В основу асимметричной криптографии положена идея использовать ключи парами: один – для зашифрования (открытый или публичный ключ), другой – для расшифрования (тайный ключ). Отметим, что указанная пара ключей принадлежит получателю зашифрованного сообщения.

*Односторонней функцией* (one-way function) называется математическая функция, которую относительно легко вычислить, но трудно найти по значению функции соответствующее значение аргумента, т. е., зная *х*, легко вычислить *f*(*x*), но по известному *f*(*x*) трудно найти подходящее значение *x*.

1. **Что такое «ранцевый (рюкзачный) вектор»? Дать определение.**

Это упорядоченный набор из n предметов.

1. **Сформулировать задачу укладки ранца.**

Дано множество предметов различного веса. Спрашивается, можно ли положить некоторые из этих предметов в ранец так, чтобы его вес стал равен определенному значению?

1. **Если вектор рюкзака имеет вид (14, 28, 56, 82, 90, 132, 197, 284, 341, 455), то какими следует принять коэффициенты *bi* из (7.1), чтобы полу-чить *S* = 517? Каким будет решение задачи для *S* = 516?**

**4. Что такое сверхвозрастающая последовательность? Привести примеры.**

*Сверхвозрастающей* называется последовательность, в которой каждый последующий член больше суммы всех предыдущих.

**5. Можно ли последовательности чисел: {89, 3, 11, 2, 45, 6, 22,}, {3, 41, 5, 1, 21, 10}, {2, 3, 11, 29, 45, 6, 39} преобразовать в сверхвозрастающие?**

**6. Записать в виде псевдокода алгоритм зашифрования и алгоритм рас-шифрования сообщения на основе задачи об укладке ранца.**

Для зашифрования сообщения (*М*) оно сначала разбивается на блоки, по размерам равные числу (*z*) элементов последовательности в ранце. Затем, счи-тая, что *1* указывает на присутствие элемента последовательности в ранце, а *0* – на его отсутствие, вычисляются полные веса рюкзаков (*Si*, *i* = 1, . . ., *z*): по одному ранцу для каждого блока сообщения с использованием открытого ключа получателя, ***e***.

1. **Используя некоторый вектор *S =* (103, 107, 211, 430, 863, 1716, 3449, 6907, 13807, 27610), вычислить ключи для зашифрования и расшифро-вания сообщений.**
2. **Можно ли, с Вашей точки зрения, одновременно зашифровывать (и, соответственно, – одновременно расшифровывать) более, чем по одному символу текста. Обосновать решение. Привести примеры решений.**

– можно, зависит от количества элементов во входном векторе и размера нашего шифртекста.

1. **Что такое «секретная лазейка»?**

Зная числа, а, *a*-1 и n («секретную лазейку»), можно восстановить сверхвозрастающую последовательность по нормальной последовательности [4]. Важно то, что числа, *а* и n («секретная пара») не обязательно должны быть теми же, что использовались при создании системы легальным пользователем.

1. **Охарактеризовать криптостойкость алгоритма на основе задачи об укладке ранца.**

Криптостойкость алгоритма во многом определяется скоростью поиска нужного варианта укладки ранца.

При реализации алгоритма ранец должен содержать не менее нескольких сотен элементов. Длина каждого члена сверхвозрастающей последовательности должна быть несколько сотен бит, а длина числа *n* – от 100 до 200 бит. Для получения этих значений практические реализации алгоритма используют генераторы ПСП.

Самый быстрый алгоритм имеет экспоненциальную зависимость от числа возможных предметов. Если добавить к последовательности весов еще один член, то найти решение станет вдвое труднее.

Потому что можно найти секретную лазейку, причем не обязательно находить те числа, которые использовались при шифровании, важно чтобы они подходили, ну эти числа a,a^-1,n.

7.1.2.3 Зашифрование сообщения

В основе операции лежит соотношение (7.1). Для зашифрования сообщения (М) оно сначала разбивается на блоки, по размерам равные числу (z) элементов последовательности в ранце. Затем, считая, что 1 указывает на присутствие элемента последовательности в ранце, а 0 – на его отсутствие, вычисляются полные веса рюкзаков (Si, i = 1, . . ., z): по одному ранцу для каждого блока сообщения с использованием открытого ключа получателя, e. Пример4. Возьмем открытое сообщение M, состоящее из 7 букв (mj), которые представим в бинарном виде (1 символ текста – 1 байт). Бинарное представление символов дано в первом столбце нижеследующей таблицы (табл. 7.1). Открытый ключ, е: {62, 93, 186, 403, 417, 352, 315, 210} Результат зашифрования (упаковки ранца) каждого блока (буквы) сообщения с помощью открытого ключа представлен в правом столбце таблицы 7.1.

Таблица 7.1 Пояснение к примеру зашифрования сообщения укладкой ранца Бинарный код символа mj сообщения Укладка ранца Вес ранца 11010000 62+93+403 558 11000010 62+93+315 470 11000000 62+93 155 11000001 62+93+210 365 11001110 62+93+417+352+315 1239 11000000 62+93 155

11001100 62+93+417+352 924

Таким образом, зашифрованное сообщение С = 558 470 155 365 1239 155 924: с1 = 558, с2 = 470 и т. д.

7.1.2.4 Расшифрование сообщения

Для расшифрования сообщения получатель (использует свой тайный ключ, d: сверхвозрастающую последовательность) должен сначала определить обратное к а число: а-1, такое что

а а-1(mod n) = 1. (7.3)

Для вычисления обратных чисел по модулю можно использовать известный нам расширенный алгоритм Евклида. После определения обратного числа каждое значение шифрограммы (ci) преобразуется в соответствии со следующим соотношением:

Si = ci а-1 mod n. (7.4)

Полученное на основании последней формулы для каждого блока число далее рассматривается как заданный вес ранца, который следует упаковать по изложенному выше алгоритму, используя сверхвозрастающую последовательность (тайный ключ получателя). Продолжим рассмотрение примера 4. В нашем примере значение а-1 = 271: 31\*271 mod 420 = 1. Вспомним, что сверхвозрастающая последовательность равна d: d= {2, 3, 6, 13, 27, 52, 105, 210}, а также n = 420, a = 31; шифртекст: 155 365 558 155 924 1239 470 Расшифрование первого блока шифртекста. Сначала вычисляем, используя (7.4), вес первого ранца (при c1=155):

S1 = c1\*а-1 (mod n) = 155\*271 (mod 420) =5.

Используем S1 =5 и с помощью сверхвозрастающей последовательности ({2, 3, 6, 13, 27, 52, 105, 210}) и известного алгоритма упаковки ранца получаем m1= 11000000. Понятно, что последней бинарной последовательности должен соответствовать некоторый символ алфавита в используемой таблице кодировки. Расшифрование остальных блоков шифртекста производится аналогично.