Глоссарий основных терминов

Абелева группа(коммутативная группа) – группа по сложению, в которой групповая операция коммутативна: $a + b = b + a$.

Авторизация – это процедура разделения пользователей на группы с разными правами доступа.

Алгоритм быстрого возведения в степень – алгоритм быстрого вычисления целой степени натурального числа.

Алгоритм Евклида – алгоритм вычисления наибольшего общего делителя Н.О.Д двух целых чисел. Основан на реккурентной формуле

$$\text{Н.О.Д.}(a, b) = \text{Н.О.Д.}(b, a \bmod b),$$

где $a \bmod b$ – целый остаток от деления a на b.

Алгоритм Евклида обобщенный – алгоритм, кроме нахождения наибольшего общего делителя d двух целых чисел A и B, также находит целые x и y такие, что выполняется формула: $Ax + By = d$.

Алгоритм Шенкса-Тоннелли – полиномиальный алгоритм извлечения квадратного корня в конечном поле.

Аудит – это процедура записи действий всех пользователей по доступу к защищаемым данным.

Аутентификация – это процедура проверки идентификатора пользователя. При входе в информационную систему пользователь должен идентифицировать себя, т.е. отождествить себя с одним из зарегистрированных в системе пользователей. Для этого в самой распространенной системе парольной аутентификации пользователь вводит свои логин и пароль.

Блочный метод шифрования – способ шифрования, при котором текст разбивается на отдельные блоки фиксированной длины, каждый из который шифруется по-отдельности.

Вычет – класс эквивалентности, образованный целыми числами по отношению эквивалентности по модулю заданного натурального числа.

Группа – непустое множество элементов G, на котором определена операция умножения $\cdot$, удовлетворяющая следующим свойствам:

1. Операция – ассоциативна: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

2. Существует элемент e: $e \cdot a = a \cdot e = a$ для любого $a \in G$

3. Для любого $a \in G$ есть обратный элемент a^{-1}: $a \cdot a^{-1} = a^{-1} \cdot a = e$.

Доступность – это это свойство информации, обеспечивающее право легальных пользователей на неограниченный доступ к всем ресурсам информационной системы или их части.

Информационная безопасность – это состояние информационной системы, в котором угрозы нарушения конфиденциальности, целостности и доступности информации сведены к минимуму.

Квадратичный вычет – элемент кольца Z_n вычетов по модулю n, является квадратом другого элемента. Элемент, не являющийся квадратичным вычетом, называется квадратичным невычетом. Для простого n определить, является ли a квадратичным вычетом, можно с помощью символа Лежандра.

Ключ шифрования / расшифрования – секретный параметр шифрования, представляющий собой последовательность символов.

Кольцо (ассоциативное) – непустое множество элементов F, на котором определена операция сложения $+$ и операция умножения $\cdot$ так, что относительно операции $+$ множество F является абелевой группой, относительно умножения – полугруппой, и эти операции связаны законами дистрибутивности:

1. $a \cdot (b + c) = a \cdot b + a \cdot c$,

2. $(b + c) \cdot a = b \cdot a + c \cdot a$.

Кольцо отличается от поля тем, что не все элементы кольца имеют обратные по умножению.

Конфиденциальность – это свойство информации, обеспечивающее ее адресный доступ к пользователям информационных систем.

Критерий простоты AKS – детерминированный полиномиальный тест проверки простоты, открытый в 2004 году индийскими математиками Агравелой, Каялом и Саксеной. Этот тест явился решением крупной научной проблемы построения детерминированного полиномиального теста простоты, однако, с практической точки зрения он не слишком удобен,

так как его оценка достигает величины $O(L^{17})$, где L–длина тестируемого числа.

Метод пробных делений – метод факторизации натурального числа n, заключающийся в последовательном делении n на все натуральные числа от 2 до $\sqrt{n}$. Метод имеет временную сложность $O(exp(n/2))$.

Метод Полларда – метод факторизации натурального числа n, разработанный в 1974 году Джоном Поллардом, заключающийся в последовательном вычислении последовательности $x_{n+1} = x_n^2 - 1 \mod n$, $n = 0, 1, 2 \ldots$ и проверке условия Н.О.Д. $(n, |x_i - x_j|) \neq 1$ до тех пор, пока не будет оно не выполнится. Метод используется в модификации Флойда, в которой на шаге $i > 0$ проверяется условие Н.О.Д. $(n, |x_i - y_i|) \neq 1$, y_i равно последнему x_j, $j < i$, такому, что номер j является степенью 2. Метод имеет временную сложность $O(exp(n/4))$.

Перестановка – одно из криптографических преобразований электронного документа (криптографический примитив), используемый при блочном методе шифрования.

Поле – непустое множество элементов F, на котором определена операция сложения $+$ и операция умножения $\cdot$ так, что относительно операции $+$ множество F является абелевой группой, относительно умножения – группой, и эти операции связаны законами дистрибутивности:

1. $a \cdot (b + c) = a \cdot b + a \cdot c$,
2. $(b + c) \cdot a = b \cdot a + c \cdot a$.

