1 Криптография

1.1

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

Шифр Цезаря. Есть алфавит из N упорядоченных символов (у каждого символа есть свой номер от 0 до $N-1$). Мы берём произвольное число a от 1 до $N-1$ (сдвиг на 0 не имеет смысла) и сдвигаем все буквы на a позиций вправо. Таким образом, новый номер символа, в начальной строке стоящего под номером n, станет равен $(n+a)\ mod\ N$.

Афинное преобразование. Есть алфавит из N упорядоченных символов (у каждого символа есть свой номер от 0 до $N-1$). Здесь для зашифровки нужно 2 параметра. Назовём из k и b. Мы применяем линейную функцию к номеру каждого символа. Новый номер элемента, стоящего в начальной строке на позиции n будет равен $(n \cdot k + b)\ mod\ N$.

Частотный анализ позволяет взломать некоторые алгоритмы шифрования. Например - афинное преобразование. Частотный анализ подрузмевает, что взломщик знает частоту встречаемости каких-то символов в данном типе текстов или языке. Он может сопоставить самый часто встречающийся символ в языке с самым частым символом в тексте, который он хочет взломать. Зная 2 самых частых символа в языке, скорее всего можно взломать систему афинного преобразования (k, b - две неизвестные, дано два уравнения).

1.2

Ключ шифрования и ключ дешифрования. Классические криптосистемы и системы с открытым ключом.

Ключ шифрования (K_E, encryption key) - набор параметров, позволяющий зашифровать текст в данной криптосистеме. Ключ дешифрования (K_D, decryption key) - набор параметров, позволяющий дешифровать текст в данной криптосистеме.

В классических криптосистемах по K_E легко получить K_D (примеры: шифр Цезаря, афинное преобразование). В системах с открытым ключом это сделать теоретически возможно, но очень сложно (высокая вычислительная сложность).

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:

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

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 $g^{ab} = (g^a)^b = (g^b)^a$. На деле тут нет передачи информации.

1.6

Системы Мэсси-Омура и Эль-Гамаля.

Система Мэсси-Омура. Все знают большую группу G порядка m. Если A хочет передать B сообщение $t \in G$, он выбирает $a \in \mathbb{N} : \text{НОД}(a, n) = 1$ и находит $d_a = a^{-1} \ (mod\ m)$. B делает то же самое (находит своё d_b). Затем происходит обмен сообщениями по следующей схеме:

1. A посылает B t^a.
2. B возвращает A $(t^a)^b$.
3. A посылает B $((t^a)^b)^{d_a} = t^b$.

Затем B расшифровывает сообщение: $(t^b)^{d_b} = t^{1+m \cdot n} = t \cdot (t^m)^n = t \cdot e^n = t$.

Система Эль-Гамаля (1983). Все знают группу G и $g \in G$ большого порядка. Каждый участник фиксирует своё a и сообщает всем g^a. Если другой участник хочет передать A своё сообщение $t \in G$, то он выбирает натуральное k и передаёт A пару $(g^k,\ t \cdot (g^a)^k)$. A дешифровывает сообщения по такой схеме: $t \cdot (g^a) \cdot (g^k)^{-a} = t \cdot g^{ak} \cdot g^{-ak} = t$. Замечание: рекомендуется выбирать своё k для разных букв слова t (автору конспекта пока непонятно, зачем)

1.7

Система RSA.

Система RSA. Выбираем большие простые числа p и q (больше 100 знаков). Эти числа держатся в секрете. Вычисляем $n_A = p \cdot q$, n общеизвестно. Находим $\varphi(n_A) = (p-1) \cdot (q-1)$ (см. функция Эйлера). Находим случайное $0 < a < n_A$ такое, что $\text{НОД}(a, \varphi(n_A)) = 1$ и находим $d_a = a^{-1} \ (mod\ \varphi(n))$. $K_D = (n_A, a)$ - публичен, $K_E = (n_a, d_a)$ - держится в секрете. Если B хочет передать A сообщение $t \in \mathbb{Z}_{n_a}$, он передаёт t^a. A дешифрует сообщение: $(t^a)^{d_A} = t \ (mod\ n_A)$. Почему? Смотрите ниже

$$t^{a \cdot d_A} \ (mod\ n_A) = t^{1+\varphi(n_A) \cdot s} \ (mod\ n_A) = t \cdot (t^{\varphi(n_A)})^s \ (mod\ n_A) = t \cdot 1^S \ (mod\ n_A) = t \ (mod\ n_A)$$

1.8

Понятие электронной подписи. Электронная подпись по Эль-Гамалю и RSA.

