Экзаменационная программа спецкурса «Криптография» (специализация *«Защита информации»*), 4 курс, 1 семестр 2006–2007 учебного года

Основные задачи криптографии. Криптосистема. Шифры сдвига, подстановки, аффинный, Хилла, перестановки.

Криптоанализ шифра Виженера. Тест Казиски. Индекс совпадения. Взаимный индекс совпадения. Матричный анализ шифра Виженера.

Вычислительная и безусловная стойкость. Абсолютно стойкая криптосистема. Теорема об абсолютной стойкости шифра сдвига. Теорема Шеннона.

Энтропия. Определение энтропии. Кодирование Хаффмена, связь с энтропией. Вогнутые функции. Неравенство Йенсена. Теорема об оценке $0 \le H(X) \le \log_2 n$, условие равенства. Определение $H(X,Y)$. Теорема: $H(X,Y) \le H(X) + H(Y)$, случай равенства. Условная энтропия, полная условная энтропия, соотношение $H(X,Y) = H(Y) + H(X \mid Y)$, неравенство $H(X \mid Y) \le H(X)$, случай равенства.

Ложные ключи и расстояние единственности, ненадежность ключа. Теорема о вычислении $H(K \mid C)$. Алфавит, биграммы, триграммы, n-граммы. Энтропия языка, избыточность языка. Теорема об оценке числа ложных ключей: $\log_2(\overline{s}_n + 1) \ge H(K) - nR_L \log_2 |\mathcal{P}|$. Случай равновероятных ключей, оценка $\overline{s}_n \ge \dfrac{|\mathcal{K}|}{|\mathcal{P}|^{nR_L}} - 1$. Формула $n_0 \approx \dfrac{\log_2 |\mathcal{K}|}{R_L \log_2 |\mathcal{P}|}$.

Произведение криптосистем.

Алгоритм RSA. Тест Ферма для определения составного числа. Псевдопростое число по основанию a. Числа Кармайкла, критерий, следствие. Тест Соловея-Штрассена. Теорема о количестве чисел, удовлетворяющих условию $\left(\dfrac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \pmod n$. Вероятностный анализ теста Соловея-Штрассена. Тест Миллера-Рабина.

Построение больших простых чисел. Критерий Люка, замечания. Числа Ферма, критерий простоты. Лемма о делимости. Теорема Поклингтона (о представлении делителей числа вида $q^k R + 1$). Теорема о простоте числа вида $FR + 1$. Следствия о простоте чисел вида $2^k R + 1$.

Теорема Диемитко (лемма о простых делителях чисел $q^k R + 1$, теорема).

Метод Маурера. Леммы о простых делителях чисел вида $2FR + 1$ и простоте этих чисел. Неравенство для функции Эйлера. Леммы о числе элементов группы $\mathbb{Z}_p^*$ заданного порядка (делящего d, равного d, делящегося на d). Неравенство $\prod_{j=1}^{n}(1-\alpha_i) \ge 1 - \sum_{i=1}^{n} \alpha_i$. Алгоритм тестирования на простоту, его вероятностный анализ, следствие о нижней границе вероятности успеха.

Алгоритмы факторизации. Алгоритм Полларда.

Криптосистема Эль-Гамаля. Алгоритм Шенкса. Алгоритм Поллига-Хеллмана. Метод вычисления индексов.

Формулировки утверждений из раздела «Построение больших простых чисел»

Лемма о делимости. *Пусть q — простое. Если $m \mid q^k R$, $m \nmid q^{k-1} R$ ($k \geq 1$), то $q^k \mid m$.*

Теорема. *Натуральное число n является простым $\Leftrightarrow$ существует такое число a, что $a^{n-1} \equiv 1 (\mathrm{mod}\, n)$ и для любого $q \mid (n-1)$, $q > 1$ выполняется соотношение $a^{(n-1)/q} \not\equiv 1 (\mathrm{mod}\, n)$.*

Теорема: *число $F_k = 2^{2^k} + 1$, $k \geq 1$ простое в том и только том случае, когда выполняется условие $3^{(F_k - 1)/2} \equiv -1 (\mathrm{mod}\, F_k)$.*

Теорема Поклингтона.

