В основу асимметричной криптографии положена идея использовать ключи парами: один – для зашифрования (открытый или публичный ключ), другой – для рас-шифрования (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 значе-ние *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.**

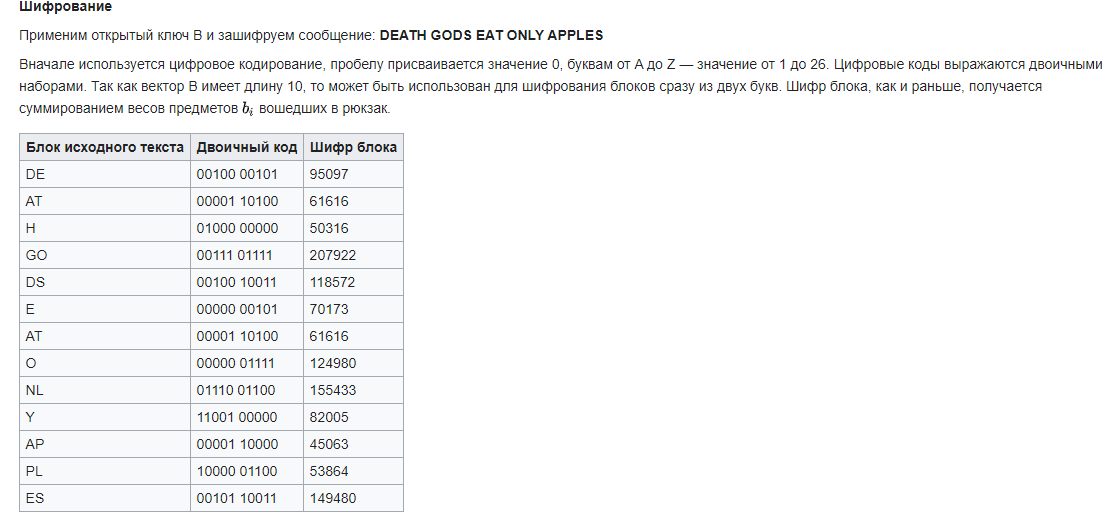
*Сверхвозрастающей* называется последовательность, в которой каждый последующий член больше суммы всех предыдущих.

**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, со-ответственно, – одновременно расшифровывать) более, чем по одному символу текста. Обосновать решение. Привести примеры решений.**



1. **Что такое «секретная лазейка»?**

Зная числа а, *a*-1 и n («секретную лазейку»), можно восстановить сверхвозрастающую последовательность по нормальной после-довательности [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.