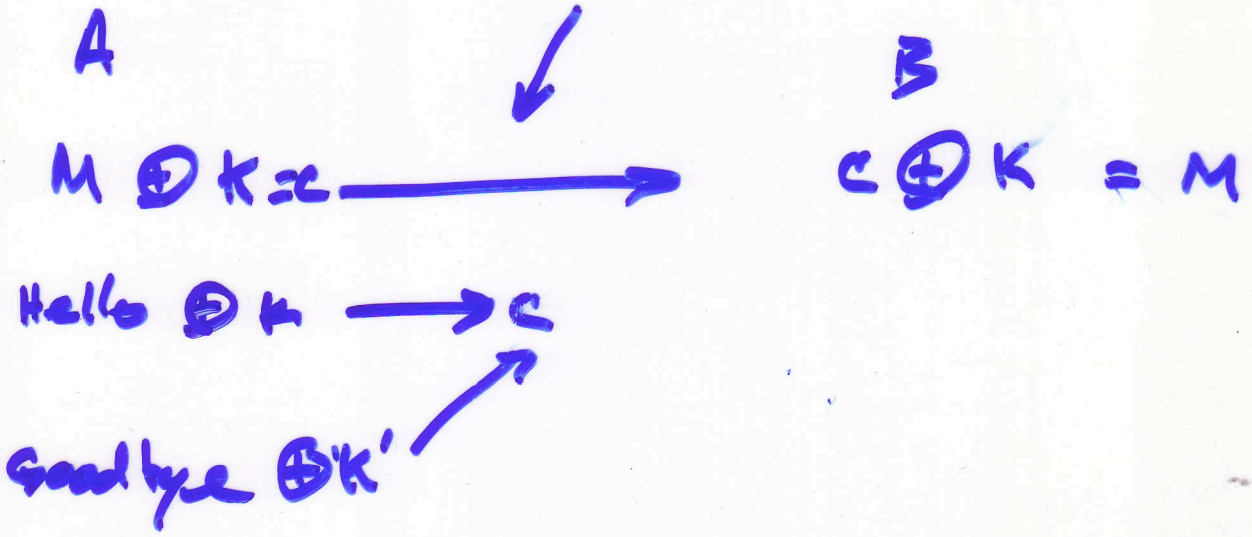
A & B secretly flip 1000 coins
write down 0/1 sequence K



→ One time Pad

Provably Secure if K secret & used once

Pseudo random seq

$$X_{n+1} = (aX_n + b) \bmod c$$

X_0 = "seed"

RSA - A Public Key Cryptosystem

Alice:

① Privately chooses two primes p, q of, say, 500 bits each, and an e rel. prime to $(p-1)(q-1)$.

② Privately computes $n = p \cdot q$ and d such that $ed \equiv 1 \pmod{(p-1)\cdot(q-1)}$

③ Publishes n and e in the phonebook

(Keep p, q, d private.)

Bob (or anyone else):

Sends her an encrypted message M by looking up her n, e and sending $c = M^e \bmod n$

Alice decrypts by computing

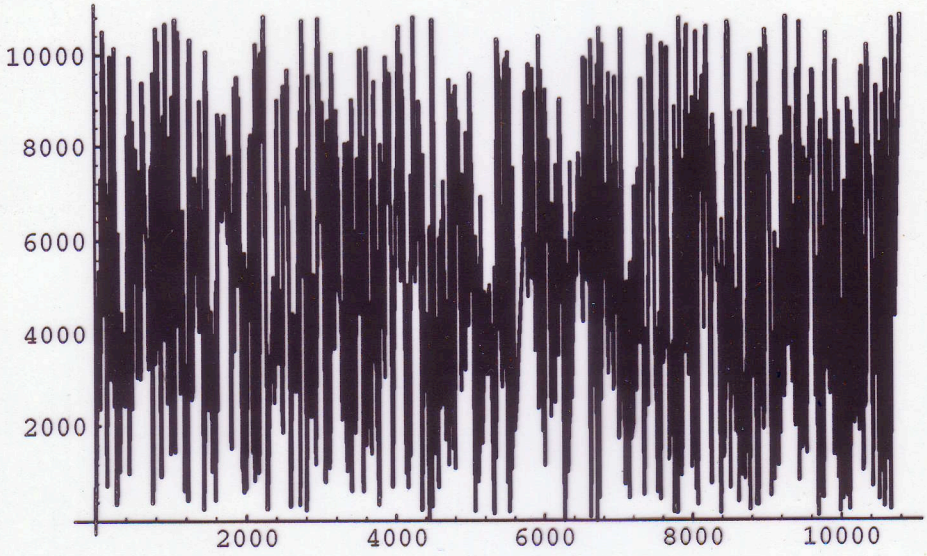
$$c^d \bmod n = M.$$

Issues:

