Математические основы криптологии

Автор курса: Применко Эдуард Андреевич
Составитель: Смирнов Дмитрий Константинович

Версия от 00:20, 1 марта 2022 г.

Оглавление

Часть 1

Домашние задания

1.1 Элементы теории групп

Задачи в этом разделе решаются со следующими параметрами:

p	**g**	**k**
23	-8	22

Задача 1.1 Убедиться, что $g \in \mathbb{Z}_p^*$ – примитивный элемент $\mathbb{Z}_p$.

Так как $p = 23$ – простое число, то $\phi(p) = p - 1 = 22$. Разложим это число на простые множители: $\phi(p) = 2 \cdot 11$. Тогда достаточно проверить следующие 2 неравенства:

$$g^{\frac{\phi(p)}{2}} = (-8)^{11} = 15 \cdot 15^{10} = 15 \cdot 18^5 = 17 \cdot 2^2 = 22 \not\equiv 1 \pmod p,$$

$$g^{\frac{\phi(p)}{11}} = (-8)^2 = 18 \not\equiv 1 \pmod p,$$

и одно равенство:

$$g^{\phi(p)} = (-8)^{22} = 18^{11} = 18 \cdot 2^5 = 18 \cdot 9 \equiv 1 \pmod p.$$

Делаем вывод, что g действительно является примитивным элементом $\mathbb{Z}_p$.

Задача 1.2 Найти образующий элемент h группы $\mathbb{Z}_{p^2}^*$

Образующий элемент группы $\mathbb{Z}_{p^n}^*, n \geq 2$ имеет вид:

$$h = g + t_0 p,\ t_0 \not\equiv g\nu \pmod p;\ \nu = (\frac{g^{\frac{p-1}{2}} + 1}{p})(\mathrm{mod}\ p) \cdot (-2)(\mathrm{mod}\ p)$$

Таким образом,

$$\nu = (\frac{(-8)^{\frac{23-1}{2}} + 1}{23})(\mathrm{mod}\ 23) \cdot (-2)(\mathrm{mod}\ 23) = (1 \cdot (-2))(\mathrm{mod}\ 23) = 21$$

$$t_0 \not\equiv (-8) \cdot 21 \ \ (\mathrm{mod}\ 23) = 16 \ \ (\mathrm{mod}\ 23)$$

$$t_1 = 1 \Rightarrow h = (-8) + 1 * 23 = 15$$

Следовательно, $h = 15$ – образующий элемент группы $\mathbb{Z}^*_{23^2}$
Задача 1.3 Подсчитать число образующих группы $\mathbb{Z}^*_{p^3}$

Число образующих группы $\mathbb{Z}^*_{23^3}$ равно $\phi(23^3) = (23-1)23^{3-1} = 11638$.
Задача 1.4 Найти элемент a группы $\mathbb{Z}^*_{p^2}$ порядка k

Так как $\forall$ натурального $k > 1$ и простого $p \geq 3$ группа $\mathbb{Z}^*_{p^k}$ является циклической, то $\mathbb{Z}^*_{23^2}$ – циклическая группа. Элемент порядка k в циклической группе порядка N имеет вид h^r, где $r = \frac{N}{k}$. Таким образом,

$$a = h^{\frac{\phi(p^2)}{k}} = 15^{\frac{22*23}{22}} = 15^{23} = 130$$

Задача 1.5 Решить сравнение $a^x \equiv b \pmod p$

p	a	b
701	2	163

I. Алгоритм согласования

1. Убедимся в том, что $a = 2$ – примитивный элемент группы $\mathbb{Z}_{701}$.

$$\phi(701) = 700 = 2^2 \cdot 5^2 \cdot 7$$

$$g^{\frac{\phi(p)}{2}} = 2^{350} = 700 \not\equiv 1 \pmod p,$$

$$g^{\frac{\phi(p)}{5}} = 2^{140} = 210 \not\equiv 1 \pmod p,$$

$$g^{\frac{\phi(p)}{7}} = 2^{100} = 19 \not\equiv 1 \pmod p,$$

$$g^{\phi(p)} = 2^{700} = 1 \equiv 1 \pmod p,$$

Таким образом, порядок элемента a равен $ord(a) = 700$.

