

RSA works!

Let M be a message, $M < n$.

encrypt, compute $M^e \pmod n$.

~~See~~ Call this N .

Send N to amazon.com
they have a private d .

they compute $N^d \pmod n$.

$$\begin{aligned} N^d \pmod n &= (M^e)^d \pmod n = M^{e \cdot d} = M^{k \cdot \phi(n) + 1} = M^{\phi(n) \cdot k} \cdot M^1 \\ &= (M^{\phi(n)})^k \cdot M = 1^k \cdot M = M \quad (\text{all mod } n) \end{aligned}$$

$$\begin{aligned} e \cdot d \pmod n &= 1 \\ \text{which means} \\ e \cdot d &= 1 + k \cdot \phi(n), \\ \text{for some integer } k \end{aligned}$$

Q: Why not just compute $\ell(pq)$ when n and e are published. then find d using the E.A. and it's reverse/unfolding?

A: Finding p and q from their product alone seems to be hard.

Note: there is no proof that it is actually mathematically intractable.
(Computationally)

Two RSA challenges:

$$\textcircled{1} \quad n = 493 \\ e = 17 \\ N = 110$$

$$\textcircled{2} \quad n = 589 \\ e = 17 \\ N = 534$$

Due Monday