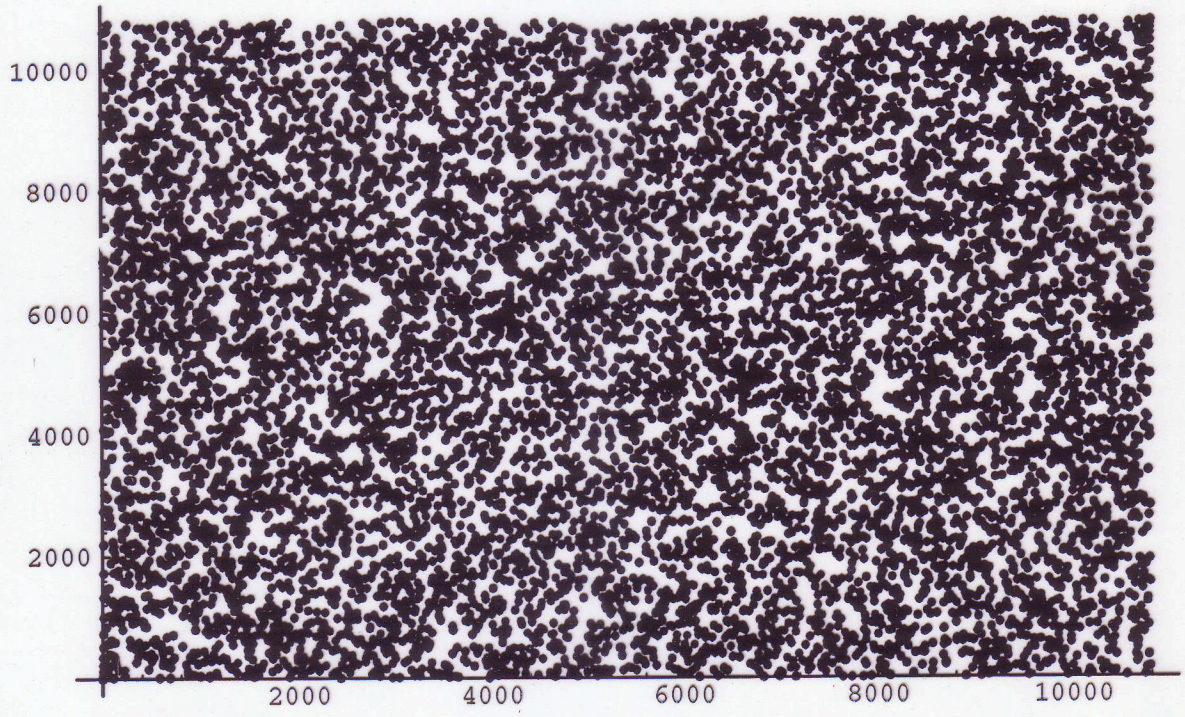
- do e, d always exist?
- how hard to compute?
- why $(M^e)^d \bmod n = M$?
- how secure?

Why does Modular powering hide things?

In[13]:=
```
PrimeQ[{101,107}]
```
Out[13]=
```
{True, True}
```
In[14]:=
```
n=101*107; Plot[{Mod[x^3,n]},{x,0,n-1}]
```



In[15]:=
```
n=101*107; ListPlot[Table[{x,Mod[x^3,n]},{x,0,n-1}]]
```



RSA Decryption

p, q Prime — private

$n = pq$ — public

e rel. primes $(p-1)(q-1)$ — public

d, $ed \equiv 1 \pmod{(p-1)\cdot(q-1)}$ — private

Encryption: $c = M^e \bmod n$

Decryption: $M' = c^d \bmod n$

] claim $M' = M$

Why does it work?

$$ed \equiv 1 \pmod{(p-1)\cdot(q-1)}$$

$$\therefore ed = 1 + k\cdot(p-1)\cdot(q-1)$$

Note: need $\gcd(M, n) = 1$

$$M' = M^{ed} = M^{1+k(p-1)(q-1)}$$

Fermat [

$$M' = M\cdot\left(M^{(p-1)}\right)^{k(q-1)} \equiv M \pmod{p}$$

$$M' = M\cdot\left(M^{(q-1)}\right)^{k(p-1)} \equiv M \pmod{q}$$

] ⇐

Chinese Remainder Theorem [

$$\therefore M' \equiv M \pmod{n}$$