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

Теорема. *Пусть $n = RF + 1$, где $1 \leq R < F$. Если для любого простого делителя q числа F $\exists$ целое a, что $a^{n-1} \equiv 1 (\mathrm{mod}\, n)$, $(a^{(n-1)/q} - 1, n) = 1$ то число n простое.*

Следствие 1. *$n = 2^k R + 1$, $k > 1$, $R < 2^k$. n простое $\Leftrightarrow \exists a \in \mathbb{Z}$, $a^{\frac{n-1}{2}} \equiv -1 (\mathrm{mod}\, n)$.*

Следствие 2. *$n = 2^k R + 1$, $k > 1$, $R < 2^k$, $3 \nmid R$. n простое $\Leftrightarrow 3^{\frac{n-1}{2}} \equiv -1 (\mathrm{mod}\, n)$.*

Теорема Диемитко

Лемма. *Пусть $n = q^k R + 1$, где q — простое число. Если $\exists a \in \mathbb{Z}$, $a^{n-1} \equiv 1 (\mathrm{mod}\, n)$, $a^{\frac{n-1}{q}} \not\equiv 1 (\mathrm{mod}\, n)$,*

то $\exists$ простой делитель p числа n, такой, что $p = q^k r + 1$ при некотором целом r.

Теорема. *Пусть $n = qR + 1$, где q — нечетное простое, R — четное и $R < 4(q+1)$. Если существует такое a, что $a^{n-1} \equiv 1 (\mathrm{mod}\, n)$, $a^{\frac{n-1}{q}} \not\equiv 1 (\mathrm{mod}\, n)$, то число n простое.*

Метод Маурера

Лемма 1. *Пусть $n = 2FR + 1$. Если для любого простого делителя q числа F существует такое целое число a, что $a^{n-1} \equiv 1 (\mathrm{mod}\, n)$, $(a^{\frac{n-1}{q}} - 1, n) = 1$, то каждый простой делитель p числа n имеет вид $p = rF + 1$ при некотором целом r. Если, кроме того, $F \geq \sqrt{n}$ или F нечетное и $R \leq F$, то число n простое.*

Лемма 2. *Пусть $n = 2FR + 1$. Предположим, что для любого простого делителя q числа F существует такое целое число a, что $a^{n-1} \equiv 1 (\mathrm{mod}\, n)$, $(a^{\frac{n-1}{q}} - 1, n) = 1$. Определим числа x, y следующими условиями: $x \geq 0$, $0 \leq y < F$, $2R = xF + y$. Если $F \geq \sqrt[3]{n}$ и число $y^2 - 4x$ не является полным квадратом, то число n простое.*

Лемма 3. *Функция Эйлера удовлетворяет неравенству $\varphi(mn) \geq \varphi(m)\varphi(n)$, m, $n \geq 1$, причем равенство имеет место в том и только том случае, когда числа m и n взаимно простые.*

ЛЕММА 4. *Пусть* p *— нечетное простое число,* $d \mid (p-1)$. *Тогда число элементов группы* $\mathbb{Z}_p^*$, *порядки которых делят число* d, *равно* d.

ЛЕММА 5. *Пусть* p *— нечетное простое число,* $d \mid (p-1)$. *Тогда число элементов группы* $\mathbb{Z}_p^*$, *порядки которых равны* d, *равно* $\varphi(d)$.

ЛЕММА 6. *Пусть* p *— нечетное простое число,* $d \mid (p-1)$. *Обозначим через* T *число элементов группы* $\mathbb{Z}_p^*$, *порядки которых делятся на* d. *Тогда имеет место неравенство* $T \geq \dfrac{\varphi(d)}{d} \cdot (p-1)$ *причем равенство имеет место в том и только том случае, когда числа* d *и* $\dfrac{p-1}{d}$ *являются взаимно простыми.*

ЛЕММА 7. *Предположим, что числа* α_1, α_2, ..., α_n *удовлетворяют условиям* $0 \leq \alpha_i < 1$, $i = 1, 2, \ldots, n$. *Тогда имеет место неравенство* $\prod_{j=1}^{n} (1-\alpha_i) \geq 1 - \sum_{i=1}^{n} \alpha_i$, *причем равенство имеет место в том и только том случае, когда все числа* α_i, *кроме, возможно, одного, равны нулю.*

АЛГОРИТМ ТЕСТИРОВАНИЯ НА ПРОСТОТУ.

Пусть $n = 2FR + 1$, $R < F$ и F нечетное. Выбираем случайным образом число a, $1 \leq a \leq n-1$. Если $a^{n-1} \equiv 1 (\mathrm{mod}\, n)$ и для любого простого делителя q числа F выполняется соотношение $(a^{(n-1)/q} - 1, n) = 1$, то n простое число. Иначе неизвестно.

ТЕОРЕМА. *Пусть* $n = 2RF + 1$ *— простое число,* $R < F$ *и* $(2R, F) = 1$. *Тогда вероятность того, что случайно выбранное число* a, $1 \leq a \leq n-1$, *будет доказывать простоту числа* a *по данному алгоритму, равна* $\dfrac{\varphi(F)}{F}$.

СЛЕДСТВИЕ. *В условиях теоремы при достаточно больших* q_1, q_2, ..., q_s *в качестве нижней оценки вероятности успеха можно взять величину* $1 - \sum_{i=1}^{s} \dfrac{1}{q_i}$.