Экзаменационная программа курса «Теория информации и криптография», мехмат, направление подготовки «ФИИТ», 3 курс, 2 семестр 2014–2015 учебного года

Энтропия (наводящие соображения, теорема о виде функции $h(p)$). Две леммы, оценка $0 \le H(X) \le \log |X|$. Совместная энтропия двух случайных величин, теорема об оценке $H(X,Y) \le H(X) + H(Y)$. Условная энтропия. Теорема: $H(X,Y) = H(X) + H(Y \mid X)$. Теорема: $H(X \mid Y) \le H(X)$.

Дискретный стационарный источник, дискретный постоянный источник. Теорема об энтропийных характеристиках дискретного стационарного источника. Понятие о кодировании, равномерный код, скорость равномерного кода. Оценка для математического ожидания дискретной случайной величины, неравенство Чебышёва. Прямая теорема (равномерного) кодирования дискретного постоянного источника.

Неравномерное кодирование. Однозначно декодируемые и префиксные коды. Теорема существования префиксного кода с заданными длинами кодовых слов (неравенство Крафта). Прямая и обратная теоремы неравномерного побуквенного кодирования. Код Хаффмана. Код Шеннона. Код Гилберта-Мура. Теоремы о неравномерном кодировании для дискретного стационарного источника в общем случае (прямая и обратная). Арифметическое кодирование.

Криптосистемы. Определение криптосистемы. Шифры сдвига, подстановки, перестановки. Аффинный шифр. Шифр Виженéра. Шифр Хилла. Шифр перестановки. Атаки на криптосистемы, принцип Керкгоффса. Тест Казиски, индекс совпадения, совместный индекс совпадения, понятие о криптоанализе шифра Виженéра.

Стойкость криптосистем. Абсолютная стойкость шифра сдвига. Теорема Шеннона. Ненадежность ключа, теорема о вычислении ненадежности ключа. Избыточность языка. Выпуклые вверх функции, неравенство Йенсена. Ложные ключи, нахождение математического ожидания числа ложных ключей, расстояние единственности.

Тесты на простоту числа. Тест на основе теоремы Ферма. Тест Соловея-Штрассена (критерий простоты чисел, следствие, алгоритм, вероятностный анализ). Понятие о тесте Миллера-Рабина.

Дискретное логарифмирование, алгоритм Поллига-Хеллмана. Криптосистема Эль-Гамаля.

Построение больших простых чисел. Лемма о делимости. Теорема Люкá, замечания. Числа Фермá, критерий простоты чисел Фермá.