14


K = 6

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

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

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

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

$$K = 6$$

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

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

$$= 41$$

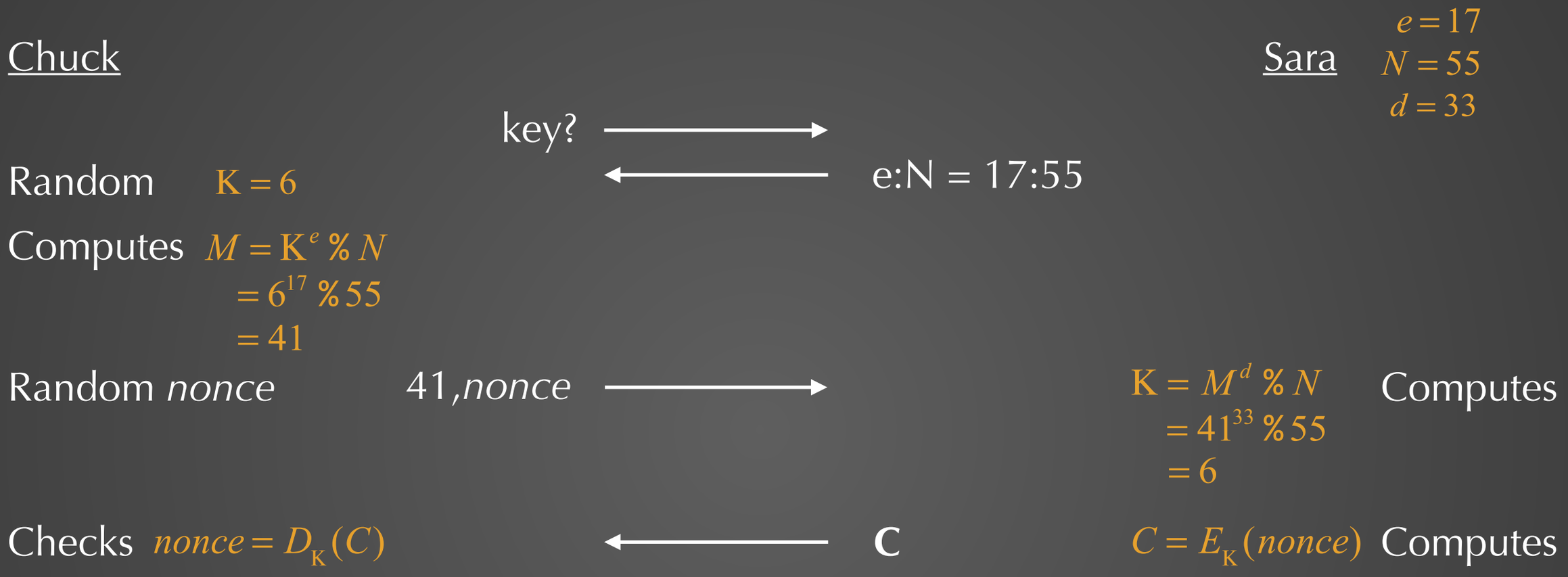
$e = 17$

$N = 55$

$d = 33$

RSA (simplified)

RSA (simplified)



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

Structure