Practical Aspect of RSA

* Key operation : $a^e \bmod n$

* Suppose :

  $a \sim 150$ digits

  $e \sim 120$ digits ,

  $\approx 10^{120}$

  $n \sim 150$ digits

* Method 1:

  ① calculate a^e

  ② Take mod n

problem : $10^2 = 100$, $1+2$ digits

$10^3 = 1000$, $1+3$ digits

10^k $1+k$ digits

$a^e > 10^e$ $1+e$ digits

$\approx 1 + 10^{120}$ digits

Too long to fit in computer

* Method 2

$a^3 \bmod n = a(a^2 \bmod n) \bmod n$

$a^4 \bmod n = a(a^3 \bmod n) \bmod n$

$a^5 \bmod n = a(a^4 \bmod n) \bmod n$

. . . .

$a^e \bmod n = a(a^{e-1} \bmod n) \bmod n$

Results $< n$, fit in computer

problem ?

<u>10^{120} steps!</u>

The Sun would burn out

before we finished.

Fact on slide 42 follows from Th 4.24

* p & q relatively prime
* Let $a = x \bmod p \in Z_p$

  $b = x \bmod q \in Z_q$
* Consider equations

$$y \bmod p = a \quad (1)$$

$$y \bmod q = b \quad (2)$$

* They have unique s/n in $Z_{pq} = Z_n$
* $y = x$ is one s/n of (1)+(2) in Z_n
* Because

$$x^{ed} \bmod p = a$$

$$x^{ed} \bmod q = b$$

$$(x^{ed} \bmod n) \bmod p = a$$

$$(x^{ed} \bmod n) \bmod q = b$$

* so $\underline{x^{ed} \bmod n}$ is also a

sln of (1) + (2)

& it is in Z_n

* By Th 4.24, we have

$$x^{ed} \bmod n = x.$$

proved.

# of muls in repeated squaring

$\leq$ s in squaring process

$+$ s in the last step

$= 2s \leq \boxed{2\log_2 e}$

$$\boxed{\begin{aligned} &2^s \leq e \\ \Rightarrow\ & s \leq \log_2 e \end{aligned}}$$

# of muls in Naive method

$= \boxed{e-1}$