1 Криптография

1.1

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

1.2

1.3

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

$$ax \equiv 1 \ (mod \ N)$$

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

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

$$a^{p-1} \equiv 1 \ (mod \ p);$$

Функция Эйлера $\varphi(n)$ — мультипликативная арифметическая функция, равная количеству натуральных чисел, меньших n 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 $a^{\varphi(m)} \equiv 1 \ (mod \ m)$. Малая теорема Ферма является следствием теореми Эйлера.

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

$$\begin{cases} M \equiv r_1 \ (mod \ n_1) \\ M \equiv r_2 \ (mod \ n_2) \\ \qquad\qquad\qquad + . \\ M \equiv r_k \ (mod \ n_k) \end{cases}$$

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

Метод повторного возведения в квадрат. Дальше идут мои личные объяснения. Пусть нам нужно возвести чилсло a в степень n. Представим n как сумму степеней двойки. Пример: $51 = 32 + 16 + 2 + 1$. Мы будем вычислять a^n циклом из n итераций. На итерации $i = \overline{0, n-1}$ будет вычисляться a^{2^i}. Причём это будет сделано с помощью уже полученного результата ($a^{2^i} = (a^{2^{i-1}})^2$). Переменная результата будет инициализирована единицей и будет домножаться на a^{2^i} каждый раз, когда i слева бит числа n не равен нулю. Таким образом, число мы возведём число в степень n примерно за $\log_2 n$ операций.