CS 280 Fall '03, Example of RSA

November 5, 2003

1. $n = pq$, $\varphi(n) = (p-1)(q-1)$.

   Pick block size $b < \min(p, q)$. Want b coprime to n.

   Pick exponent e with $\gcd(e, \varphi(n)) = 1$

   Get $e^{-1} (= s$ with $1 = se + t\varphi(n))$. Publish n and e.

   If message block is x_i then send $y_i = x_i^s \bmod n$.

2. receives y_i and computes $y_i \bmod n$

   $= (x_i)^{se} \bmod n$

   $= (x_i)^{1+k\varphi(n)} \bmod n$

   $= x_i (x_i^{\varphi(n)})^k \bmod n$

   $= x_i 1^k \bmod n = x_i$

E.g., send $X =$ "invest in bonds" using $p = 61$, $q = 127$.
So publish $n = 7747$, compute $\varphi(n) = 7560$, pick and publish $e = 3113$.
Compute $e^{-1} = s = \ldots = 17$
So $X \to$ 0813 2104 1819 0813 0114 1303 1823 (added a X)
Raise each to 17th power and send
2169 0628 5540 2169 6560 6401 4829