13

- This scheme is computationally expensive (i.e. slow)
  - Use for key establishment (and digital signatures)

e *d*

- Exponentiating by e is encryption; exponentiating by d is decryption

$$2 < \mathrm{K} < N - 1 \qquad \left(\mathrm{K}^{e} \% N\right)^{d} \% N = \mathrm{K}$$

- Why do this?
  - Because for

$e : N = 17 : 55$ $d : N = 33 : 55$

-
- Chooses , finds
- Public key: ; Private key:

$e = 17$ d $(e \cdot d)\ \%\ \varphi(N) = 1$

$\Rightarrow (17d)\ \%\ 40 = 1 \quad \Rightarrow d = 33$

-
- Chooses , finds where

$$p = 5, q = 11 \quad \Rightarrow N = pq = 55$$

$$\varphi(N) = (p-1)(q-1) = 40$$

- Chooses

- Sara creates a key pair

RSA (simplified)

RSA (simplified)

- Sara creates a key pair
  - Chooses $p = 5, q = 11 \Rightarrow N = pq = 55$ & $\varphi(N) = (p-1)(q-1) = 40$
  - Chooses $e = 17$, finds d where $(e \cdot d)\ \%\ \varphi(N) = 1$

$$\Rightarrow (17d)\ \%\ 40 = 1 \quad \Rightarrow d = 33$$

  - Public key: $e : N = 17 : 55$; Private key: $d : N = 33 : 55$
- Why do this?
  - Because for $2 < \mathrm{K} < N - 1$, $\left(\mathrm{K}^e\ \%N\right)^d\ \%N = \mathrm{K}$
    - Exponentiating by e is encryption; exponentiating by d is decryption
  - This scheme is computationally expensive (i.e. slow)
    - Use for key establishment (and digital signatures)

RSA (simplified)