Принципы построения функций, используемы в криптографических системах

Определение1: функция определяется двумя множествами X и Y и правилом, которое назначает каждому элементу из множества X один элемент из множества Y.

Множество X называется областью определения функции и множество Y - областью ее значений. Если элемент $x \in X$, то образом данного элемента является элемент из множества Y: $y = f(x)$, где $y \in Y$. Соответственно, прообразом y является элемент $x \in X$, для которого выполняется $y = f(x)$. Обычно записывают, что функция f, отобража-ющая элементы из множества X в множество У есть : X -> Y. Множество всех элементов из У, имеющих хотя бы один прообраз, называется образом функции a и обозначается Im(f)=Y.

Определение 2: функция называется однозначной (отображением один в один), если каждый элемент из множества Y является образом не более одного элемента из множества X. Пример – гипербола y=1/x

Определение 3: функция называется отображением в себя, если каждый элемент области значений Y есть образ по крайней мере одного элемента области определения.

Например, функция f: X -> Y есть отображение в себя, если множество всех образов совпадает с областью значений данной функции: Im(f) = Y. Пример-парабола $y=x^3-7x+6$

Определение 4: функция называется биекцией, если она является однозначной и Im(f) = Y .Пример-парабола $y=x^3$

Определение 5: если функция f является биекцией X в Y, то существует простой способ вычислить биекцию Y в X следующим образом: для каждого $y \in Y$ определяют значение функции g(y)=x, где $x \in X$ и f(x) = y.

Функция g, полученная из f, называется обратной функцией к f и обозначается $g=f^{-1}$.

Рассмотрим простой пример биективной функции и обратной к ней. Пусть множество X= { a, Ь, c, d, e} и множество Y= { 1, 2, 3, 4, 5 } . Зададим функцию f: X ->Y графически (рис. 2.1). Легко убедиться что данная функция биективная и что существует обратная к ней функция $g=f^{-1}$. Областью определения функции g является множество

f: X ->Y g: Y-> X

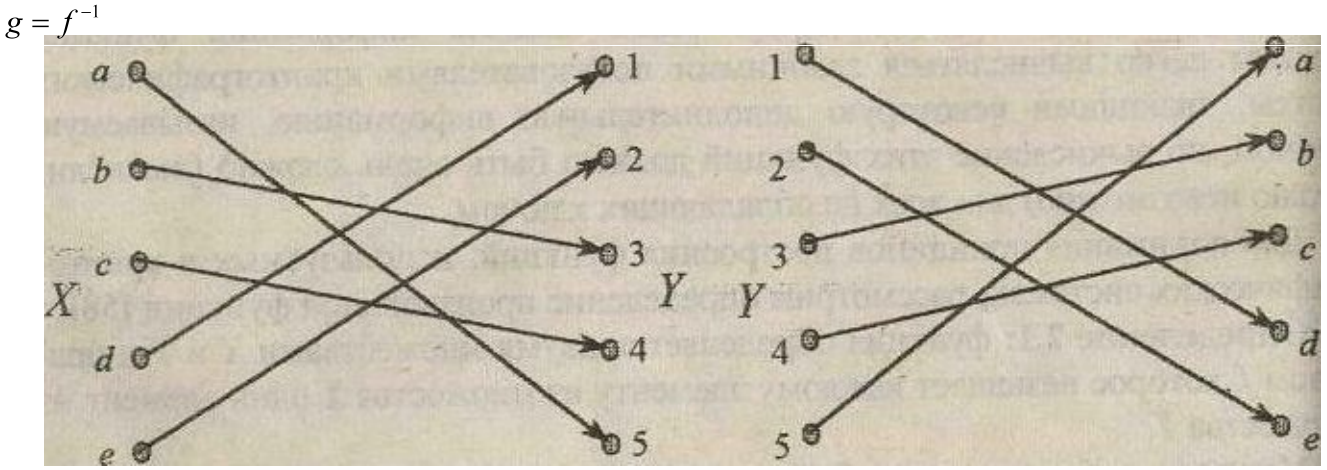

Рис. 1. Биективная функция f и обратная к ней $g=f^{-1}$

Существование обратной функции к функции шифрования является основой построения систем шифрования информации. Если биективную функцию использовать для шифрования сообщений из множества X в множество криптограмм У, то с помощью обратной функции можно однозначно дешифровать криптограммы в сообщения. Если функция шифрования не является биективной, то однозначное дешифрование невозможно (из криптограммы по обратному отображению восстанавливается несколько различных сообщений).

Среди биективных функций есть класс функций, наиболее часто используемый для построения симметричных криптографических систем защиты информации. Такие функции называются инволюциями и существуют при условии, что область определения X функции совпадает с областью ее изменения Y, т. е. X=Y = S.

