МАТЕМАТИЧЕСКИЕ ВОПРОСЫ КРИПТОГРАФИИ

проф. А. М. Зубков

1/2 года, 4 курс

1. Шифр простой замены и шифр Виженера. Метод вскрытия шифра простой замены.

2. Определение совершенного шифра. Теорема о числе ключей в совершенном шифре. Совершенное шифрование длинных текстов, его достоинства и недостатки.

3. Теорема о числе высоковероятных цепочек в последовательности независимых испытаний.

4. Энтропия распределения на конечном алфавите. Свойства энтропии. Максимальное значение энтропии. Оценки энтропии совместного распределения и энтропии условного распределения.

5. Префиксные коды. Неравенства Крафта–МакМиллана.

6. Теорема о минимальной длине кода.

7. Понятие о псевдослучайных числах. Рекуррентные датчики псевдослучайных чисел как отображения конечного множества. Распределение длины отрезка апериодичности случайного отображения.

8. Свойства периодов рекуррентной последовательности. Минимальный период линейной рекуррентной последовательности по составному модулю. Китайская теорема об остатках.

9. Функция Эйлера. Теорема Эйлера.

10. Определение первообразного корня. Существование первообразного корня по простому модулю. Для каких модулей существуют первообразные корни? Максимальный возможный период рекуррентной мультипликативной последовательности.

11. Линейные рекуррентные последовательности над конечным полем. Матричное и полиномиальное представления последовательностей и связь между ними.

12. Импульсные последовательности. Характеристический многочлен и производящая функция рекуррентной последовательности.

13. Порядки многочлена и характеристической матрицы. Условия максимальности периода линейной рекуррентной последовательности над конечным полем.

14. Свойства решетчатости мультипликативной рекуррентной последовательности. Спектральный тест и его геометрический смысл.

15. Теорема Колмогорова об оптимальных отображениях. Формализация понятия случайности.

16. Применения алгоритмов сортировки: композиция шифрующих отображений, шифрование без обмена ключами, простой алгоритм дискретного логарифмирования.

17. Простейший алгоритм сортировки, цифровая сортировка, сортировка слиянием.

18. Нижняя оценка среднего числа сравнений в алгоритмах сортировки, основанных на попарных сравнениях элементов.

19. Быстрая сортировка. Алгоритм поиска члена вариационного ряда с заданным номером.

20. Современные блочные шифраторы. Стандарт шифрования данных США.

21. Криптография с открытым ключом. Общая схема системы шифрования с открытым ключом. Схема обмена ключами. Схема электронной подписи. Схема аутентикации.

22. Системы шифрования Райвеста–Шамира–Адлемана и Эль-Гамаля.

23. Метод построения больших простых чисел.

24. Алгоритмы умножения многоразрядных чисел и больших матриц.

25. Поиск делителя натурального числа методом Полларда.

26. Метод нахождения делителя натурального числа, основанный на поиске сравнений второй степени.

27. Описание алгоритма дискретного логарифмирования.

28. Пороговые схемы разделения секрета. Построение пороговых схем с помощью линейных соотношений.

29. Построение схемы разделения секрета с произвольной системой доступа.