- This scheme is computationally expensive (i.e. slow)

  - Use for key establishment

- Exponentiating by   is encryption; exponentiating by   is decryption

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

- Why do this?

  - Because for

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

-

- Chooses   , finds

- Public key: ;   Private key:

$$e = 17 \qquad d \qquad (e \cdot d) \mathbin{\%} \varphi(N) = 1$$

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

-

- Chooses   , finds   where

$$p = 5, q = 11 \implies N = pq = 55$$
$$\varphi(N) = (p-1)(q-1) = 40$$

• Chooses

- Sara creates a key pair

RSA (simplified)

RSA (simplified)

- Sara creates a key pair

  - Chooses $p = 5, q = 11 \Rightarrow N = pq = 55$
  $$\& \quad \varphi(N) = (p-1)(q-1) = 40$$

  - Chooses $e = 17$, finds d where $\left(e \cdot d\right) \% \varphi(N) = 1$
  $$\Rightarrow \left(17d\right) \% 40 = 1 \quad \Rightarrow d = 33$$

  - Public key: $e : N = 17 : 55$; Private key: $d : N = 33 : 55$

- Why do this?

  - Because for $2 < K < N - 1, \quad \left(K^e \% N\right)^d \% N = K$

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

  - This scheme is computationally expensive (i.e. slow)

    - Use for key establishment

13

RSA (simplified)