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

Кафедра информационной безопасности киберфизических систем

Москва 2024

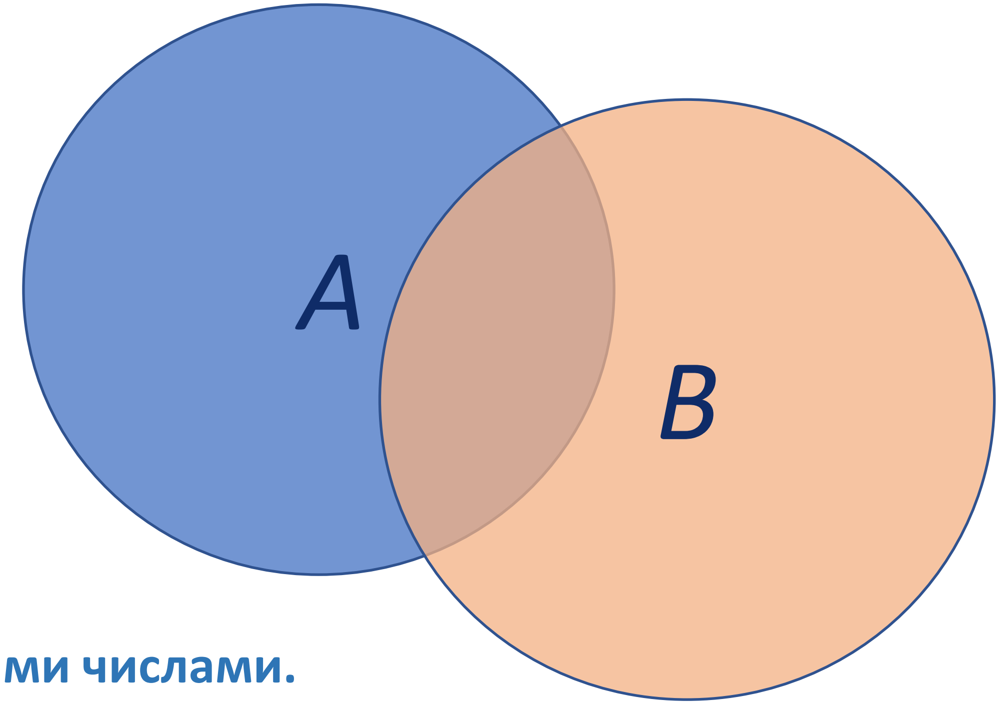
Криптографические методы защиты информации

Алгебраические структуры, группы, подгруппы

Алгебраические структуры

Множества

- **Множество** — это совокупность элементов, объединенных неким общим признаком.
- Числовые множества:
  - множество натуральных чисел $\mathbb{N}$,
  - множество целых чисел $\mathbb{Z}$,
  - множество рациональных чисел $\mathbb{Q}$,
  - множество действительных чисел $\mathbb{R}$,
  - множество комплексных чисел $\mathbb{C}$.



Криптографические алгоритмы оперируют целыми числами.

Алгебраические операции

- На множестве X задана **алгебраическая операция** $*$, если любой упорядоченной паре элементов $x, y \in X$ поставлен в соответствие однозначно определенный элемент $z \in X$, который обозначается как $z = x * y$.
- Множество X с заданной на нем алгебраической операцией $*$ называется **алгебраической структурой** и обозначается $(X;*)$.

- **Примеры алгебраических структур:**
  - $(\mathbb{Z};+)$: алгебраическая структура.
  - $(\mathbb{Z};:)$: не алгебраическая структура.
  - $X = \{a, b, c\}$

$*$	a	b	c
a	a	c	a
b	b	a	a
c	c	b	a

Свойства алгебраических операций

- **Ассоциативность:**

  $\forall\, x, y, z \in X \;\Rightarrow x * (y * z) = (x * y) * z.$

- **Существование нейтрального элемента:**

  $\exists!\, e$ такой, что $\forall x \in X \Rightarrow x * e = e * x = x.$

- **Существование обратимых элементов** (при наличии нейтрального элемента):

  $x, y \in X$ — взаимно обратные элементы, если $x * y = y * x = e$, тогда $y = x^{-1}$.

- **Коммутативность:**

  $\forall\, x, y \in X \;\Rightarrow x * y = y * x.$

- **Свойство квазигруппы:**

  $\forall\, a, b \in X$ однозначно разрешимы уравнения $a * x = b$ и $y * a = b$.

Типы алгебраических структур

- **Полугруппа:**
  - ассоциативность.
- **Моноид:**
  - ассоциативность;
  - наличие нейтрального элемента.
- **Квазигруппа:**
  - свойство квазигруппы.

Группы и подгруппы

Группы

- Алгебраическая структура $(G;\cdot)$ является **группой**, если она обладает следующими свойствами:
  - ассоциативность;
  - существование нейтрального элемента, называемого единицей группы 1_G;
  - обратимость всех элементов.
- Если групповая операция *коммутативна*, группа называется **абелевой**.

- Формы записи группы:
  - **мультипликативная**: $(G;\cdot),\ a\cdot a^{-1}=1.$
  - **аддитивная**: $(G;\ +),\ a+(-a)=0.$

Подгруппы

- Подмножество H группы G называется **подгруппой** группы G, если H само является группой относительно той же операции, что и G.
- Обозначение: $H \leq G$ или $H < G$.

