Московский институт электроники и математики им. А.Н. Тихонова

Кафедра информационной безопасности киберфизических систем

Москва 2024

Криптографические методы защиты информации

Кольца

Общие сведения о кольцах

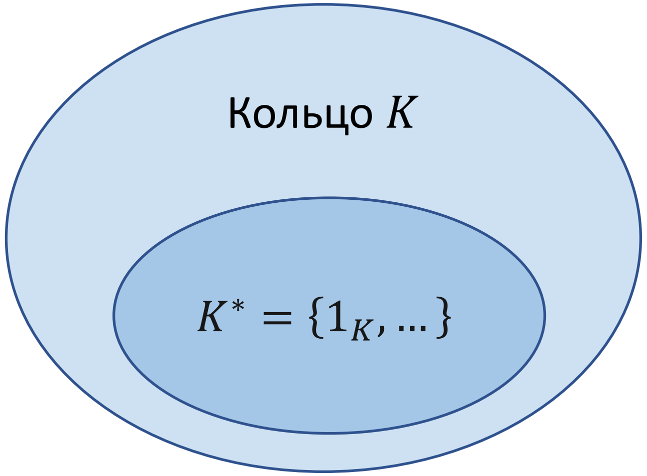
Понятие кольца

- На множестве K задана **структура кольца**, если на нем заданы две алгебраические операции, называемые сложением $(+)$ и умножением $(\cdot)$, причём выполняются следующие свойства:
  - $(K;+)$ является абелевой группой;
  - $(K;\cdot)$ является полугруппой;
  - выполняется двоякая дистрибутивность умножения относительно сложения, когда $\forall\, a,b,c \in K \Rightarrow \begin{cases} a(b+c) = ab+ac, \\ (a+b)c = ac+bc. \end{cases}$
- $(K;+;\cdot)$ — обозначение кольца.
- Абелева группа $(K;+)$ называется **аддитивной группой** кольца K.
- Полугруппа $(K;\cdot)$ называется **мультипликативной полугруппой** кольца K.
- Нейтральный элемент аддитивной группы кольца называется **нулем кольца** и обозначается 0_K или просто 0.

Свойства колец

- Виды колец:
  - если в $(K;\cdot)$ есть нейтральный элемент, называемый единицей кольца 1_K, то кольцо K называется **кольцом с единицей**;
  - если умножение в кольце K коммутативно, то кольцо K называется **коммутативным кольцом**.
- Простейшие свойства колец:
  - $0 \cdot x = x \cdot 0 = 0 \ \forall\, x \in K$;
  - $(-x) \cdot y = x \cdot (-y) = -(xy) \ \forall\, x, y \in K$;
  - $(-x) \cdot (-y) = xy \ \forall\, x, y \in K$;
  - $(-1_K) \cdot x = -x \ \forall\, x \in K$, если $\exists\, 1_K \in K$.

- Элемент u кольца с единицей K называется **обратимым элементом**, если $\exists\, u^{-1} \in K$ такой, что $u^{-1} \cdot u = u \cdot u^{-1} = 1_k$.
- Обратимые элементы кольца с единицей K образуют группу K^*.



Свойства колец

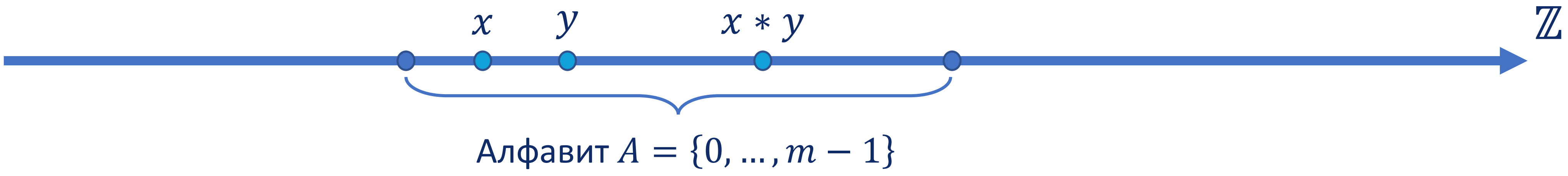
- В кольце с единицей K элементы вида 1, $1+1=2\cdot 1$, …, $\underbrace{1+\cdots+1}_{l}=l\cdot 1$ называются **целыми элементами кольца**.
  - Если все целые элементы кольца K отличны от нуля, то K называется кольцом **нулевой характеристики**, $\operatorname{char} K = 0$.
  - Если для некоторого $l \in \mathbb{N}$ выполняется $l\cdot 1 = 0$, причем l является наименьшим числом, обладающим данным свойством, то K называется кольцом **ненулевой характеристики** $\boldsymbol{l}$, $\operatorname{char} K = l$.

