопасность алгоритма RSA на основе полученных результатов.

Практическое задание № 2. Разработка системы электронной подписи.

Это практическое задание поможет студентам изучить на практике разработку системы электронной подписи, провести оценку безопасности и эффективности системы, сделать вывод о ее применимости для защиты информации.

Цель работы – *познакомиться с принципами и методами разработки системы электронной подписи для обеспечения целостности и установления авторства информации*.

Оборудование: Компьютер с установленными программами для разработки и выполнения кода (например, Python).

Шаги выполнения:

- Изучить принципы работы системы электронной подписи и алгоритмы, используемые для ее разработки (алгоритм хэширования, алгоритмы RSA и Эль-Гамаля).
- Написать программу на выбранном языке программирования, реализующую систему электронной подписи с использованием выбранных алгоритмов.
- Протестировать программу на различных входных данных.
- Оценить безопасность и эффективность разработанной системы электронной подписи.

Типовые вопросы к экзамену:

1. Что такое криптология? Криптография? Криптоанализ?
2. Какие задачи ставятся перед криптографией?
3. Какие основные этапы исторического развития криптографии?
4. Какие вы знаете параметры оценки криптографических преобразований?
5. Существует ли абсолютно стойкий шифр?
6. Что такое стойкость в криптографии? Какие виды бывают? Как их вычислять?
7. Какие уязвимости шифров вы знаете? Как их избегают?
8. Что такое словарная атака?
9. Что такое метод дифференциального криптоанализа и как он применяется в криптографии?
10. Что такое MITM? как обнаруживается и предотвращается?
11. Что такое частотный криптоанализ и как он работает?
12. Какой метод атак существует на шифр Виженера?
13. Что такое модульная арифметика?
14. Что такое группа, кольцо и поле в математической теории и как они применяются в криптографии?
15. Как линейные преобразования и матрицы связаны с криптографией?
16. Что такое алгебраическая модель шифра? Какие у неё компоненты? Какие альтернативы?
17. Как обеспечить безопасность обмена ключами в криптографии?
18. Что такое асимметричное шифрование и чем оно отличается от симметричного шифрования?
19. Что такое криптографический протокол?
20. Что такое шифрование с открытым ключом?
21. Расскажите про протокол RSA
22. Расскажите про протокол Диффи-Хеллмана
23. Расскажите про трёхэтапный протокол Шамира
24. Расскажите про протокол разделения серета
25. Расскажите про схему Блома
26. Расскажите про ГОСТы симметричного шифрования
27. Что такое DES и AES?
28. Что такое сети Фейстеля и SP-сети?
29. Что такое криптографические хэш-функции и как они используются для обеспечения целостности данных?
30. Что такое цифровая подпись и как она обеспечивает аутентификацию и непротиворечивость данных?
31. Что такое аутентификация? Какие факторы вам известны?
32. Что такое протоколы безопасного обмена информацией и какие примеры таких протоколов существуют?
33. Что такое протоколы аутентификации и приведите примеры таких протоколов?
34. Что такое протоколы защиты интернета вещей (IoT)?