2. Выбираем минимальное m: $m^2 \geq ord(a) \Rightarrow m = 27$.
3. Вычисляем $c = a^m = 2^{27} = 62$.
4. Составляем два множества:

i	1	2	3	4	5	6	7	8	9	10	11	12	13	14
c^i	62	339	689	658	138	144	516	447	375	117	244	407	699	577

i	15	16	17	18	19	20	21	22	23	24	25	26	27
c^i	23	24	86	425	413	370	508	652	467	213	588	4	248

j	0	1	2	3	4	5	6	7	8	9	10	11	12	13
ba^j	163	326	652	603	505	309	618	535	369	37	74	148	296	592

j	14	15	16	17	18	19	20	21	22	23	24	25	26
ba^j	483	265	530	359	17	34	68	136	272	544	387	73	146

В таблицах совпадают элементы под номерами $i = 22$ и $j = 2$.

5. Таким образом, $x = mi - j = 27 \cdot 22 - 2 = 592$.

Ответ: $x = 592$.

II. Алгоритм Полига-Хеллмана

Порядок поля $\mathbb{Z}_{701}$ равен $N = \phi(701) = 700 = 2^2 \cdot 5^2 \cdot 7$. Количество простых множителей в разложении этого числа $t = 3$.

1. Вычисляем матрицу с элементами $(i, j) = a^{j\frac{N}{p_i}}$, $i = \overline{1, t}$, $j = \overline{0, p_i - 1}$:

p_i \ j	0	1	2	3	4	5	6
2	$2^{0\cdot\frac{700}{2}}$	$2^{1\cdot\frac{700}{2}}$	-	-	-	-	-
5	$2^{0\cdot\frac{700}{5}}$	$2^{1\cdot\frac{700}{5}}$	$2^{2\cdot\frac{700}{5}}$	$2^{3\cdot\frac{700}{5}}$	$2^{4\cdot\frac{700}{5}}$	-	-
7	$2^{0\cdot\frac{700}{7}}$	$2^{1\cdot\frac{700}{7}}$	$2^{2\cdot\frac{700}{7}}$	$2^{3\cdot\frac{700}{7}}$	$2^{4\cdot\frac{700}{7}}$	$2^{5\cdot\frac{700}{7}}$	$2^{6\cdot\frac{700}{7}}$

p_i \ j	0	1	2	3	4	5	6
2	1	700	-	-	-	-	-
5	1	210	638	89	464	-	-
7	1	19	361	550	636	167	369

2. Далее находим $x_i = \log_a b \pmod{p_i^{k_i}} = \gamma_0 + \gamma_1 p_i + ... + \gamma_{k_i-1} p_i^{k_i-1}, \gamma_j \in \mathbb{Z}_p$. Последовательно находим γ_j из $M(p, \gamma_j) = b_j^{\frac{N}{p^{j+1}}}$, где $b_j = ba^{-\gamma_0 - \gamma_1 p - ... - \gamma_{j-1}p^{j-1}}$, а M – определённая выше матрица.

а) $x_1 = \log_2 163 \pmod{2^2}$, $p = 2$, $k = 2$

$M(p, \gamma_0) = b^{\frac{N}{p}} = 163^{\frac{700}{2}} = 1 \Rightarrow \gamma_0 = 0$, $b_1 = ba^{-\gamma_0} = 163 \cdot 2^{-0} = 163$

$M(p, \gamma_1) = b_1^{\frac{N}{p^2}} = 163^{\frac{700}{4}} = 1 \Rightarrow \gamma_1 = 0$

$\Rightarrow x_1 = \gamma_0 + \gamma_1 p = 0 + 0 \cdot 2 = 0$

б) $x_2 = \log_2 163 \pmod{5^2}$, $p = 5$, $k = 2$

$M(p, \gamma_0) = b^{\frac{N}{p}} = 163^{\frac{700}{5}} = 638 \Rightarrow \gamma_0 = 2$, $b_1 = ba^{-\gamma_0} = 163 \cdot 2^{-2} = 216$

$M(p, \gamma_1) = b_1^{\frac{N}{p^2}} = 216^{\frac{700}{25}} = 89 \Rightarrow \gamma_1 = 3$

$\Rightarrow x_2 = \gamma_0 + \gamma_1 p = 2 + 3 \cdot 5 = 17$

в) $x_3 = \log_2 163 \pmod 7$, $p = 7$, $k = 1$

$M(p, \gamma_0) = b^{\frac{N}{p}} = 163^{\frac{700}{7}} = 636 \Rightarrow \gamma_0 = 4$

