# Экзаменационная программа курса «Теория информации и криптография», мехмат, 3 курс, направление подготовки «Информационные технологии», 2 семестр 2010-2011 учебного года

Определение криптосистемы. Шифр подстановки. Шифр сдвига. Шифр Виженéра. Шифр Хилла, объем ключевого пространства шифра Хилла. Шифр перестановки. Атаки на криптосистемы, принцип Керкгоффса. Тест Казиски, индекс совпадения, совместный индекс совпадения, понятие о криптоанализе шифра Виженéра.

Энтропия дискретной случайной величины. Простейшие свойства энтропии. Две леммы, оценка $0 \le H(X) \le \log m$. 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: $H(X \mid) \le H(X)$.

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 Чебышева. Прямая теорема (равномерного) кодирования дискретного постоянного источника. Обратная теорема (равномерного) кодирования дискретного постоянного источника (б/д).

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. Понятие о коде Хаффмана. Коды Шеннона. Код Гилберта-Мура. Теоремы о неравномерном кодировании в общем случае (обратная и прямая). Арифметическое кодирование.

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.

Алгоритм RSA.

Квадратичные вычеты и невычеты. Число квадратичных вычетов и невычетов. Критерий Эйлера. Символ Лежандра, простейшие свойства символа Лежандра. Квадратичный закон взаимности (без доказательства). Символ Якóби (определение, свойства символа Якóби).

ПРОСТЫЕ ЧИСЛА. Тест Ферма. Числа Кармайкла, критерий, следствие. Тест Соловея-Штрассена (лемма, алгоритм, теорема, вероятностный анализ). Тест Миллера-Рабина. Алгоритм факторизации чисел (алгоритм Полларда).

Построение больших простых чисел. Лемма о делимости. Критерий Люка́. Числа Ферма, критерий простоты чисел Ферма. Теорема Поклингтона. Теорема о простоте чисел вида $FR+1$. Критерий простоты чисел вида $2^k R+1$.

Криптосистема Эль-Гамаля. Алгоритм Поллига-Хеллмана дискретного логарифмирования.

## ФОРМУЛИРОВКИ НЕКОТОРЫХ ТЕОРЕМ

КРИТЕРИЙ ЛЮКА́. *Натуральное число $n$ является простым в том и только том случае, когда существует такое число $a$, что $a^{n-1} \equiv 1 (\mathrm{mod}\, n)$ и для любого $q \mid (n-1)$, $q>1$ выполняется соотношение $a^{\frac{n-1}{q}} \not\equiv 1 (\mathrm{mod}\, n)$.*

ТЕОРЕМА ПОКЛИНГТОНА. *Пусть $n = q^k R+1$, где $q$ простое число, $k \geq 1$. Если существует такое целое $a$, что $a^{n-1} \equiv 1 (\mathrm{mod}\, n)$, $(a^{(n-1)/q}-1, n)=1$, то каждый простой делитель $p$ числа $n$ имеет вид $p = q^k r+1$ при некотором натуральном $r$.*

ТЕОРЕМА. *Пусть $n = RF+1$, где $1 \leq R < F$. Если для любого простого делителя $q$ числа $F$ существует такое $a \in \mathbb{Z}$, что $a^{n-1} \equiv 1 (\mathrm{mod}\, n)$ $(a^{\frac{n-1}{q}}-1, n)=1$, то число $n$ простое.*

СЛЕДСТВИЕ. *Пусть $n = 2^k R+1$, где $k>1$, $R<2^k$ и $3 \nmid R$. Тогда число $n$ является простым в том и только том случае, когда $3^{\frac{n-1}{2}} \equiv -1 (\mathrm{mod}\, n)$.*