- **Пример** — кольцо целых чисел $\mathbb{Z}$:
  - коммутативное кольцо с единицей;
  - кольцо нулевой характеристики;
  - группа обратимых элементов $\mathbb{Z}^* = \{-1,1\}$.

Классы колец

- **Кольца классов вычетов**:
  - строятся на основе кольца целых чисел;
  - реализуют арифметику остатков.
- **Кольца многочленов**:
  - являются основой для построения полей Галуа.

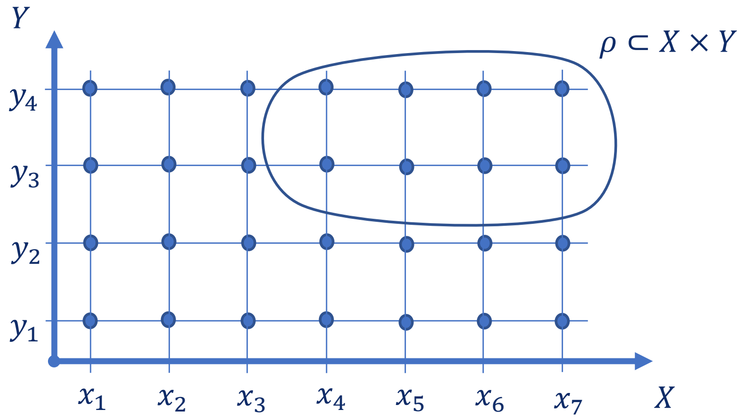
Для криптографии наибольшей ценностью обладают конечные структуры.



Кольца классов вычетов

Бинарные отношения

- **Бинарным отношением** ρ между множествами X и Y называется произвольное подмножество декартового произведения $X \times Y$, $\rho \subseteq X \times Y$.
- Если $X = Y$, то ρ есть бинарное отношение на множестве X.



- Бинарное отношение ρ на множестве X называется **отношением эквивалентности**, если выполняются три свойства:
  - **рефлексивность**: $x\rho x \ \forall x \in X$;
  - **симметричность**: $x\rho y \Rightarrow y\rho x \ \forall x, y \in X$;
  - **транзитивность**: $x\rho y, y\rho z \Rightarrow x\rho z \ \forall x, y, z \in X$.
- Множество X с заданным на нем отношением эквивалентности ρ разбивается на попарно непересекающиеся **классы эквивалентности**, где классом эквивалентности элемента x называется множество $\bar{x} = \{y \in X | x\rho y\}$.

Множества классов вычетов по модулю n

- Зададим на $\mathbb{Z}$ отношение эквивалентности ρ_n для некоторого $n \in \mathbb{N}$: $a\rho_n b \;\Leftrightarrow a \equiv b (\mathrm{mod}\, n)$, то есть a и b имеют одинаковый остаток от деления на n.
- Отношение ρ_n разбивает $\mathbb{Z}$ на классы эквивалентности, называемые **классами вычетов**.

$$\mathbb{Z} = \boxed{\begin{array}{c|c|c|c|c} \bar{0} & \bar{1} & \bar{2} & \dots & \overline{n-1} \end{array}}$$

- $\bar{a} = \{x \in \mathbb{Z} | x = kn + a, k \in \mathbb{Z}\}$ — класс вычетов a по модулю n.
- $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$ — множество классов вычетов по модулю n, $|\mathbb{Z}_n| = n$.
- **Пример** для $n = 4$:
  - $\bar{0} = \{\dots, -8, -4, 0, 4, 8, 12, \dots\}$;
  - $\bar{1} = \{\dots, -7, -3, 1, 5, 9, 13, \dots\}$;
  - $\bar{2} = \{\dots, -6, -2, 2, 6, 10, 14, \dots\}$;
  - $\bar{3} = \{\dots, -5, -1, 3, 7, 11, 15, \dots\}$.

