20

$$K = 3$$

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

$$C_s = H(A \mid C_c \mid \mathrm{K}_c)$$

$$C_s = H(A \mid C_c \mid \mathrm{K}_s)$$

$$C_c = H(A|B|\mathrm{K}_c)$$

$$C_c = H(A|B|\mathrm{K}_s)$$

$$\begin{aligned} \mathrm{K} &= (B - g^{x})^{a+x} \,\%\, N \\ &= (9 - 2^{5})^{11+5} \,\%\, 13 \\ &= 3 \end{aligned}$$

$$\begin{aligned} \mathrm{K} &= (Av)^{b} \,\%\, N \\ &= (7 \cdot 6)^{4} \,\%\, 13 \\ &= 3 \end{aligned}$$

$$
\begin{aligned}
b &= 4 \\
B &= v + g^{b} \,\%\, N \\
&= 6 + 2^{4} \,\%\, 13 \\
&= 9
\end{aligned}
$$

$$a = 11$$

$$A = g^a \,\%\, N$$

$$= 2^{11} \,\%\, 13$$

$$= 7$$

$x = 5$

$v = 6$

$x = 5$

$v = 6$

- Chuck keeps (secret) and gives to Sara (verifier)

$x = 5$

$v = g^x \,\%\, N = 2^5 \,\%\, 13 = 6$

- Chuck chooses and calculates

$g = 2, N = 13$

SRP (simplified)

SRP (simplified)

Chuck and Sara agree to use $g = 2, N = 13$ (public)

- Chuck chooses $x = 5$ and calculates $v = g^x \,\%\, N = 2^5 \,\%\, 13 = 6$
  - Chuck keeps $x = 5$ (secret) and gives $v = 6$ to Sara (verifier)

$x = 5$ Chuck			Sara $v = 6$
Random	$a = 11$		$b = 4$ Random
Computes	$A = g^a \,\%\, N = 2^{11} \,\%\, 13 = 7$	Id,7 →	
		← 9	$B = v + g^b \,\%\, N = 6 + 2^4 \,\%\, 13 = 9$
Computes	$\mathrm{K} = (B - g^x)^{a+x} \,\%\, N = (9 - 2^5)^{11+5} \,\%\, 13 = 3$		$\mathrm{K} = (Av)^b \,\%\, N = (7 \cdot 6)^4 \,\%\, 13 = 3$ Computes
Computes	$C_c = H(A \mid B \mid \mathrm{K}_c)$	Cc →	
Checks	$C_s = H(A \mid C_c \mid \mathrm{K}_c)$		$C_c = H(A \mid B \mid \mathrm{K}_s)$ Checks
		← Cs	$C_s = H(A \mid C_c \mid \mathrm{K}_s)$ Computes

- Chuck and Sara *establish* $\mathrm{K} = 3$ via *key agreement*

Structure