1.Rabin

RSA e=2,rabin 算法

2.包里有什么

根据b0的值，可以求出w的值

分析数组v中的值不是1就是0，且b数组中的值在模m的情况下都是w的倍数，所以c在模m的情况下也是w的倍数，因此有c同余k*w mod m.再分析bin（k）中等于1的位置，v数组中也必定是1，其余为0.

将bin（k）右移一位，再逆序，就是v数组全部，即plain.

代码：

```
m =152863722253103833295869496511433041577389657189101762949342 4

b0=693566065333254565209687760347302145851105369329893131379 26

c =936020621334873611514207530577393971617346516097865987654621 62

w =b0//2

from Crypto.Util.number import *

k=inverse(w,m)*c %m

a=bin(k>>1)

a=b'1111110000101110100101101111110101110110001110110110011101001011011111010100
1110010000110010001101111101010011110110011101000011011001100111110100111011000
1011001111101011001110111001000010111010001 1'

b=a[::-1]

print(b)

d=0b1100010111010000100111011100110101111100110100011011100101111100110011011000
0010111001101111001010111111011000100110000100111001010111110110100101110011011 0
1110001101110101111101101001011101000011111 1

print(long_to_bytes(d))
```

3.RSA大冒险

1.猜测m<p

2.加密过程中，p不变，q改变，所以两次n的gcd为p

3.e为3很小，直接爆破m

4.加密过程中，e变化，n不变，共模攻击。