Лекция 1. Введение

Криптография как учение об искусстве тайнописи возникла в древние времена. Потребность шифровать и передавать шифрованные сообщения возникла очень давно. Известны специальные шифровальные устройства V-VI веков до нашей эры, а именно две специальные палки одинаковой длины и диаметра. Эти палки назывались *скиталами*. Когда один из двух союзников должен был передать другому некоторое сообщение, то на скиталу наматывалась длинная полоска папируса и сообщение писалось вдоль скиталы. Эта полоска передавалась другому союзнику и он мог ее прочесть, только намотав на такую же скиталу.

В настоящее время *криптология* – это наука, содержащая две взаимосвязанные части, а именно, криптографию, изучающую различные методы шифрования текстов и их расшифрования, и *криптоанализ*, изучающий методы, позволяющие расшифровать перехваченное сообщение, не зная самого ключа для расшифрования.

Позднее шифры усложнялись, совершенствовались и применялись вплоть до 70-х годов XX века в основном в военных и политических кругах для обеспечения конфиденциальности информации. Однако с развитием предпринимательской деятельности частных фирм, появлением компьютерных сетей, в особенности, Интернета, появилось много новых проблем защиты информации. В банковской сфере важной задачей является задача *обеспечения целостности информации*, т.е. ее поступления в неискаженном виде, а также гарантии поступления из известного источника, т.е. задача *аутентификации* (проверка подтверждения авторства). В настоящее время в деловых кругах широко используется *электронная подпись*. Еще одна задача криптографии связанная с появлением электронных денег – это *обеспечение неотслеживаемости* расходов клиента в электронных деньгах, т.е. свойство которым обладают

обычные бумажные деньги. Задача была поставлена в работах Шаума в 80-х годах XX века и какое-то время оставалась не замеченной. Речь идет о правах клиента свободно распоряжаться своими деньгами. С другой стороны, полная неотслеживаемость вредна и может способствовать росту организованной преступности.

Современная криптография существенно использует математические методы и понятия, в частности, такие разделы как 1) теорию конечных колец и и полей; 2) теорию чисел; 3) матрицы; 4) большие простые числа; 5) теорию вероятности и т.д.

Тема 1. Сравнения, кольца вычетов, расширенный алгоритм Евклида

Определение 1. Два целых числа a и b называются *сравнимыми по модулю* m, если их разность делится на m. Число m называется *модулем сравнения*, а факт сравнимости чисел записывается как $a \equiv b \bmod m$.

Если m – модуль сравнения, то при делении произвольного целого числа на m с остатком можно получить один из m различных остатков, а именно: $0,1,2,\ldots,m-1$. Таким образом, любое целое число a можно представить в виде

$$a = mq + r, \tag{1}$$

где

$$r \in \{0,1,2,\ldots,m-1\} \tag{2}$$

– *остаток* от деления a на m, а q – *неполное частное* от деления.

Таким образом, все целые числа можно распределить по m классам:

$$\bar{0} = \{lm\},\ \bar{1} = \{1+lm\},\ldots,\ \overline{m-1} = \{m-1+lm\}, \tag{3}$$

где $l \in \mathbb{Z}$, т.е. это произвольное целое число.

Определение 2. Множества $\overline{0}, \overline{1}, \ldots, \overline{m-1}$ называются *классами вычетов по модулю* m.

Над классами вычетов можно производить обычные операции сложения и умножения:

$$\overline{r_1} + \overline{r_2} = \overline{r_1 + r_2}; \quad \overline{r_1} \cdot \overline{r_2} = \overline{r_1 \cdot r_2} \tag{4}$$

Определение 3. Множество классов вычетов (2) по модулю m с операциями сложения и умножения, определенные формулами (3), называется *кольцом вычетов по модулю* m и обозначается $\mathbb{Z}_m$.

Как правило, элементы кольца вычетов мы будем обозначать обычными числами $\{0,1,2,\ldots,m-1\}$, опуская черту сверху.

Пример 1. Постройте таблицы сложения и умножения в кольце $\mathbb{Z}_4$.

Решение. $\mathbb{Z}_4 = \{0,1,2,3\}$.

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Важную роль в криптографии играет понятие обратимости элемента.

Определение 4. Элемент a^{-1} в кольце вычетов называется *обратным к элементу* a, если их произведение равно единичному вычету 1. Элемент a называется *обратимым*, если он имеет обратный элемент.

