С/к естественно-научного содержания ``Арифметические вопросы криптографии и теория чисел’’, ½ г.

Профессор В.Н.Чубариков

1. Понятие информации и её кодирование. Помехоустойчивость, увеличение скорости передачи информации, защита информации.
2. Секретные и открытые ключи. Алфавитное кодирование. Префиксные коды. 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 Вильсона, малая 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.