Математические основы криптографии

Автор курса: Применко Эдуард Андреевич
Составители: Смирнов Дмитрий Константинович,
Соколов Александр ??

2022 г.

Оглавление

Глава 1

Элементы теорий групп и чисел

1.1 Делимость в кольце целых чисел. НОД, алгоритм Евклида. Критерий взаимной простоты двух чисел.

1.2 Сравнения и их свойства. Китайская теорема об остатках. Кольцо вычетов. Функция Эйлера и её свойства.

1.3 Теоремы Эйлера и Ферма. Критерий обратимости, алгоритм вычисления обратного элемента.

1.4 Криптографическая теорема (обоснование криптосистемы РСА).

1.5 Теорема о цикличности мультипликативной группы по примарному модулю.

1.6 Решение сравнений первой степени.

1.7 Сравнения второй степени. Символ Лежандра и его свойства.

1.8 Алгоритмы решения сравнений второй степени по простому модулю.

1.9 Символ Якоби и его свойства. Числа Блюма и их свойства. Эквивалентность задачи факторизации и решения сравнения второй степени.

1.10 Алгоритмы решения сравнений второй степени по примарному и составному модулю.

1.11 Группа, порядок элемента. Теорема Лагранжа.

.

1.12 Нормальный делитель, фактор – группа, первая теорема о гомоморфизме.

1.13 Кольцо многочленов, идеал, теорема Безу, кольцо главных идеалов.

1.14 Конечное поле. Теорема о простом подполе конечного поля. Строение конечного поля. Теорема о примитивном элементе.

1.15 Построение конечных полей. Алгоритм вычисления обратного элемента. Арифметические операции в конечном поле.

1.16 Алгоритмы вычисления дискретного алгоритма.

1.17 Криптосистема Эль - Гамаля. Протокл Диффи - Хеллмана.

1.18 Минимальный многочлен и его свойства. Теорема об изоморфизме конечных полей одной мощности.

1.19 Примитивный многочлен и его свойства. Теорема о разложении многочлена $f(x) = xp^n – x$ на неприводимые многочлены. Критерий принадлежности элемента поля собственному подполю.

1.20 Теорема о группе автоморфизмов конечного поля.

1.21 Рекуррентные последовательности над конечным полем, линейные рекуррентные последовательности (ЛРП). Характеристический и минимальный многочлен ЛРП и их свойства.

1.22 Теорема об определении структуры ЛРП по её характеристическому многочлену. Теорема о ЛРП максимального периода.

1.23 Прямое произведение групп. Теорема о представлении группы в виде прямого произведения своих подгрупп.

1.24 Теорема о примарной абелевой группе.

1.25 Теорема о разложении конечной абелевой группы в произведение своих циклических подгрупп.

1.26 Нормализатор, централизатор, класс сопряженных элементов конечной группы. Теорема о числе множеств сопряженных с данным. Теорема о центре примарной группы. Теорема Коши.

1.27 Двойные смежные классы и их свойства. Теорема Силова (первая)

1.28 Вторая и третья теоремы Силова.

1.29 Группы подстановок. Инвариантное множество, орбита. Теорема об индексе стабилизатора группы. Теорема о транзитвности нормализатора подгруппы транзитвной группы. (Ут . 13.4).

1.30 Лемма Бернсайда.

1.31 Регулярные и полурегулярные группы. Порядок полурегулярной группы.

1.32 Блоки и импримитивные группы. Критерий импримитивности. Теорема о импримитивности транзитивной группы с интранзитивным нормальным делителем.

1.33 Примитивные группы. Кратная транзитивность. Критерий кратной транзитивности.

1.34 Теорема о группе автоморфизмов конечной группы.

1.35 Утверждение об изоморфизме стабилизатора и специальной группы автоморфизмов регулярной подгруппы (Ут . 13.5). Утверждение о порядке регулярного нормального делителя кратно транзитивной группы.

1.36 Простая группа. Теорема о простоте знакопеременной группы. Теорема о нормальном делителе симметрической группы.