Определение 6: пусть S есть конечное множество и функция f является биекцией, отображающей S в S (т. е. f : S ->S). Функция f называется инволюцией, если $f=f^{-1}$.

Из определения видно, что у инволюции совпадают не только область определения и область изменения функции, но и обратная функция с прямой функцией. Поэтому если множество сообщений совпадает с множеством криптограмм, то при использовании инволюции функция шифрования совпадает с функцией дешифрования, что очень удобно при построении систем шифрования информации. Следовательно, последовательное применение сначала функции шифрования, а затем функции дешифрования к произвольному сообщению $x \in S$ однозначно восстанавливает данное сообщение: f(f(x))=x

f: S->S

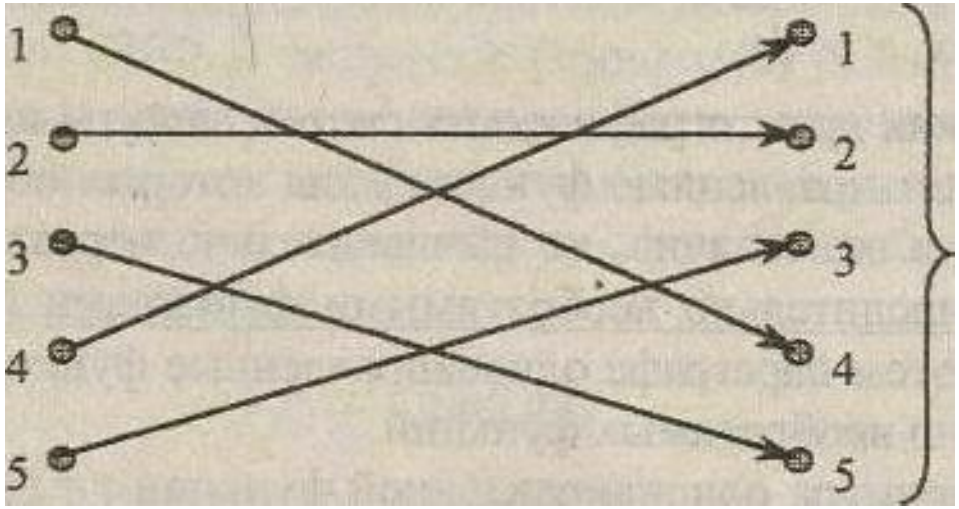

Рис. 2. Инволюция f для множества S = {1,2,3,4,5}

На рис. 2 показан простой пример инволюции f для множества S = { 1,2,3,4,5 }. Легко убедиться, что четное число последовательных применений инволюции f восстанавливает любой зашифрованный элемент x множества S. Пример – побитовая функция XOR (⊕), т. e.f(x)=x ⊕ *a*, где a=const, тогда f(f(x))=(x ⊕ *a*) ⊕ *a* = x

ОДНОНАПРАВЛЕННЫЕ ФУНКЦИИ

Особую роль в криптографии играют однонаправленные функции (ОНФ), которые в общем случае не являются биективными.

Определение7: однонаправленная функция есть такая функция f для которой для каждого x из области ее определения X вычислительно просто определить значение функции y = f(x), но практически для всех y из области Y функции, вычислительно невозможно отыскать любое x такое, что y =f(x).

Принципиальным условием однонаправленности функции является сложность (невозможность) вычисления обратного преобразования к ней. Обратное преобразование к ОНФ может существовать, но не являться функцией в смысле определения 1. Обратное преобразование может быть также неоднозначным, то есть практически для всех y из области значений Y функции невозможно отыскать единственное значение x такое, что y = f(x) . Неоднозначность обратного преобразования означает, что допустимых значений $x \in X$ может быть множество, и каждое из них удовлетворяет уравнению y = f(x).

Для выяснения неоднозначности обратного преобразования конкретной функции необходимо убедиться, что выполнение прямого и обратного преобразований не обеспечивает взаимно однозначного соответствия между элементами множеств X и Y. Примером существования неоднозначных обратных преобразований является функция y=x2 , для которой каждому образу $y \in Y$ (исключая y=0) соответствуют два отличающиеся друг от друга прообраза xi и xj :

$$x_i = \sqrt{y} \qquad x_j = -\sqrt{y}$$

Для построения криптографических систем зашиты информации чаще пользуются ОНФ, для которых обратное преобразование существует и однозначно, но вычислительно нереализуемо. Такие ОНФ называются вычислительно необратимыми функциями.

