HW8.wxmx 1 / 2

```
p:next_prime(382956327891237462038293748015);
q:next_prime(932343245242348534753975296852);
n:p·q;
e:2^20+1;
     1048577
pn:(p-1)\cdot(q-1);
gcd(e, pn);
m:09711011610510010511510111511609709810810511510410
c:power_mod(m, e, n);
n:712446816787;
    712446816787
e:6551;
    6551
c:273095689186;
    273095689186
pn:totient(n);
    712445114176
inv_mod(e, pn);
     368022327335
```

HW8.wxmx 2 / 2

```
power_mod(c, %, pn);
516975928768

m:111110101;
111110101

c:power_mod(m, e, n);
573878944579

m:116119111;
116119111

c:power_mod(m, e, n);
432406862407
```