Кольца классов вычетов по модулю n

- Зададим на $\mathbb{Z}_n$ две алгебраические операции:
  - **сложение**: $\bar{a} \oplus \bar{b} = \overline{a+b} \quad \forall\, \bar{a}, \bar{b} \in \mathbb{Z}_n$;
  - **умножение**: $\bar{a} \otimes \bar{b} = \overline{a \cdot b} \quad \forall\, \bar{a}, \bar{b} \in \mathbb{Z}_n$.
- Структура $(\mathbb{Z}_n;\ \oplus;\ \otimes)$ является коммутативным кольцом с единицей, называемым **кольцом классов вычетов по модулю n**.
  - $0_K = \bar{0}$ — нуль кольца;
  - $1_K = \bar{1}$ — единица кольца.
- $\mathbb{Z}_n^*$ — группа обратимых элементов кольца $\mathbb{Z}_n$.
- **Теорема.** Ненулевой элемент $\bar{a} \in \mathbb{Z}_n$ является обратимым тогда и только тогда, когда $\text{НОД}(a, n) = 1$.
- **Пример** для $n = 10$:
  - $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{8}, \bar{9}\}$;
  - $\mathbb{Z}_{10}^* = \{\bar{1}, \bar{3}, \bar{7}, \bar{9}\}$;
  - $\bar{1} \otimes \bar{1} = \overline{1 \cdot 1} = \bar{1}$, $\bar{3} \otimes \bar{7} = \overline{3 \cdot 7} = \overline{21} = \bar{1}$, $\bar{9} \otimes \bar{9} = \overline{9 \cdot 9} = \overline{81} = \bar{1}$.

Кольца многочленов

Многочлены над кольцом

- Пусть $(K;+;\cdot)$ – коммутативное кольцо с единицей.
- Любая конечная последовательность элементов кольца K вида $a=(a_0,a_1,\dots,a_n)$ называется **многочленом над кольцом $\boldsymbol{K}$**:
  - если $a_n\neq 0$, то a является многочленом степени n, $\deg(a)=n$, а a_n называется старшим коэффициентом многочлена a;
  - если $a_n=1$, то a называется нормированным многочленом;
  - многочлен вида $a=(a_0)$ называется константой.
- **Пример** для $K=\mathbb{Z}_{12}$:
  - $a=\left(\overline{2},\overline{5},\overline{0},\overline{11},\overline{2},\overline{3}\right)$ – многочлен степени 5;
  - $b=\left(\overline{3},\overline{7},\overline{1}\right)$ – нормированный многочлен степени 2;
  - $c=\left(\overline{5}\right)$ – многочлен-константа.

Операции над многочленами

- Пусть $a = (a_0, a_1, \dots, a_m)$, $b = (b_0, b_1, \dots, b_n)$, $m \le n$,
  - **сложение:** $a \oplus b = c$, $c = (c_0, c_1, \dots, c_n) = (a_0 + b_0, a_1 + b_1, \dots, a_m + b_m, b_{m+1}, \dots, b_n)$.
  - **умножение:** $a \otimes b = c$, $c = (c_0, c_1, \dots, c_{m+n})$, где $c_i = \sum_{j=0}^{i} a_j \cdot b_{i-j}$, $i = \overline{0, m+n}$.
- Введем многочлен первой степени $X = (0_K, 1_K) = (0, 1)$:
  - $X^0 = (1)$, $X^1 = (0, 1)$, $X^2 = (0, 0,1)$, $X^3 = (0, 0,0,1)$, …, $X^m = (0, 0, \dots, 0,1)$,
  - $a = (a_0, a_1, \dots, a_m)$= $(a_0) \oplus (0, a_1) \oplus \dots \oplus (0, 0, \dots, a_m)$= $a_0 \oplus a_1 \otimes \mathrm{X} \oplus a_2 \otimes X^2 \oplus \dots \oplus a_m \otimes X^m$.
- Множество всевозможных многочленов над кольцом K с заданными на нем операциями сложения и умножения многочленов является коммутативным кольцом с единицей и обозначается $K[X]$.
- **Пример**:
  - Кольцо многочленов над кольцом классов вычетов $\mathbb{Z}_n[X]$.