Поля Галуа – конечные поля, названные по имени выдающего французского математика Эвариста Галуа (1811 – 1832), построившего теорию конечных полей (теория Галуа). Любое поле Галуа содержит p^k элементов, где p–простое число, называемое характеристикой поля, а $k \geq 1$–натуральное число, и обозначается $GF(p^k)$.

Полугруппа – непустое множество элементов, на котором определена операция умножения $\cdot$, удовлетворяющая следующим свойствам:

1. Операция – ассоциативна: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
2. Существует элемент e: $e \cdot a = a \cdot e = a$ для любого a

Порядок элемента a группы G – наименьшее число k такое, что $a^k = 1$. Обозначается $ord_G(a)$.

Поточный метод шифрования – способ шифрования, при котором текст шифруется посимвольно. Примером поточного метода шифрования являются RC4, разработанный в 1987 году Рональдом Ривестом.

Последовательность Фиббоначчи – числовая последовательность вида $\{1, 1, 2, 3, 5 \ldots\}$, образуемая по правилам: $a_0 = a_1 = 1;\ a_{n+2} = a_n + a_{n+1}$.

Примитивный корень конечного поля – элемент a конечного поля, среди целых степеней a^k которого встретятся все элементы этого поля (кроме нулевого).

Простое число – натуральное число, не имеющее других делителей, кроме 1 и самого себя.

Решето Аткина – оптимизированный алгоритм построения множества всех простых чисел, меньших некоторого положительного числа x.

Решето Эратосфена – алгоритм построения множества всех простых чисел, меньших некоторого положительного числа x путем последовательного вычеркивания всех кратных первого еще невычеркнутого элемента в исходном множестве, состоящем из всех натуральных чисел n, $2 \leq n \leq x$.

Сервисы информационной безопасности – это основные комплексы защитных средств, предназначенные для поддержки безопасности информационной системы. Основными сервисами являются аутентификация, авторизация и аудит.

Символ Лежандра – функция от натурального a и простого p:

$$\left(\frac{a}{p}\right) = \begin{cases} 1, \text{ если } (\exists\, x)\, x^2 \equiv a \bmod p, \\ -1, \text{ если не}(\exists\, x)\, x^2 \equiv a \bmod p, \\ 0, \text{ если } p \mid a. \end{cases}$$

Сложность алгоритма (временная) – верхняя граница времени работы алгоритма для всех входов заданной длины. Вместо времени работы обычно используется условное количество элементарных операций. Например, алгоритм сортировки массива методом пузырька имеет сложность $O(n^2)$, что означает, что для всех массивов длины n требуется не более, чем

$C \cdot n^2$ элементарных операций сравнения и перестановки элементов, C–константа, не зависящая от n.

Теорема Ферма (малая) – утверждение, доказанное выдающимся французским ученым Пьером Ферма (1601–1665) о том, что для любого натурального числа a и простого числа p, не сравнимых по умножению, выполняется формула

$$a^{p-1} \mod p = 1$$

Тест Миллера-Рабина – вероятностный тест проверки простоты натурального числа. Тест утверждает, что число n–составное, если найдется $2 \leq a < n$ такое, что $b = a^d \neq \pm 1 (\mathrm{mod}\ n)$, и последовательность $\{b_i : 1 \leq i \leq s-1\}$ не содержит $n-1$, где $n-1 = 2^s \cdot d$, d–нечетно, $b_0 = b$, $b_{i+1} = b_i^2 \mod n$. Элемент a, нарушающий хотя бы одно из этих условий, называется свидетелем простоты n. Если же среди k случайных чисел $2 \leq a < n$ все оказались свидетелями простоты, то n–простое с вероятностью ошибки менее 4^{-k}.

Тест Соловея — Штрассена – вероятностный тест проверки простоты натурального числа. Тест опирается на следующую теорему:

Если n — нечетное составное число, то количество целых чисел a, взаимно простых с n и меньших n, удовлетворяющих сравнению

$$a^{(n-1)/2} \equiv \binom{a}{n} \ (\mathrm{mod}\, n), \tag{1}$$

не превосходит $n/2$, (a/n)– символ Якоби.

Тест Поклингтона – тест простоты натурального числа, основанный на теореме Поклингтона.

Шифрование – преобразование, преобразующее электронный документ в нечитаемую последовательность символов для защиты файла от чтения людьми, не имеющими соответствующих прав доступа. Это преобразование зависит от *ключа шифрования.*

Угроза информационной безопасности – потенциально возможное событие, которое может привести к нанесению вреда информационной системе и хранящейся в ней информации.

Системы шифрования с открытым ключом – криптографические системы

Факторизация – процедура разложения целого числа в произведение простых сомножителей и их степеней.

DES (Data Encryption Standard) — симметричный алгоритм шифрования, разработанный фирмой IBM и утвержденный правительством США в 1977 году как официальный стандарт.

RSA – метод шифрования с открытым ключом, основанный на сложности задачи факторизации (разложений на множители) больших целых чисел. Криптостойкость RSA определяется длиной ключа, которая по криптографическим стандартам равна 1024, 2048 или 4096 бит.