Раздел 3.

Сжатие текстов.

Предварительное построение словаря.

Алфавитное кодирование.

Префиксные схемы.

Неравенство Макмиллана.

Оптимальное кодирование.

Алгоритм Хаффмана.

Основы кодирования.

Схема передачи информации по каналам связи.

Помехоустойчивое кодирование.

Кодирование с исправлением ошибок.

Кодовое расстояние. Коды Хемминга.

Раздел 4

Алгебра чисел.

Арифметика остатков.

НОД.

Алгоритм Евклида.

Диофантовы уравнения.

Китайская теорема об остатках.

Символы Лежандра и Якоби.

Парадокс дней рождений.

Простые числа.

Тесты на простоту чисел.

Генерация простых чисел.

Введение в криптографию.

Докомпьютерные методы шифрования.

Шифры перестановки.

Сложность вскрытия шифров перестановки.

Шифры замены.

Сложность вскрытия шифров замены.

Метод гаммирования.

Шифрование с открытым ключом.

Распределение ключей.

Алгоритм Диффи-Хеллмана.

Симметричные алгоритмы шифрования.

Хэш-функции.

Шифр AES.

Шифр RC5

Асимметричное шифрование.

Цифровая подпись.

Алгоритм RSA.