ВОПРОСЫ К ЭКЗАМЕНУ

по спецкурсу «Введение в криптографию»

2025-2026 учебный год.

1. Основные задачи и понятия криптографии. Схема передачи шифрованной информации. Возможные угрозы со стороны оппонента. Правила Керхгоффса. Алгебраическая модель шифра.
2. Шифр простой замены. Математическая модель. Омофонный шифр (криптоанализ), шифр с пустышками, номенклатор. Группа, симметрическая группа. Доказательство того, что множество подстановок образует группу.
3. Криптоанализ одноалфитного шифра замены методом частотного анализа. Криптоанализ одноалфитного шифра замены на основе подобранного текста.
4. Энтропия вероятностной схемы. Информация. Энтропия языка. Избыточность языка. Расстояние единственности. Вывод формулы информации.
5. Модели открытого текста. Детерминированная, вероятностная стационарная и вероятностная нестационарная модели открытых текстов.
6. Шифр вертикальной перестановки. Математическая модель. Принципы вскрытия вертикальной перестановки.
7. Шифр Виженера. Математическая модель. Тест Казиски.
8. Индекс Фридмана. Теорема. Взаимный индекс совпадения. Криптоанализ шифра Вижинера методом Фридмана – алгоритм.
9. Шифр Кардано. Математическая модель. Мощность множества ключей. Криптоанализ. Книжный шифр.
10. Шифратор Джефферсона-Базери. Математическая модель. Метод вскрытия шифра.
11. Шифр Плейфера. Математическая модель. Эквивалентные ключи шифра Плейфера. Метод вскрытия шифра. Усложнения шифра Плейфера: шифры два квадрата и четыре квадрата.
12. Шифр ADFGVX. Различное распределение вероятностей в строках и столбцах.
13. Шифр Хилла. Математическая модель. Мощность множества ключей.
14. Шифр гаммирования. Математическая модель. Восстановление вероятностей знаков неравновероятной гаммы. Восстановление текстов, зашифрованных неравновероятной гаммой. Глубина чтения в колонках.
15. Криптоанализ шифра гаммирования при повторном использовании гаммы. Криптоанализ шифра гаммирования при использовании короткой гаммы.
16. Уравнение шифрования дискового шифратора. Метод Тьюринга криптоанализа Энигмы.
17. Шифры не распространяющие искажения типа «замена знаков». Утверждение.
18. Теорема Маркова.
19. Шифры не распространяющие искажения типа «пропуск-вставка символов». Теорема Глухова М.М. (без доказательства)