По вики: электронная подпись - реквизит электронного документа, полученный в результате криптографического преобразования информации с использованием закрытого ключа подписи и позволяющий проверить отсутствие искажения информации в электронном документе с момента формирования подписи (целостность), принадлежность подписи владельцу сертификата ключа подписи (авторство), а в случае успешной проверки подтвердить факт подписания электронного документа (неотказуемость).

Попроще: электронная подпись - штука, позволяющая убедиться, что отправленное сообщение не было искажено и что его отправил какой-то конкретный участник системы.

Электронная подпись по Эль-Гамалю. Все знают большое простое число p и $g \in \mathbb{Z}_p$. Каждый пользователь выбирает своё натуральное a и держит его в секрете, но сообщает всем g^a. У A на сайте размещено h_A (имя). Чтобы убедить B, что информация приходит от A, A выбирает k такое, что $1 < k < p-1$ и $\text{НОД}(k, p-1) = 1$. Далее он находит $k^{-1} \ (mod\ p-1)$ и вычисляет 2 числа: g^k и $s = (h_A - a \cdot g^k) \cdot (k^{-1} \ (mod\ p-1))$. Теперь A передаёт B пару $(g^k,\ s)$. Получив это, B вычисляет $(g^a)^{g^k} \cdot (g^k)^s = g^{g^k a + ks} = g^{h_A}$. Magic! Затем всё просто: B вычисляет g^{h_A} и проверяет, совпадает оно с полученным значением.

Электронная подпись по RSA. ???.

1.9

Задача о рюкзаке и рюкзачная криптосистема.

Задача о рюкзаке. Дан набор $A = \{a_1, \ldots, a_n\}$ из n различных положительных чисел и целое положительное число s. Необходимо найти набор таких a_i, чтобы в сумме они давали ровно s.

Быстровозрастающий набор в задаче о рюкзаке - это такой набор, в котором каждый элемент больше суммы всех предыдущих ($\sum_{i=1}^{j-1} a_i < a_j$).

Рюкзачная криптосистема. Возьмём быстрорастущий набор A и вычислим сумму всех его элементов S. Теперь выберем модуль $m > S$. Затем необходимо выбрать число t, взаимно простое с m и обратный к нему элемент по данному модулю. Теперь мы сможем получить новый набор B, элементы которого будет задаваться по следующей формуле: $\forall i : b_i = t \cdot a_i \ (mod\ m)$. Все параметры системы, кроме набора B, являются секретными. Автор (администратор) системы выкладывает в общий доступ набор B, с помощью которого другие участники зашифровывают свои сообщения.

Как происходит зашифровка? Передаются двоичные слова, длина которых равна количеству элементов в наборе B. Зашифрованное сообщение будет в виде числа c, задающегося формулой $\sum_{i=0}^{n-1} b_i \cdot w_i$, где n - размер набора B, а w_i - i-ый слева бит двоичного слова, отсчёт начинается с нуля.

Как администратор системы расшифровывает сообщение? Он начинает вычислять число v по формуле: $v = t^{-1} \cdot c \ (mod\ m)$. И затем для этого числа находит решение задачи о рюкзаке для набора A. При этом вхождение/невхождение элемента из набора A он помечает 1 и 0 соответственно. Тогда он получает то двоичное число, которое ему хотел передать участник системы. Magic!

P.S. Эта криптосистема считается не слишком безопасной. Однажды некто предложил вариант взлома. Позже брешь прикрыли, став использовать тот же самый алгоритм 2 раза, но доверие уже пропало.

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 $n = d \cdot \frac{n}{d}$. Дальше по индукции раскладываем $\frac{n}{d}$.