Пример 2. В кольце $\mathbb{Z}_4$ укажите все обратимые и все необратимые элементы.

Решение. Непосредственно из таблицы умножения можно усмотреть, что множество обратимых элементов есть $\{1,3\}$: $1^2=1,\ 3^2=1.$ Элементы 0 и 2 обратимыми не являются. Более того, $2^2=0.$

Легко видеть, что умножение в кольце вычетов ассоциативно и коммутативно и существует единица 1 относительно умножения. Классы вычетов будем обозначать по их представителям, т.е. натуральным числам $0,1,\ldots,m-1.$ Кольцо вычетов по модулю m обозначается $Z_m.$

Замечание 1. Кольца вычетов дают основные примеры конечных колец и полей, которые играют важную роль в приложениях алгебры. Свойство обратимости является существенным при решении различных задач в криптографии и теории кодирования. Этот факт важен, так как здесь нужно иметь процессы, которые идут в противоположных направлениях: шифрование и дешифрование, кодирование и декодирование.

Для любых двух целых чисел a и $b\neq 0$ возможно *деление с остатком*, т.е. представление числа a в виде:

$$a=bq+r, \tag{5}$$

где

$$0\le r<|b|. \tag{6}$$

Определение 6. Наибольшим общим делителем (НОД) двух целых чисел a и $b\neq 0$ называется положительное число $d\neq 0$, которое делится на любой общий делитель c чисел a и b, т.е. из того, что $a=a_1c$ и $b=b_1c$, следует, что $d=qc$.

Для нахождения наибольшего общего делителя (НОД) двух целых чисел служит алгоритм Евклида, который состоит в последовательном применении деления с остатком, а именно:

$$r_0 = a,\ r_1 = b,\quad r_0 = r_1 q_1 + r_2,\ r_1 = r_2 q_2 + r_3,\ \ldots,\quad r_{n-2} = r_{n-1} q_{n-1} + r_n,$$

$$r_{n-1} = r_n q_n. \qquad (7)$$

Наибольший общий делитель целых чисел a и $b \neq 0$ далее будем обозначать (a,b).

Теорема 1 (теорема Евклида). *Наибольший общий делитель* (a,b) *двух целых чисел* a *и* $b \neq 0$ *равен последнему ненулевому остатку в цепочке* (7).

Доказательство. Доказательство основано на простом наблюдении, что для равенства (5) верно $(a,b) = (b,r)$, что проверяется непосредственно. В самом деле, если d – общий делитель чисел a и b, то $a = a_1 d,\ b = b_1 d$. Следовательно, из равенства (5) имеем, что $r = a - bq = d(a_1 - b_1 q)$, т.е. r делится на d. Поэтому, d есть делитель (b,r).

Обратно, таким же образом всякий общий делитель b и r, есть делитель (a,b). Следовательно, для цепочки делений (7) имеем равенства

$$(r_0, r_1) = (r_1, r_2) = \ldots = (r_{n-1}, r_n) = r_n. \qquad (8)$$

С другой стороны, в силу неравенства (6) в цепочке (7) справедливы неравенства

$$|r_1| > r_2 > \ldots > r_{n-1} > r_n \geq 0. \qquad (9)$$

Следовательно, процесс деления с остатком закончится на конечном шаге.

Следствие. *В алгоритме Евклида для нахождения наибольшего общего делителя ненулевых целых чисел* a *и* b *вычисления производятся по формулам*

$$r_0 = a,\ r_1 = b,\ r_k = r_{k-2} - r_{k-1} q_{k-1}\ (2 \leq \mathrm{k} \leq \mathrm{n}), \qquad (10)$$

причем верны неравенства (9).

Теорема 2 (о линейном представлении НОД). *Если* $d=(a,b)$, *то существуют целые числа* u и v, *для которых верно равенство*

$$d=ua+vb. \qquad (11)$$

Множители u и v в представлении (11) называются *множителями Безу*.