В качестве примера однонаправленной функции y = f(x) рассмотрим известную дискретную функцию дискретного возведения в степень $y=a^x \pmod p$, где x - целое число от 1 до p -1 включительно, а вычисление производится по модулю p, где p - очень большое простое число; a - целое число ($1 < a < p$) степени которого $a^1, a^2, \ldots a^{p-1}$, взятые по mod p , равняются в некотором порядке числам 1,2, ...,p -1. Такие значения *a* называются примитивными элементами. Напомним, что простым числом называется целое число, которое не делится ни на какие числа, кроме себя самого и единицы.

Например, при простом числе p = 7 можно выбрать примитивный элемент *a=3* , т.к. $a1 \pmod 7 = 3$, $a2 \pmod 7 = 2$, $a3 \pmod 7 = 6$, $a4 \pmod 7 = 4$, $a5 \pmod 7 = 5$, $a6 \pmod 7 = 1$

Арифметика вычетов

a≡b (mod n), если a = b+kn для некоторого целого k. Если a неотрицательно и 0<b<n, можно рассматривать b как остаток при делении a на n. Иногда b называют **вычетом** *a* по модулю n, иногда *a* называется конгруэнтным b по модулю n. Множество чисел от 0 до n-1 образует **полное множество вычетов** по модулю n. Это означает, что для любого целого *a* его остаток по модулю *n* является некоторым числом от 0 до n-1. Операция *a* mod *n* обозначает остаток от *a* , являющийся некоторым числом от 0 до n-1. Эта операция – **приведение по модулю**. 5 mod 3=2. *n* добавляется к результату операции получения остатка, если она возвращает отрицательное число. Арифметика остатков коммутативна, ассоциативна, дистрибутивна, кроме того, приведение каждого промежуточного результата по модулю *n* дает тот же результат, как и выполнение всего вычисления с последующим приведением конечного результата по модулю *n*.

$(a + b) \bmod n = ((a \bmod n) + (b \bmod n)) \bmod n$

$(a - b) \bmod n = ((a \bmod n) - (b \bmod n)) \bmod n$

$(a * b) \bmod n = ((a \bmod n) * (b \bmod n)) \bmod n$

$(a *(b + c)) \bmod n = (((a *b) \bmod n)+((a*c) \bmod n)) \bmod n$

Арифметика вычетов легче реализуется на PC , т.к. она ограничивает диапазон промежуточных значений и результата – для k битовых вычетов n они будут не длиннее, чем 2 k бит. Вычисление степени числа по модулю другого числа представляет собой последователь-ность умножений и делений, и существуют приемы, ускоряющие эти действия. Например, $a^x \bmod n$ при x=8:

$a*a*a*a*a*a*a*a \bmod n$ равноценно

$((a^2 \bmod n)^2 \bmod n)^2 \bmod n$

Эффективные алгоритмы многократного приведения по модулю для одного *n* метод Монтгомери, алгоритм Баррета.

Операция, обратная возведению в степень по модулю n , вычисляет дискретный логарифм. Обратное число для 4 – ¼, т.к. 4*1/4=1. 4*x =1 (mod 7) эквивалентно обнаружению целых *x* и *k*, таких, что 4x=7к+1,т.е. x такого, что 1=(*a**x) mod *n*

Для вычисления обратных функций (и НОД двух чисел) используется алгоритм Эвклида (300 лет д.н.э.+200). Алгоритм итеративен, Кнут показал, что среднее число делений равно: $0.843*\log_2(n) +1.47$. Функция вида $y=a^x(\text{mod } p)$ вычисляется сравнительно просто, а обратная к ней функция вида $y=\log_a y$ является вычислительно сложной практически для всех $1 < y < p$ при условии, что не только *p* велико, но и *p-1* имеет большой простой множитель (лучше всего, если это будет другое простое число, умноженное на 2). Известно, что для дискретного возведения в степень (требуется примерно $2\log_2 p$ умножений и порядка $3\log_2 p$ бит памяти, а для вычисления обратной функции (задача вычисления дискретных логарифмов требуется не менее $p^{1/2}$ операций и такое же количество бит памяти..

