**Ассим. шифры:**

идея использ. ключи парами: 1 - для зашифр (откр), 2 - для расшифр (тайный)  
эта пара принадл. получателю зашифр. сообщ-я  
в основе одностор. ф-я

**Односторон. ф-я** – матем. ф, к-ю легко вычислить, но трудно найти по значению ф-и соотв. значение аргумента: зная х, легко найти у но не наоборот!

**Сверхвозр. посл-сть** – к. член больше суммы всех предыдущих: {2, 3, 6, 13, 27, 52, 105, 210}

**Задача об укладке ранца:**

**S**=(s1,…,sz) – **ранцевый вектор** – упоряд. набор из z(≥3) нат. чисел  
Вход – пара (**S**, S), где S – нат. число, **S** – р.вектор  
Решение – подмн-во из **S**, сумма = S  
 S = b1s1 + … + bzsz b = 0 (нет) или 1 (кладут)

**Трудный ранец** – примен в кач. откр ключа **е**, кот. легко использ для зашифрования, но невозможно – для расшифрования. В кач-ве закр. ключа **d** (*сверхвозр. посл*.) примен **легкий ранец**, кот. предост. простой способ расшифр сообщения

**Алг. укладки ранца на основе сверхвозр. посл.:**

1) Выбир. число S, кот. сравнивается с весом самого тяжелого предмета (dz)  
2) S< предмет в ранец не кладут (0), иначе – кладут (1) и S-di  
3) Если S=0, решение найдено, иначе нет

**Откр. ключ е** – норм. посл-сть, формир на основе закр.ключа и не позв. легко решить задачу об укладке ранца.  
Для получ. е={e1…ez} : ei = di\*a (mod n), n > суммы всех чисел посл-сти, НОД (a,n)=1

**Зашифрование сообщения:**

откр. сообщ М сост. из 3 букв (mj)  
откр. ключ е: {62, 93, 186, 403, 417, 352, 315, 210}

|  |  |  |
| --- | --- | --- |
| Бинарный код символа mj сообщения | Укладка ранца | Вес ранца |
| 11010000 | 62+93+403 | 558 |
| 11000010 | 62+93+315 | 470 |
| 11000000 | 62+93 | 155 |

Зашифр. сообщ С = 558 470 155 365 1239 155 924: с1 = 558, с2 = 470…

**Расшифрование сообщения:**

Исп. тайный ключ d = {2, 3, 6, 13, 27, 52, 105, 210}  
1) опред. а-1 : а\*а-1 (mod n) = 1 (расш. алг Евклида)  
2) к. ci преобр: Si = ci\*a-1 mod n  
3) Исп-я Si с пом. d и известного алгоритма упаковки получаем mi   
 пр.: Si=5: 5-3=2; 2-2=0; mi=110000000

**Безопасность криптоалгоритма на основе задачи об укладке ранца:**

\* опр-ся скоростью поиска нужного варианта укладки  
 на практике неск. 100 элементов == исп. генераторы ПСП  
\* самый быстрый алг. имеет *экспоненц*. зависимость от числа возм. предметов  
 доб. к весам 1 предмет == найти решение х2 труднее  
\* НЕ КРИПТОСТОЙКИЕ  
 зная числа а, а-1, n **(«секретную лазейку»)** м. восст. сверхвозр. посл-сть  
 а и n **(«секретная пара»)** необяз. те же, что исп. при создании с-мы

ЗАДАНИЕ:

\* генерация сверхвозр. посл-сти (тайного ключа)  
 старший член – число[100 бит], z=8 (ASCII)  
\* вычисл. норм. посл-сти (откр. ключа)  
\* зашифр / расшифр ФИО  
\* оценка времени