

# 1 Криптография

## 1.1

Постановка задачи. Простейшие криптосистемы. Сдвиг и аффинное преобразование. Частотный анализ. Биграммы.

## 1.2

## 1.3

Вычет  $a$  называется обратимым по модулю  $N$ , если существует вычет  $x$  такой, что

$$ax \equiv 1 \pmod{N}$$

Вычет является обратимым тогда и только тогда, когда он взаимно прост с модулем ( $\text{НОД}(a, N) = 1$ ).

Теорема Ферма утверждает, что если  $p$  - простое число и  $a$  - целое число, не делящееся на  $p$ , то

$$a^{p-1} \equiv 1 \pmod{p};$$

Функция Эйлера  $\varphi(n)$  — мультипликативная арифметическая функция, равная количеству натуральных чисел, меньших  $n$  и взаимно простых с ним. При этом полагают по определению, что число 1 взаимно просто со всеми натуральными числами, и  $\varphi(1) = 1$ . Пример:  $\varphi(24) = 8$ : 1, 5, 7, 11, 13, 17, 19, 23.

Теорема Эйлера гласит, что если  $a$  и  $m$  взаимно просты, то  $a^{\varphi(m)} \equiv 1 \pmod{m}$ . Малая теорема Ферма является следствием теоремы Эйлера.

Китайская теорема об остатках. Пусть  $n_1, n_2, \dots, n_k$  - некоторые попарно взаимно простые числа, а  $r_1, r_2, \dots, r_k$  - некоторые целые числа. Тогда существует такое целое число  $M$ , что оно будет решением системы уравнений:

$$\begin{cases} M \equiv r_1 \pmod{n_1} \\ M \equiv r_2 \pmod{n_2} \\ \quad \quad \quad + . \\ M \equiv r_k \pmod{n_k} \end{cases}$$

Причём это решение единственно по модулю  $n_1 \cdot n_2 \cdot \dots \cdot n_k$