

Copyright © 2018 Knoxen, LLC. All Rights Reserved.



K = 6

- Chuck and Sara *establish* *via key transport*

- They could use a DH *key agreement* instead

$$nonce = D_K(C) \qquad C = E_K(nonce)$$

$$K = M^d \% N$$

$$= 41^{33} \% 55$$

$$= 6$$

$$K = 6$$

$$\begin{aligned} M &= K^e \% N \\ &= 6^{17} \% 55 \\ &= 41 \end{aligned}$$

$$e = 17$$

$$N = 55$$

$$d = 33$$

RSAA(simplified)

RSA (simplified)

Chuck

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

Random $K = 6$

key? \longleftrightarrow e:N = 17:55

Computes $M = K^e \% N$
 $= 6^{17} \% 55$
 $= 41$

Random *nonce* 41,*nonce* \longrightarrow

$$\begin{aligned} K &= M^d \% N \\ &= 41^{33} \% 55 \\ &= 6 \end{aligned}$$

Checks $\text{nonce} = D_K(C)$ ← C

$C = E_K(\text{nonce})$ Computes

- Chuck and Sara *establish* **K = 6** via *key transport*
 - They could use a DH *key agreement* instead

Structure