RSA factoring, Malleability

Claim: (last time) If you can compute d given (N, e) then you can find nontrivial sqrt of unity mod N

$$x \not\equiv_N \pm 1 \qquad x^2 \equiv_N 1$$

Algo: given N, e, d $(ed \equiv_{\varphi(N)} 1)$

write $ed - 1 = 2^s \cdot r$ where r odd

pick random $w \leftarrow \mathbb{Z}_N$

starting with w^r, keep iteratively squaring (mod N) until you reach 1

Malleability of RSA:

$$\text{RSA: } m \longmapsto m^e \bmod N$$

Q: given $c = m^e$ (RSA "encryption" of unknown m)

can you find RSA enc of "related" msg?

A: $c \rightsquigarrow c^2 = (m^e)^2 = (m^2)^e$ = RSA enc of m^2

$c \rightsquigarrow c^x$ is RSA enc of m^x

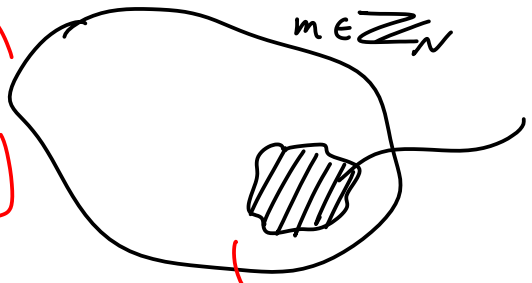
$c \rightsquigarrow c \cdot x^e = (m^e)(x^e) = (mx)^e$

(ok since e is public)

Claim: Suppose algo $\mathcal{A}$ inverts RSA (given m^e, N, e returns m) but only for 1% of $m \in \mathbb{Z}_N$

$\Rightarrow$ Then there is a way to invert RSA on all inputs

NOT: for all $m \in \mathbb{Z}_N$, A has 1% chance of being correct



m's for which A gives right answer

A always gives wrong answer

SuperInverter(c, N, e):

// want to find $m : m^e = c$

repeat:

$x \leftarrow \mathbb{Z}_N$

$c' = c \cdot x^e$ // c' is RSA enc of $m \cdot x = m'$

$\tilde{m} \leftarrow A(c', N, e)$

if $\tilde{m}^e = c'$: // A was successful

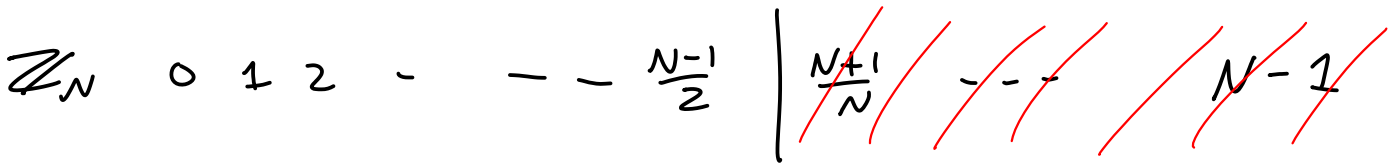
return $\tilde{m} \cdot x^{-1}$

each time thru loop, $m \cdot x$ has 1% chance of being a good input for A

Claim: If given m^e, N, e you can determine whether $m < N/2$, then you can invert RSA

Ex: Suppose I have $c = m^e$ for unknown m

① run algo on c, find that m is in 1st half



② run algo on $c \cdot 2^e = (2m)^e$, find that $2m$ is in 2nd half of $\mathbb{Z}_N$