Оценки временной и емкостной сложности алгоритмов нахождения дискретных логарифмов свидетельствуют об субэкспоненциальной вычислительной сложности их выполнения, и при значениях *p* длиною сотни и тысячи бит данные алгоритмы вычислительно нереализуемы Рассмотрим возможные варианты использования ОНФ:1. решение задачи обеспечения безопасности использования пароля, по которому осуществляется доступ пользователя к ресурсам и услугам в автоматизированных системах. Известно, что размещение в явном виде в памяти ЭВМ паролей доступа пользователей небезопасно. Нарушитель, просмотрев файл паролей доступа, способен выдать себя за любого законного пользователя системы; 2. задача аутентификации пользователей автоматизированной системы может быть эффективно решена с использованием ОНФ. В частности, безопасным решением этой задачи может быть размещение в доступном для просмотра злоумышленником блоке памяти автоматизированной системы не самих паролей, а значений ОНФ от паролей доступа. Пусть каждый пользователь случайно выберет свой секретный пароль *x* и вычислит значение $y=a^x(\mathrm{mod}\ p)$

Открытое значение y вместе с именем пользователя может быть помещено в список паролей доступа в блок памяти ЭВМ. Законный пользователь для получения доступа в автоматизированную систему предъявляет свое число x. ЭВМ вычисляет по этому числу значение однонаправленной функции и сравнивает с хранящимся значением y. При совпадении этих значений пользователь становится идентифицированным и получает требуемый доступ. Злоумышленник, узнавший y, не в состоянии вычислить x и тем самым получить доступ как законный пользователь к защищаемым ресурсам и услугам. Если злоумышленник способен подсмотреть ввод пароля законным пользователем, то значение x и соответствующее ему y должны меняться после каждого использования (пароль должен быть одноразовым). Очевидно, что знание злоумышленником некоторых значений функции и соответствующих им аргументов не должно облегчать ему задач вычисления пароля по известному значению функции. Другим примером использования данной ОНФ является криптосистема открытого распространения ключа В. Диффи и М. Хеллмана.

Она предназначена для обеспечения криптосвязности двух корреспондентов сети связи без предварительного обмена секретной ключевой информацией. Пусть каждому корреспонденту сети известны значения чисел *a* и *p*. Эта часть ключевой информации является открытой, и допустимо ее знание нарушителем. Каждый корреспондент, например, корреспондент Ai, независимо от других случайно и равновероятно выбирает себе число xi из множества целых чисел 1,2. . ,p-1. Значение xi является индивидуальным секретным ключом корреспондента Ai вычисляет свой открытый ключ yi =ax (mod p) и помещает число yi в открытый заверенный справочник, доступный всем для чтения и защищенный от подмены. Точно так же каждый корреспондент Aj сети выбирает свой секретный ключ xj вычисляет открытый ключ yj =ax (mod p) и открыто публикует его

. Когда пара корреспондентов Ai и Aj хотят установить между собой криптосвязность для обмена секретными сообщениями, то корреспондент A_i, имея свой секретный ключ x_i и открытый ключ y_j корреспондента A_j вычисляет $K_{ij}=y^x_j \bmod p$ Корреспондент A_j по своему секретному ключу x_j и открытому ключу y_i корреспондента A_i вычисляет Kji аналогичным образом: $K_{ji}=y^x_i \bmod p$. Покажем, что, имея разную ключевую информацию, корреспонденты сформировали одинаковые ключи:

$$K_{ij} = y_j^{x_i} \bmod p = (a^{x_j})^{x_i} \bmod p = a^{x_j x_i} \bmod p$$

$$K_{ji} = y_i^{x_j} \bmod p = (a^{x_i})^{x_j} \bmod p = a^{x_i x_j} \bmod p$$

В силу коммутативности операции возведения

$$a^{x_j x_i} \bmod p \quad a^{x_i x_j} \bmod p$$

И поэтому Kij = Kji. Сформированный таким образом секретный ключ корреспонденты могут затем использовать как ключ шифрования передаваемых друг другу секретных сообщений. Для определения ключа Kij нарушитель должен решить задачу вычисления дискретного логарифма, например, вычисляя $x_i=\log_a y_i$, что при соответствующем выборе размерности параметра p может быть сделано вычислительно нереализуемым. Используемая в криптосистеме открытого распространения ключей Диффи Хеллмана однонаправленная функция не имеет вычислительно простого обратного отображения даже для законных пользователей, знающих секретную ключевую информацию. Однонаправленные функции, не имеющие и не требующие вычислительно простого обратного отображения для законных пользователей, широко применяются в таких криптографических задачах, в которых используется необратимое преобразование некоторых данных. Наиболее часто встречаемой задачей такого типа является формирование в шифрообразующем устройстве из сравнительно коротких ключей значительно более длинных шифрующих последовательностей, используемых для криптографической защиты сообщений.

