С/к ``Избранные главы криптографии’’, 1 г.

Профессор В.Н.Чубариков

1. Шифр: алгоритм, секретные и открытые ключи. Конфиденциальность, целостность, установление подлинности (аутентификация), цифровая подпись. Канал связи. Помехоустойчивость, увеличение скорости передачи информации, защита информации. Азбука Морзе. Код Фано.
2. Алфавитное кодирование. Префиксные коды. Коды Шеннона и Гилберта—Мура. Неравенство Крафта—МакМиллана. Теорема о минимальной длине префиксного кода.
3. Циклические коды. Конечные поля. Неприводимые многочлены.
4. Криптографические протоколы. Протокол для игры ``Орёл-решка’’ по телефону. Электронная подпись.
5. Сложность арифметических операций. Алгоритм Евклида. Операции в кольце вычетов. Дискретное преобразование Фурье. Наименьший первообразный корень.
6. Проверка числа на простоту: решето Эратосфена, критерий Вильсомалая теорема Ферма, числа Кармайкла, тесты Соловея—Штрассена, Рабина—Миллера.
7. Полиномиальный тест проверки на простоту.
8. Построение больших простых чисел. Критерий Люка. Числа Мерсенна.
9. Алгоритмы разложения натуральных чисел на множители. Метод квадратичного решета.
10. Криптографическая система RSA. Задача об укладке рюкзака. ``Рюкзачная’’ система шифрования. Криптографические хеш-функции.
11. Китайская теорема об остатках. Арифметический вариант шифра Виженера.
12. Шифры перестановки и шифры замены. Блочные и поточные шифры.
13. Шифры гаммирования. Восстановление текстов, зашифрованных неравновероятной гаммой.
14. Криптографические хеш-функции. Цифровая подпись.
15. Квантово-криптографический протокол открытого распределения ключей.