Ассиметричные коды. Задача о рюкзаке

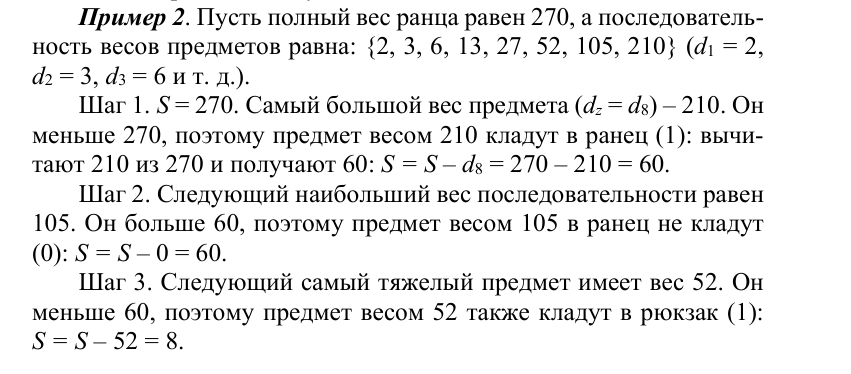
Основа АК в том, что одна пара ключей для зашифрования (открытый ключ), а другая для расшифрования (закрытый). Оба типа принадлежат получателю сообщения. В основе лежит:

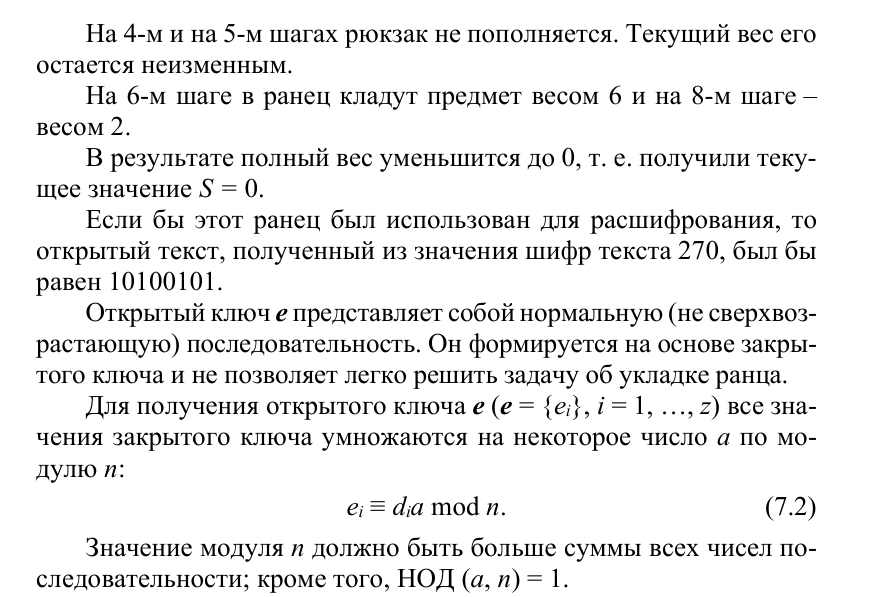
Односторонняя функция. По известному x легко вычислить f(x), но по известному f(x) сложно найти подходящее x. Пример, дискретный логарифм.

Суть метода шифрования для задачи об укладке рюкзака заключается в том, что существует два решения задачи: легкое (закрытый ключ/для расшифрования) и сложное (открытый ключ/для шифрования).

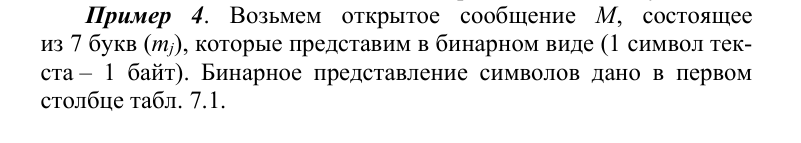
В качестве d приватного расшифрования применяется сверхвозрастающая последовательность – каждый последующий член больше суммы всех предыдущих.

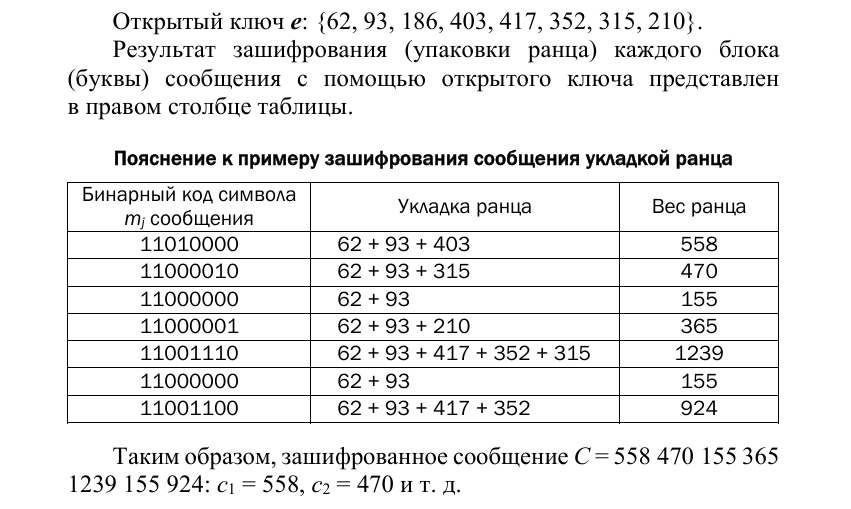
Алгоритм укладки ранца на основе сверхвозрастающей последовательности



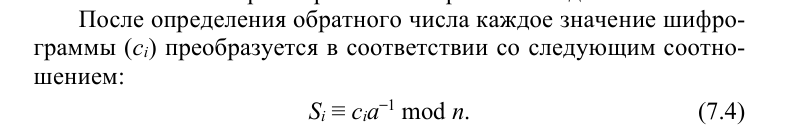


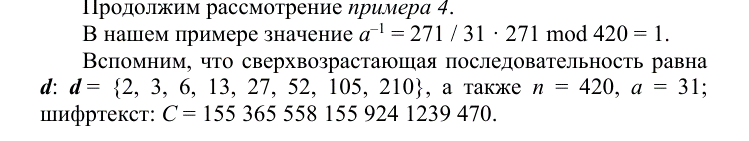
Зашифрование сообщения

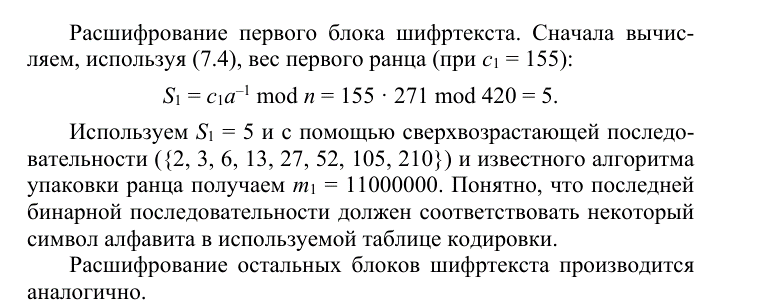




Расшифрование сообщения







Криптостойкость зависит от скорости поиска нужного варианта укладки ранца. На реальных задача ранец должен содержать не менее сотен элементов. Поэтому практическая реализация выполняется через генераторы ПСП.

Эта задача имеет экспоненциальную зависимость от числа возможных предметов. При добавлении одного элемента, решение задачи становится вдвое сложнее.

Ранцевые криптосистемы больше не являются криптостойкими. Зная, a, a-1 n можно восстановить сверхвозрастающую последовательность по нормальной.