

# Элементы криптографического анализа

Автор курса: Тимонина Елена Евгеньевна  
Составитель: Смирнов Дмитрий Константинович

2022 г.

# Оглавление

1	Введение	1
2	Определение шифра. Простейшие примеры.	2
2.1	Что такое подстановка? . . . . .	2
2.2	Что такое группа, и почему множество $S_m$ из примера 2.1 образует группу? . . . . .	2
2.3	Почему группа $S_n$ из примера 2.2 является симметрической?	3
2.4	Что такое кольцо? Что такое кольцо вычетов по модулю $m$ ?	3
2.5	Какую алгебраическую структуру представляет собой кольцо $\mathbb{Z}_m$ при $m = 2$ ? . . . . .	4

Лекция 1

Введение

## Лекция 2

# Определение шифра. Простейшие примеры.

### 2.1 Что такое подстановка?

Подстановка — это взаимно однозначная функция, которая переводит буквы алфавита в буквы того же самого алфавита.

### 2.2 Что такое группа, и почему множество $S_m$ из примера 2.1 образует группу?

Множество  $G \neq \emptyset$  с бинарной операцией " $\circ$ ", называется группой, если выполнены условия:

1.  $\forall a, b \in G \quad a \circ b \in G$ ;
2.  $\forall a, b, c \in G \quad a \circ (b \circ c) = (a \circ b) \circ c$ ;
3.  $\exists e \in G: \forall a \in G \quad e \circ a = a \circ e = a$ ;
4.  $\forall a \in G \quad \exists b \in G: a \circ b = b \circ a = e$

Множество  $S_m$  вводится как множество всех подстановок на конечном алфавите  $A = \{a_1, \dots, a_m\}$ . Проверим выполнение аксиом группы:

1. Подстановка  $k \in S_m$  — отображение  $k: A \rightarrow A$ .  $\forall k_1, k_2 \in S_m$  рассмотрим суперпозицию  $k_1 \circ k_2$ . Так как  $k_1 \circ k_2: A \rightarrow A \rightarrow A$ , то  $k_1 \circ k_2 \in S_m$  и первая аксиома верна.

2.  $\forall k_1, k_2, k_3 \in S_m \quad k_1 \circ (k_2 \circ k_3) = k_1 \circ k_2(k_3(a)) = k_1(k_2(k_3(a))) = k_1(k_2(a)) \circ k_3(a) = (k_1 \circ k_2) \circ k_3$ .

3. Поскольку  $S_m$  — множество всех подстановок, то найдётся тождественная подстановка:  $\exists e \in S_m: \forall a \in A \quad e(a) = a$ . Тогда  $\forall k \in S_m$  верно

### 2.3. Почему группа $S_N$ из примера 2.2 является симметрической? 3

$$e \circ k = e(k(a)) = k(a) = k(e(a)) = k \circ e.$$

4. Так как подстановка – взаимно однозначная функция, то  $\forall k \in S_m$  существует обратная функция:  $\exists k^{-1}: A \rightarrow A \Rightarrow k^{-1} \in S_m$ , для которой будет выполнено равенство  $k \circ k^{-1} = k(k^{-1}(a)) = k^{-1}(k(a)) = k^{-1} \circ k$ . При этом,  $\forall a \in A \quad k^{-1}(k(a)) = a = e(a)$ .

Выполнены все аксиомы группы, следовательно  $S_m$  – группа.

### 2.3 Почему группа $S_n$ из примера 2.2 является симметрической?

Симметрической группой  $n$ -го порядка называется множество  $S(X)$  всех биективных отображений  $f: X \rightarrow X$ , где  $X$  – конечное множество из  $n$  элементов. Группа  $S_n$  в примере 2.2 определяется как группа подстановок на множестве  $X = \{1, \dots, n\}$ . Подстановка – это биективное отображение,  $X$  – конечное множество из  $n$  элементов. Следовательно, по определению, группа  $S_n$  является симметрической.

### 2.4 Что такое кольцо? Что такое кольцо вычетов по модулю $m$ ?

Множество  $K$  называется кольцом, если в  $K$  определены две операции “+” (сложение) и “·” (умножение) и выполняются следующие условия  $\forall a, b, c \in K$ :

1.  $a + b \in K, a \cdot b \in K$ ;
2.  $a + (b + c) = (a + b) + c, a(bc) = (ab)c$ ;
3.  $a + b = b + a$ ;
4.  $(a + b)c = ac + bc$ ;
5.  $\exists 0 \in K: a + 0 = a$ .

Кольцом вычетов по модулю  $m$  называется такое кольцо  $\mathbb{Z}/m = \{C_0, C_1, \dots, C_{m-1}\}$  ( $C_r$  – смежный класс вычетов по модулю  $m$ ), в котором операции сложения и умножения определяются следующими правилами:

1.  $C_a + C_b = C_r$ , где  $r \equiv (a + b) \pmod{m}$ ;
2.  $C_a C_b = C_r$ , где  $r \equiv ab \pmod{m}$

То есть,  $C_a + C_b$  – это класс, в который входит число  $a + b$ , а  $C_a C_b$  – класс, в который входит число  $ab$ .

2.5 Какую алгебраическую структуру представляет собой кольцо  $\mathbb{Z}_m$  при  $m = 2$ ?

Теорема 1. Если  $p$  – простое число и  $p \geq 2$ , то  $\mathbb{Z}_m$  – поле характеристики  $p$ .

По теореме 1 кольцо  $\mathbb{Z}_2$  является полем характеристики 2.