Tuesday, February 3, 2015 3:20 PM

Figure 1.9 RSA.

Bob chooses his public and secret keys.

- He starts by picking two large (n-bit) random primes p and q.
- His public key is (N, e) where $N = pq$ and e is a $2n$-bit number relatively prime to $(p-1)(q-1)$. A common choice is $e = 3$ because it permits fast encoding.
- His secret key is d, the inverse of e modulo $(p-1)(q-1)$, computed using the extended Euclid algorithm.

Alice wishes to send message x to Bob.

- She looks up his public key (N, e) and sends him $y = (x^e \bmod N)$, computed using an efficient modular exponentiation algorithm.
- He decodes the message by computing $y^d \bmod N$.

$p = 5$ & $q = 11 \Rightarrow N = 55$, $e = 3$, $(p-1)(q-1) = 40$

$\gcd(3, 40) = 1$, we ~~case~~ use extended Euclid to find d

$40 = 13 \cdot 3 + 1 \Rightarrow 1 = \underline{40} - 13 \cdot \underline{3} \Rightarrow 3^{-1} \equiv -13 \equiv 27 \bmod 40$

$x = 13 \Rightarrow y = 13^3 = 52 \bmod 55$

$y^{27} = 52^{27} = 13 \bmod 55$

hence $13 = (13^3)^{27} \bmod 55$