- **Критерий подгруппы**:

  $H \leq G$ тогда и только тогда, когда $\forall\, x, y \in H \Rightarrow xy^{-1} \in H$.

- **Примеры:**
  - $(\mathbb{Z}; +)$ — группа.
  - $A \subset \mathbb{Z}$ — множество четных целых чисел, является подмножеством $\mathbb{Z}$, является подгруппой $(\mathbb{Z}; +)$.
  - $B \subset \mathbb{Z}$ — множество нечетных целых чисел, является подмножеством $\mathbb{Z}$, **не является подгруппой** $(\mathbb{Z}; +)$.

Циклические группы

Целочисленные степени и целочисленные кратные элементов группы

- Пусть $(G;\cdot)$ — некоторая группа и $g \in G$. Для любого $n \in \mathbb{Z}$ целочисленной степенью элемента g называется элемент $g^n \in G$:

$$g^n = \begin{cases} \underbrace{g \cdot g \dots \cdot g}_{n}, & \text{если } n > 0, \\ \underbrace{g^{-1} \cdot g^{-1} \dots \cdot g^{-1}}_{|n|}, & \text{если } n < 0, \\ 1_G, & \text{если } n = 0. \end{cases}$$

- Свойства целочисленных степеней:
  - $\forall\, m, n \in \mathbb{Z} \Rightarrow g^m \cdot g^n = g^{m+n}$;
  - $\forall\, m, n \in \mathbb{Z} \Rightarrow (g^m)^n = g^{mn}$.

- Пусть $(G;+)$ — некоторая группа и $g \in G$. Для любого $n \in \mathbb{Z}$ целочисленным кратным элемента g называется элемент $ng \in G$:

$$ng = \begin{cases} \underbrace{g + g + \dots + g}_{n}, & \text{если } n > 0, \\ \underbrace{(-g) + (-g) + \dots + (-g)}_{|n|}, & \text{если } n < 0, \\ 0_G, & \text{если } n = 0. \end{cases}$$

- Свойства целочисленных кратных:
  - $\forall\, m, n \in \mathbb{Z} \Rightarrow mg + ng = (m+n)g$;
  - $\forall\, m, n \in \mathbb{Z} \Longrightarrow n(mg) = (nm)g$.

Целочисленные степени и целочисленные кратные элементов группы

- Пусть $(G; \cdot)$ — некоторая группа и $g \in G$. Обозначим множество всевозможных целочисленных степеней элемента $g \in G$ как $\langle g \rangle = \{\dots, g^{-1}, g^0 = 1_G, g, g^2, \dots\}$.
- Пусть $(G; +)$ — некоторая группа и $g \in G$. Обозначим множество всевозможных целочисленных кратных элемента $g \in G$ как $\langle g \rangle = \{\dots, -g, 0g = 0_G, g, 2g, \dots\}$.

- $\langle g \rangle$ — подгруппа группы G, **порожденная** элементом $g \in G$.
- Элемент $g \in G$ — **образующий** подгруппы $\langle g \rangle$.

Конечные циклические группы

- Группа G называется **циклической группой**, если $G = \langle g \rangle$ для некоторого $g \in G$, который называется образующим циклической группы G.
- Виды циклических групп:
  - **бесконечные**: все целочисленные степени образующего элемента g в циклической группе $\langle g \rangle$ различны;
  - **конечные**: $g^m = g^n$ для некоторых целых чисел $m \neq n$.
- **Порядком** элемента $g \in G$ называется наименьшее натуральное число k такое, что $g^k = 1_G$, $O(g) = k$.
- Если $O(g) = k$, то $G = \langle g \rangle$ — это конечная циклическая группа порядка k, причем $|G| = O(g) = k$.
- Пусть G — некоторая конечная группа и $g \in G$, тогда $\langle g \rangle \leq G$ — конечная циклическая подгруппа, порожденная элементом g.

Конечные циклические группы имеют криптографическое приложение.

Примеры циклических групп

- **Бесконечные** циклические группы:

  — $(\mathbb{Z}; +) = \langle 1 \rangle$.

- **Конечные** циклические группы:

  — $(\mathbb{Z}^*; \cdot) = (\{-1, 1\}; \cdot) = \langle -1 \rangle$.

  — $G = \left\langle A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \right\rangle = \{1_G, A, A^2, A^3\}$,

  $$A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, A^2 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, A^3 = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, A^4 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = 1_G.$$

Свойства конечных циклических групп и подгрупп

- **Теорема Лагранжа**. Пусть G — конечная группа порядка n. Если $H \leq G$ и $|H| = k$, то $n = ks$ для некоторого $s \in \mathbb{N}$.
- **Следствие из теоремы Лагранжа**. Если G — конечная группа порядка n, то $g^n = 1_G \; \forall g \in G$.
- **Обратная теорема**. Пусть G — конечная циклическая группа и $|G| = n$. Если d есть делитель n, то существует и единственная подгруппа H группы G такая, что $|H| = d$.
- **Теорема об образующих элементах.** Пусть $G = \langle g \rangle$ — конечная циклическая группа, порожденная своим элементом g, и $|G| = n$. Элемент $g^k \in G$ является образующим группы G тогда и только тогда, когда выполняется условие $\text{НОД}(k, n) = 1$.
- **Теорема о подгруппе конечной циклической группы.** Любая подгруппа конечной циклической группы G является циклической группой.

Спасибо за внимание!

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

+7 923 403 09 21
oevsyutin@hse.ru