X = 92 => Y = X % 4 == 0

May be I wrong some where. Then you guy can fix me, that would be great!!

(1)

4 characters A,B,C,D (subtitution with 0-9)

P\_A = 40%; P\_B = 20%; P\_C = 10%; P\_D = 30%

A: 9,8,7,6

B: 5,4

C: 3

D: 2,1,0

=> using this flatten the frequency of each symbol

(2)

k = Y\*2+1 = 1

1.

Select p,q in range(10+k,20+k)

p = 13; q = 19

e min sat

=> e = 5 ( 3 not coprime (prime-1) in case prime<21)

2.

phi = (p-1)\*(q-1) = 216

d = pow(e,-1,phi) = 65

3.

c = pow(0b10001^(Y%16),e,p\*q) == 101

4.

send: E(m)||another\_D(E(m)) and pub\_key\_another

using another pubkey-private to create hash

(3)

hash\_size = (Y+2)\*16 (bits) == 32 (bits) == 4 (bytes) (useless in this excercise)

chip[i] can do: pow(10,i)\*1000 (hash/sec)

price : pow(i,i/2)\*1000 ($)

banks send HOST

A format 1200 bytes each packets (Y+1)\*100 (Gbytes/hour)

B format 1500 bytes ---- 128 bytes ---> = 100\*pow(2,30) (bytes/hour)

C format 1800 bytes (C format >= 50%)

(each format fix size and

already include 1 hash)

This excercise question: minimum price bank have to invest hash\_gen\_machine ??

total\_bytes\_HOST\_receive\_per\_sec = 100\*pow(2,30)/3600 (bytes/sec)

total\_packets\_HOST\_receive\_per\_sec = 100\*pow(2,30)/(3600\*128) (bytes/sec)

number\_of\_packet\_require\_to\_send\_file\_C = total\_packets\_HOST\_receive\_per\_sec\*50%

number\_of\_packet\_require\_to\_send\_file\_AB = 1-number\_of\_packet\_require\_to\_send\_file\_C

we can calculate the number packet at least to send each format file:

A need = ceil(1200/128) = 10 (packets)

B need = ceil(1500/128) = 12 (packets)

C need = ceil(1800/128) = 15 (packets)

=> each file has a hash in file format

total\_hash\_in\_file\_C\_per\_sec = number\_of\_packet\_require\_to\_send\_file\_C/15

total\_hash\_in\_file\_B\_per\_sec = number\_of\_packet\_require\_to\_send\_file\_B/12

total\_hash\_in\_file\_A\_per\_sec = number\_of\_packet\_require\_to\_send\_file\_A/10

=> the worst case scenario: 50% AB contain only A (need more hash)

total\_hash\_in\_file\_A\_per\_sec = number\_of\_packet\_require\_to\_send\_file\_AB/10

hash\_per\_sec = total\_hash\_in\_file\_C\_per\_sec+total\_hash\_in\_file\_A\_per\_sec

number\_machine = ceil(hash\_per\_sec/(pow(10,i)\*1000))

price = ceil(hash\_per\_sec/(pow(10,i)\*1000)) \* pow(i,i/2)\*1000

min\_price = 2000$

if i == 2