Пример сложения многочленов в кольце $\mathbb{Z}_{12}[X]$

- Пусть $a = (\bar{2}, \bar{5}, \bar{3})$, $\deg(a) = 2$, $a = (\bar{3}, \bar{0}, \bar{2}, \bar{1}, \bar{7})$, $\deg(b) = 4$.
  - $a \oplus b = c = (c_0, c_1, c_2, c_3, c_4)$, $\deg(c) = \max(\deg(a), \deg(b)) = 4$
  - $c_0 = a_0 + b_0 = \bar{2} + \bar{3} = \bar{5}$;
  - $c_1 = a_1 + b_1 = \bar{5} + \bar{0} = \bar{5}$;
  - $c_2 = a_2 + b_2 = \bar{3} + \bar{2} = \bar{5}$;
  - $c_3 = b_3 = \bar{1}$;
  - $c_4 = b_4 = \bar{7}$;
  - $c = (\bar{5}, \bar{5}, \bar{5}, \bar{1}, \bar{7})$.

Пример умножения многочленов в кольце $\mathbb{Z}_{12}[X]$

- Пусть $a = (\bar{2}, \bar{5}, \bar{3}\,)$, $\deg(a) = 2$, $a = (\bar{3}, \bar{0}, \bar{2}, \bar{1}, \bar{7})$, $\deg(b) = 4$.
  - $a \otimes b = c = (c_0, c_1, c_2, c_3, c_4, c_5, c_6)$, $\deg(c) = \deg(a) + \deg(b) = 6$;
  - $c_0 = a_0 \cdot b_0 = \bar{2} \cdot \bar{3} = \bar{6}$;
  - $c_1 = a_0 \cdot b_1 + a_1 \cdot b_0 = \bar{2} \cdot \bar{0} + \bar{5} \cdot \bar{3} = \bar{3}$;
  - $c_2 = a_0 \cdot b_2 + a_1 \cdot b_1 + a_2 \cdot b_0 = \bar{2} \cdot \bar{2} + \bar{5} \cdot \bar{0} + \bar{3} \cdot \bar{3} = \bar{1}$;
  - $c_3 = a_0 \cdot b_3 + a_1 \cdot b_2 + a_2 \cdot b_1 = \bar{2} \cdot \bar{1} + \bar{5} \cdot \bar{2} + \bar{3} \cdot \bar{0} = \bar{0}$;
  - $c_4 = a_0 \cdot b_4 + a_1 \cdot b_3 + a_2 \cdot b_2 = \bar{2} \cdot \bar{7} + \bar{5} \cdot \bar{1} + \bar{3} \cdot \bar{2} = \bar{1}$;
  - $c_5 = a_1 \cdot b_4 + a_2 \cdot b_3 = \bar{5} \cdot \bar{7} + \bar{3} \cdot \bar{1} = \bar{2}$;
  - $c_6 = a_2 \cdot b_4 = \bar{3} \cdot \bar{7} = \bar{9}$;
  - $c = (\bar{6}, \bar{3}, \bar{1}, \bar{0}, \bar{1}, \bar{2}, \bar{9})$.

Свойства многочленов над кольцом

- Собственным делителем многочлена $u \in K[X]$ называется многочлен $v \in K[X]$, такой, что $\deg(v) < \deg(u)$ и $u = q \cdot v$, $q \in K[X]$.
- Многочлен $p \in K[X]$ называется **неприводимым многочленом**, если он не имеет собственных делителей и $\deg(p) > 0$.

На основе бесконечного кольца многочленов $K[X]$ может быть построено бесконечное или конечное ***кольцо многочленных вычетов*** *аналогично тому, как строится кольцо классов вычетов на основе кольца целых чисел.*

Спасибо за внимание!

Евсютин Олег Олегович
Заведующий кафедрой информационной безопасности киберфизических систем
Канд. техн. наук, доцент

+7 923 403 09 21
oevsyutin@hse.ru