$\Rightarrow x_3 = \gamma_0 = 4$

3. На основе вычисленных выше значений $x_1, x_2, ..., x_t$ и китайской теоремы об остатках находим искомый логарифм:

$$x = \sum x_i \frac{N}{p_i^{k_i}} [(\frac{N}{p_i^{k_i}})^{-1} \pmod{p_i^{k_i}}] \pmod N = 0 \cdot \frac{700}{2^2}[(\frac{700}{2^2})^{-1} \pmod{2^2}] +$$

$$+17 \cdot \frac{700}{5^2}[(\frac{700}{5^2})^{-1} \pmod{5^2}] + 4 \cdot \frac{700}{7}[(\frac{700}{7})^{-1} \pmod 7] \pmod{700} =$$

$$= 476 \cdot [28^{-1} \pmod{25}] + 400 \cdot [100^{-1} \pmod 7] \pmod{700} =$$

$$= 476 \cdot 17 + 400 \cdot 4 \pmod{700} = 592$$

Ответ: $x = 592$.

1.2

Часть 2

Билеты

2.1 Делимость в кольце целых чисел. НОД, алгоритм Евклида. Критерий взаимной простоты двух чисел.

2.2 Сравнения и их свойства. Китайская теорема об остатках. Кольцо вычетов. Функция Эйлера и её свойства.

2.3 Теоремы Эйлера и Ферма. Критерий обратимости, алгоритм вычисления обратного элемента.

2.4 Криптографическая теорема (обоснование криптосистемы РСА).

2.5 Теорема о цикличности мультипликативной группы по примарному модулю.

2.6 Решение сравнений первой степени.

2.7 Сравнения второй степени. Символ Лежандра и его свойства.

2.8 Алгоритмы решения сравнений второй степени по простому модулю.

2.9 Символ Якоби и его свойства. Числа Блюма и их свойства. Эквивалентность задачи факторизации и решения сравнения второй степени.

2.10 Алгоритмы решения сравнений второй степени по примарному и составному модулю.

2.12 Нормальный делитель, фактор – группа, первая теорема о гомоморфизме.

2.13 Кольцо многочленов, идеал, теорема Безу, кольцо главных идеалов.

2.14 Конечное поле. Теорема о простом подполе конечного поля. Строение конечного поля. Теорема о примитивном элементе.

2.15 Построение конечных полей. Алгоритм вычисления обратного элемента. Арифметические операции в конечном поле.

2.16 Алгоритмы вычисления дискретного алгоритма.

2.17 Криптосистема Эль - Гамаля. Протокл Диффи - Хеллмана.

2.18 Минимальный многочлен и его свойства. Теорема об изоморфизме конечных полей одной мощности.

2.19 Примитивный многочлен и его свойства. Теорема о разложении многочлена $f(x) = xp^n - x$ на неприводимые многочлены. Критерий принадлежности элемента поля собственному подполю.

2.20 Теорема о группе автоморфизмов конечного поля.

2.21 Рекуррентные последовательности над конечным полем, линейные рекуррентные последовательности (ЛРП). Характеристический и минимальный многочлен ЛРП и их свойства.

2.22 Теорема об определении структуры ЛРП по её характеристическому многочлену. Теорема о ЛРП максимального периода.

2.23 Прямое произведение групп. Теорема о представлении группы в виде прямого произве-

2.25 Теорема о разложении конечной абелевой группы в произведение своих циклических подгрупп.

2.26 Нормализатор, централизатор, класс сопряженных элементов конечной группы. Теорема о числе множеств сопряженных с данным. Теорема о центре примарной группы. Теорема Коши.

2.27 Двойные смежные классы и их свойства. Теорема Силова (первая)

2.28 Вторая и третья теоремы Силова.

2.29 Группы подстановок. Инвариантное множество, орбита. Теорема об индексе стабилизатора группы. Теорема о транзитвности нормализатора подгруппы транзитвной группы. (Ут . 13.4).

2.30 Лемма Бернсайда.

2.31 Регулярные и полурегулярные группы. Порядок полурегулярной группы.

2.32 Блоки и импримитивные группы. Критерий импримитивности. Теорема о импримитивности транзитивной группы с интранзитивным нормальным делителем.

2.33 Примитивные группы. Кратная транзитивность. Критерий кратной транзитивности.

2.34 Теорема о группе автоморфизмов конечной группы.

2.35 Утверждение об изоморфизме стабилизатора и специальной группы автоморфизмов регулярной подгруппы (Ут . 13.5). Утверждение о порядке регулярного нормального делителя кратно транзитивной группы.

2.36 Простая группа. Теорема о простоте знакопеременной группы. Теорема о нормальном