1 Криптография

1.1

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

1.2

1.3

Необходимые сведения из теории чисел. Обратимость вычета по данному модулю. Алгоритм нахождения обратного элемента. Малая теорема Ферма. функция Эйлера и теорема Эйлера. Китайская теорема об остатках. Возведение в степень методом повторного возведения в квадрат.

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:

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

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 на предыдущей итерации 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, мы возведём число в степень n примерно за $\log_2 n$ операций.

1.4

Группа — множество, на котором определена ассоциативная бинарная операция, причём для этой операции имеется нейтральный элемент (аналог единицы для умножения), и каждый элемент множества имеет обратный.

Конечная группа - группа с ограниченным числом элементов. Пример конечной группы - вычеты по модулю n.

Пусть G - конечная группа, $m = |G|$ (порядок группы, количество элементов). Теорема: $\forall g \in G : g^m = e$.

Порядок элемента g (записывают, как $ord(g)$) - наименьшее натуральное s такое, что $g^s = e$. Считают, что $ord(g) = \infty$, если такого s не существует.

Группа G называется циклической, если $\exists g \in G : G = \{g^k, k \in \mathbb{Z}\}$. Пример циклической группы - вычеты по модулю n с операцией сложения.

1.5

Задача дискретного логарифмирования и система Диффи-Хеллмана обмена ключами.

Задача дискретного логарфмирования. Пусть G - конечная группа и $g \in G$. Задача: для $h \in \{g^s, s \in \mathbb{Z}\}$ найти натуральное k такое, что $h = g^k$. k - дискретный логарифм элемента h по основанию g. Замечание: такое k - не единственное, так как $g^m = e \implies g^k = g^{m+k} = g^{2m+k} = ... = g^{nm+k}, n \in \mathbb{N}$. Основная фишечка: возведение в степень быстрое, а нахождение логарифма - долгое.

Система Диффи-Хеллмана (1976). Все знаю конечную группу G и элемент g достаточно большого порядка. $G = (\mathbb{Z}_p \backslash \{0\}, \times)$. Важно, что $|G| = p - 1$, p - большое простое. Эта группа циклическая. Что происходит? Алиса фиксирует своё некоторое натуральное число a, держит его в секрете, но вычисляет и выкладывает значение g^a. После этого любые 2 участника сформируют у себя общее число $g^{ab} = (g^a)^b = (g^b)^a$.

1.6

1.7

1.8

1.9

1.10

Проверка числа на простоту и проблема факторизации. Решето Эратосфена. Псевдопростые числа и числа Кармайкла. Метод Поклингтона. $(p-1)$ метод Полларда.

Псевдопростые числа и числа Кармайкла. Если p - простое, то $\forall a < p : a^{p-1} \equiv 1 \ (mod\ p)$ (малая теорема Ферма). Метод Кармайкла позволяет точно сказать, является ли число непростым, но не позволяет утверждать обратного. Если $\exists a < p$ такое, что $a^{p-1} \not\equiv 1 \ (mod\ p)$, то число p - не простое. Если для данного p $\forall a < p : a^{p-1} \equiv 1 \ (mod\ p)$, но при этом само число не являетя простым, то его называют числом Кармайкла (пример: 561).

Метод Поклингтона проверки числа на простоту. Предположим, что у числа $n-1$ есть простой делитель $p > \sqrt{n} - 1$. Если $\exists a$ (целое) такое, что выполены 2 условия:

1. $a^{n-1} \equiv 1 \ (mod\ n)$
2. $(a^{\frac{n-1}{p}} - 1, n) = 1$

То число n - простое.

$(p-1)$-метод Полларда разложения числа на множители. Выберем число m, которое делится на все натуральные числа $\leq c$ (Пример: $c!$). Возьмём q такое, что $2 \leq q \leq n-2$. Вычислим $q^m \ (mod\ n)$. Если $q^m \neq 1 \ (mod\ n)$, продолжаем. Вычисляем $d = \text{НОД}(q^m - 1, n)$. Если $d \neq 1$, то $n = d \cdot \frac{n}{d}$.