Формирование непредсказуемых для нарушителя и равновероятных шифрующих последовательностей большой длины является основой построения поточных шифраторов. Стойкость данного типа систем шифрования в основном определяется вычислительной сложностью нахождения нарушителем обратного отображения к функции формирования шифрующей последовательности. Кроме однонаправленных функций, не имеющих вычислительно простого обратного отображения даже для законных пользователей, знающих секретную ключевую информацию, в криптографии широко используются однонаправленные функции, для которых знание секретного ключа дает возможность законному пользователю вычислительно просто находить обратное отображение. Такие ОНФ получили название однонаправленных функций с потайным ходом, иногда их называют однонаправленными функциями с лазейкой.).

ОДНОНАПРАВЛЕННЫЕ ФУНКЦИИ С ПОТАЙНЫМ ХОДОМ

Определение 8: однонаправленная функция с потайным ходом есть однонаправленная функция f_z с дополнительным свойством, называемым “потайным ходом", таким, что, зная информацию z потайного хода для каждого $y \in Im(f)$, вычислительно просто определить $x \in X$, удовлетворяющее уравнению $y = f_z(x)$. Для нарушителя, не знающего информации z потайного хода, нахождение обратного отображения $x=f_z^{-1}(y)$ может быть сделано вычислительно нереализуемым. Поэтому информация z может служить секретным ключом законного пользователя ОНФ с потайным ходом.

Стремительное развитие криптографии в последние два десятилетия во многом стало возможным благодаря открытию американскими учеными В.Диффи и М. Хэллманом однонаправленных функций с потайным ходом, которые используются для различных криптосистем защиты информации.

На основе однонаправленных функций с потайным ходом можно построить криптосистемы аутентификации информации в условиях взаимного недоверия корреспондентов системы шифрования информации, в которых отправители сообщений могут пользоваться несекретными ключами шифрования, криптосистемы обмена секретной ключевой информации по открытым каналам связи и многие другие криптосистемы, существование которых было невозможным до появления рассматриваемых криптографических функций. Оценивая стойкость криптосистем, построенных на основе известных однонаправленных функций с потайным ходом, отметим, что ни одна из них не является безусловно стойкой Это объясняется тем, что нарушитель с бесконечными вычислительными ресурсами способен вычислить обратное отображение к таким функциям Однонаправленные функции с потайным ходом относятся к вычислительно необратимым функциям.

Определение 9: функция вычислительно необратима, если не существуют алгоритмы нахождения обратного отображении к ней с полиномиальной вычислительной сложностью.

Данное определение предполагает, что могут существовать алгоритмы обращения вычислительно необратимой функции с произвольно большой сложностью Поэтому стойкость произвольных криптосистем на основе однонаправленных функций с потайным ходом заведомо ниже безусловно стойкой и может быть оценена не выше вычислительно стойкой.

Однонаправленная функция РША с потайным ходом

В 1978 году была предложена первая однонаправленная функция с потайным ходом, положенная в основу широко используемой на практике несимметричной криптографической системы РША. Первые буквы фамилий авторов - Р. Ривеста, А. Шамира и Л. Адлемана - образовали общепринятое название предложенной ими функции и криптосистемы. Для описания направленной функции РША с потайным ходом требуются некоторые знания из элементарной теории чисел. Пусть НОД(I,n) означает наибольший общий делитель целых i и n. Для каждого положительного целого числа n функция Эйлера Ф(n) определяется как число положительных целых чисел i, не превосходящих n и таких, что НОД(i,n)=1. Если для целых чисел i и n выполняется НОД(i,n)=1, то такие числа называются взаимно простыми числами, т.е. они не имеют никаких общих делителей, кроме единицы. Очевидно, что для i простого числа p все числа, меньшие его, являются взаимно простыми с ним и значение функции Эйлера: $\Phi(p)=p-1$ (2.8) Соответственно для произведения n=pq для двух неравных простых чисел p и q

$$\Phi(n) = \Phi(pq) = (p-1)(q-1)$$

Последний необходимый нам факт из теории чисел: для числа e, удовлетворяющего условиям 0<e<Φ(n) и НОД(ϕ(n),e) = 1, существует единственное число d такое, что 0<e<Φ(n) и

$de=1 \pmod{\Phi(n)}$ (2.10)

Однонаправленная функция РША с потайным ходом определяется как дискретное возведение значения x в степень ключа e

$f_z(x): y=x^e \pmod n$ (2.11)

где x есть положительное целое число, не превосходящее n (0<e<n), а информация потайного хода z={p,q,d} , где p и q являются большими простыми числами, а значение e есть положительное целое, не превосходящее Φ(n), для которого НОД (e, Φ(n)) =1

Функция $f_z(x)$ имеет обратную функцию вида

$f^{-1}_z(y): x=y^d \pmod n$ (2.12)

где значение d есть единственное положительное целое, меньшее Φ (n) и удовлетворяющее условию

$de=1 \pmod{\Phi(n)}$