Public Key Encryption from trapdoor permutations

Is RSA a one-way function?

Is RSA a one-way permutation?

To invert the RSA one-way func. (without d) attacker must compute:

$$x \quad \text{from} \quad c = x^e \pmod{N}.$$

How hard is computing e'th roots modulo N ??

Best known algorithm:

- Step 1: factor N (hard)
- Step 2: compute e'th roots modulo p and q (easy)

Shortcuts?

Must one factor N in order to compute e'th roots?

To prove no shortcut exists show a reduction:

– Efficient algorithm for e'th roots mod N

$\Rightarrow$ efficient algorithm for factoring N.

– Oldest problem in public key cryptography.

Some evidence no reduction exists: (BV'98)

– "Algebraic" reduction $\Rightarrow$ factoring is easy.

How **not** to improve RSA's performance

To speed up RSA decryption use small private key d $\quad$ ($d \approx 2^{128}$)

$$\boxed{c^d = m \pmod N}$$

Wiener'87: $\quad$ if $d < N^{0.25}$ then RSA is insecure.

BD'98: $\quad$ if $d < N^{0.292}$ then RSA is insecure $\quad$ (open: $d < N^{0.5}$)

<u>Insecure:</u> priv. key d can be found from (N,e)

Wiener's attack

Recall: $e \cdot d = 1 \pmod{\varphi(N)} \Rightarrow \exists\, k \in Z: \quad e \cdot d = k \cdot \varphi(N) + 1$

$\varphi(N) = N\text{-}p\text{-}q+1 \Rightarrow |N - \varphi(N)| \le p+q \le 3\sqrt{N}$

$d \le N^{0.25}/3 \Rightarrow$

Continued fraction expansion of e/N gives k/d.

$e \cdot d = 1 \pmod{k} \Rightarrow \gcd(d,k)=1 \Rightarrow$ can find d from k/d

End of Segment