LATTIC homework hw11 yan liang 112889478

4/19/2018.

1.

M=(3,7,19,43,89,195),

Let me just run it once and the later one is similar as the first one, S=260,

195<260 so it is in, 260-195=65 89>65 not in, 43<65 in, so remaining will be 22,

Keep going, 19<22, in, 3 remaining, 7 pass and 3 in ,

So the sequence will be (1,0,1,1,01)

Which means 3+19+43+195=260 so it works for this one

M=(5,11,25,61,125,261)

The algorithms does not work, since there is no sequence that satisfy sum problem in this sequence.

M=(2,5,12,28,60,131,257)

S=334 similarly to preblem1 we will get

(0,1,1,0,1,0,1)

5+12+60+257=334.

M=(4,12,15,36,75,162) S=214

The algorithms does not work since 4+12>15 so it is not a super increasing sequence.

2.

public key is M=(5186,2779,5955,2307,6599,6771,6296,7306,4115,637)

S=25916, A=4392 B=8387

Find inverse(A) in sage

sage: R=Integers(**8387**)

sage: gcd(**8387**,**4392**)

1

sage: R(**4392**)^(-**1**)

2683

sage:

Then we can calculate ri

The by multiply inverse(A) and then mod B

(5,14,30,75,160,351,750,1579,3253,6510)

Encrypted message S=25916 S-PRIME=R(2683)*R(25916)=4398

The we use the super increasing sequence r(I) to solve the problem

(0,1,1,0,0,1,1,0,1,0)

So the message being send is the above sequence.

3.

(a) We need to find a matrix that solve this problem A*B'=B since B and B' is 3*3 so the A should be 3*3

Since B is a basis, so all B should be invertible

So we just need A=B*(B'^-1)

Putting in sage we get this:

[13/3 3 -11/3]

[-1 -1 4]

[1/3 0 4/3]

(b)

|v|=3.74

|w|=4.58

V*w=-2+12+(-2)=8

So cos(theta)=8/(3.74*4.58) . theta=62.16 degrees.

6.7

sage: b=matrix([[**1**,**3**,-**2**],[**2**,**1**,**0**],[-**1**,**2**,**5**]])

sage: b.determinant

sage: b.determinant()

-35

So the volume should be 35, the volume can be calculated using the deterministic of the base.