В качестве следствия из доказательства теоремы имеем

Следствие 1. *Наибольший общий делитель ненулевых целых чисел* a *и* b, *а также множители Безу* u *и* v *в формуле* (11) *можно найти с помощью расширенного алгоритма Евклида, в котором вычисления производятся по формулам* (10) *и формулам*

$$x_0=1, x_1=0,\ y_0=0, y_1=1,$$
$$x_k=\mathrm{x}_{k-2}-\mathrm{x}_{k-1}\mathrm{q}_{k-1},\ \mathrm{y}_k=\mathrm{y}_{k-2}-\mathrm{y}_{k-1}\mathrm{q}_{k-1}\ \ (2\le \mathrm{k}\le \mathrm{n}). \qquad (12)$$

Вычисления по формулам (10) и (12) *производятся вплоть до получения первого нулевого остатка. Если* $r_{n+1}=0$, но $r_n\neq 0$, *то вычисления заканчиваются и полагаем* $d=r_n$, $u=x_n$, $v=y_n$.

Следствие 2. *Числа* a и b *взаимно просты тогда и только тогда, когда*

$$ua+vb=1 \qquad (13)$$

для некоторых целых чисел u и v.

Теорема 3 (критерий обратимости элемента кольца вычетов). *Элемент* b *кольца вычетов по модулю* m *обратим тогда и только тогда, когда он взаимно прост с модулем* m, *т.е. наибольший общий делитель чисел* b *и* m *равен* 1, *т.е.*

$$(b,m)=1. \qquad (14)$$

Доказательство теоремы 3. Пусть m натуральное число и b – целое число такое, что $0<b\le m-1$ и $(b,m)=1$. В силу следствия 2 из теоремы 2 равенство (17) при $a=m$ выполняется для некоторых

целых u и v. Тогда $um = 1 - vb$, т.е. $vb \equiv 1 \bmod m$. Следовательно, $b^{-1} \bmod m \equiv v$.

Обратно, если элемент b имеет обратный v по модулю m, то $vb \equiv 1 \bmod m$, т.е. $vb - 1 = -um$ для некоторого целого u. Отсюда получаем справедливость равенства $vb + um = 1$. Теорема доказана.

Определение 7. Кольцо вычетов называется *полем*, если любой ненулевой его элемент имеет обратный.

Следствие. Кольцо вычетов Z_m является полем в том и только том случае, если модуль m есть простое число.

Для практического нахождения решения уравнения (11) и, в частности, (13) можно использовать так называемый расширенный алгоритм Евклида, который описан в следствии 1 из теоремы 2.

Способ нахождения обратного элемента по модулю m описывается перед задачей 2 ниже.

Примеры решения задач.

Задача 1. Найдите наибольший общий делитель (a,b) и множители Безу u, v, удовлетворяющие равенству (11) для чисел 851 и 667.

*Решение***.** Положим

$$r_0 = 851,\ r_1 = 667,\ x_0 = 1,\ y_0 = 0,\ r_0 = ax_0 + by_0,\ x_1 = 0,\ y_1 = 1,$$

Решение задачи с помощью расширенного алгоритма Евклида может быть достаточно коротко записано в виде следующей таблицы:

i	0	1	2	3	4	5	6	7
r_i	851	667	184	115	69	46	23	0
q_i	–	1	3	1	1	1	2	
x_i	1	0	1	–3	4	–7	11	
y_i	0	1	–1	4	–5	9	–14	

На каждом шаге сначала подбирается неполное частное q_{k-1} как наибольшее целое число, удовлетворяющее неравенству $r_{k-2} - r_{k-1}q_{k-1} \geq 0$. Затем в таблице производятся вычисления по формулам (12) и (13) вплоть до получения в строке r_i нулевого остатка.
Проверка: $851 \cdot 11 + 667 \cdot (-14) = 9361 - 9338 = 23$.
Ответ: $d = 23,\ u = 11,\ v = -14.$

Расширенный алгоритм Евклида позволяет вычислять обратные элементы в кольцах вычетов. Для этого следует применить расширенный алгоритм Евклида для нахождения u и v в представлении (11), взяв в качестве первого числа a модуль m, т.е. для представления

$$mu + bv = 1 \qquad (14')$$

Тогда при условии, что $0 < b < m$, в качестве обратного элемента элементу b по модулю m можно взять элемент v.

Задача 2. Найдите обратный элемент a^{-1} для $a = 17$ по модулю $m = 91.$
Решение. Заметим, что $(17,91) = 1.$ Следовательно, по теореме 3 обратный 17^{-1} по модулю $m = 91$ существует. Для его нахождения применим расширенный алгоритм Евклида, а именно найдем числа u и v, удовлетворяющие равенству $1 = mu + av,$ т.е. $1 = 17u + 91v.$
Положим $r_0 = 91,\ r_1 = 17,\ x_0 = 1,\ y_0 = 0,\ x_1 = 0,\ y_1 = 1,$
Дальнейшие вычисления запишем, как в примере 5, в виде таблицы.

