14

$K = 6$

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

$nonce = D_K(C)$

$C = E_K(nonce)$

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

$$\mathrm{K} = 6$$

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

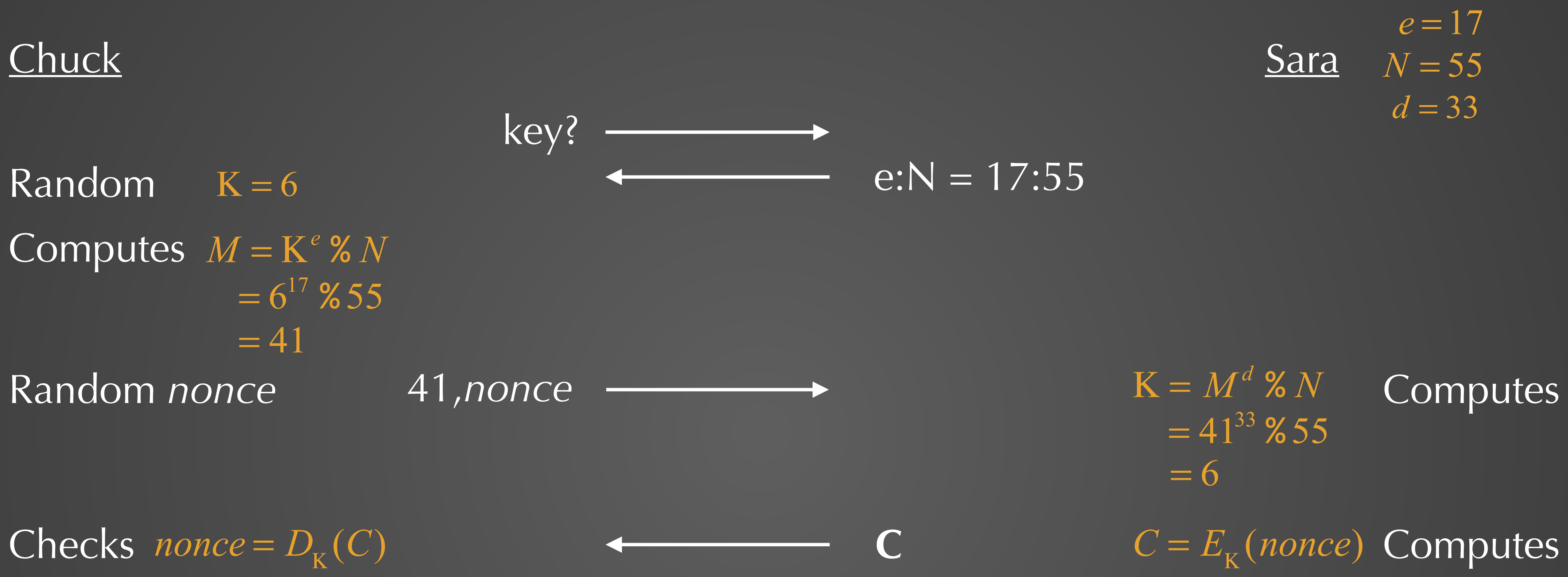
$$e = 17$$

$$N = 55$$

$$d = 33$$

RSA (simplified)

RSA (simplified)



Chuck

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

key? →

Random $\mathrm{K} = 6$

← e:N = 17:55

Computes $M = \mathrm{K}^e \,\%\, N$

$= 6^{17} \,\%\, 55$

$= 41$

Random *nonce*

41,*nonce* →

$\mathrm{K} = M^d \,\%\, N$

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

$= 6$

Computes

Checks $nonce = D_{\mathrm{K}}(C)$

← **C**

$C = E_{\mathrm{K}}(nonce)$ Computes

- Chuck and Sara *establish* $\mathrm{K} = 6$ via *key transport*
    - They could use a DH *key agreement* instead

Structure