I	0	1	2	3	4	5
r_i	91	17	6	5	1	0
q_i	–	5	2	1	5	
x_i	1	0	1	–2	3	
y_i	0	1	–5	11	–16	

Проверка: $91 \cdot 3 + 17 \cdot (-16) = 1.$ Теперь
$17^{-1} \bmod 91 \equiv -16 \equiv 75 \bmod 91.$
Ответ: $17^{-1} \bmod 91 \equiv 75.$

Замечание 2. Этот алгоритм применим при условии, что элемент $a < m$. В противном случае, следует либо привести элемент a по модулю m к такому случаю, либо понять, что иначе в качестве a^{-1} следует брать не v, а u.

Дополнительные задачи для самостоятельного решения

1. Найдите наибольший общий делитель d двух целых чисел, а также множители Безу u и v в их линейном представлении (8): а) 217 и 413; б) 4214 и 1176; в) 3751 и 1023; г) 5529 и 4559.

2. Определите, являются ли следующие пары целых чисел взаимно простыми а) 1722 и 1355; б) 2356 и 1519.

3. а) Постройте таблицы сложения и умножения для колец вычетов Z_5, Z_6 и Z_8; б) укажите группы U_m обратимых элементов этих колец; в) укажите множества $Div(Z_m)$ делителей нуля в них.

4. Решите сравнения в кольцах вычетов:

а) $x^2 \equiv 5 \bmod 11$; б) $x^2 \equiv 10 \bmod 13$; в) $x^2 \equiv 11 \bmod 14$;

г) $x^2 \equiv 16 \bmod 21$; д) $x^2 \equiv 1 \bmod 8$.

5. С помощью расширенного алгоритма Евклида найдите обратный элемент a^{-1} по модулю m: а) $a = 19,\ m=93$; б) $a = 31,\ m=73$; в) $a = 181,\ m=101$; г) $a = 305,\ m=107$; д) $a = 653,\ m=309$.

6. Укажите все обратимые элементы в кольцах вычетов а) Z_6, б) Z_8, в) Z_{12}, г) Z_{15}, д) Z_{11}, а также число обратимых элементов в них.

7*. Определите, какие из следующих колец вычетов являются полями: Z_{29}, Z_{101}, Z_{187}, Z_{203}, Z_{317}, Z_{541}, Z_{667}?

Ответы

1. а) $d=7,\ u=10,\ v=-19$; б) $d=98,\ u=-5,\ v=18$; в) $d=341,\ u=-1,\ v=4$; г) $d=97,\ u=-14,\ v=17$. **2.** а) взаимно простые; б) не взаимно простые, так как $d=31$.

3. $U_5=\{1,2,3,4\}$, $U_6=\{1,5\}$, $U_8=\{1,3,5,7\}$. **4.** а) $\{4,7\}$; б) $\{6,7\}$; в) $\{5,9\}$; г) $\{4,10,11,17\}$; д) $\{1,3,5,7\}$.

5. а) $19^{-1}\bmod 93\equiv 49$; б) $31^{-1}\bmod 73\equiv 33$; в) $181^{-1}\bmod 101\equiv 80^{-1}\bmod 101\equiv 24$; г) $305^{-1}\bmod 107\equiv 91^{-1}\bmod 107\equiv 20$; д) $653^{-1}\bmod 309\equiv 35^{-1}\bmod 309\equiv 53$. **6.** а) $U_6=\{1,5\}$, $|U_6|=2$; б) $U_8=\{1,3,5,7\}$, $|U_8|=4$; в) $U_{12}=\{1,5,7,11\}$, $|U_{12}|=4$; г) $U_{15}=\{1,2,4,7,8,11,13,14\}$, $|U_{15}|=8$; д) $U_{11}=\{1,2,3,4,5,6,7,8,9,10\}$, $|U_{11}|=10$. **7*.** Полями являются $\mathbb{Z}_{29}$, $\mathbb{Z}_{101}$, $\mathbb{Z}_{317}$, $\mathbb{Z}_{541}$.

10.09.2014

Лектор д.ф.-м.н., профессор А.В. Тищенко