



(huck and Sara Actablish

$$C_s = H(A | C_c | K_c)$$

$$C_s = H(A | C_c | K_s)$$

$$C_c = H(A \mid B \mid \mathbf{K}_c)$$

$$C_c = H(A \mid B \mid \mathbf{K}_s)$$

$$K = (B - g^{x})^{a+x} \% N$$

$$= (9 - 2^{5})^{11+5} \% 13$$

$$= 3$$

$$= 3$$

$$K = (Av)^{b} \% N$$

$$= (7 \cdot 6)^{4} \% 13$$

$$= 3$$



$$b = 4$$

$$B = v + g^{b} \% N$$

$$= 6 + 2^{4} \% 13$$

$$= 9$$



$$a = 11$$

$$A = g^{a} \% N$$

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

$$= 7$$



x = 5v = 6 x = 5

v = 6

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

Chuck chooses

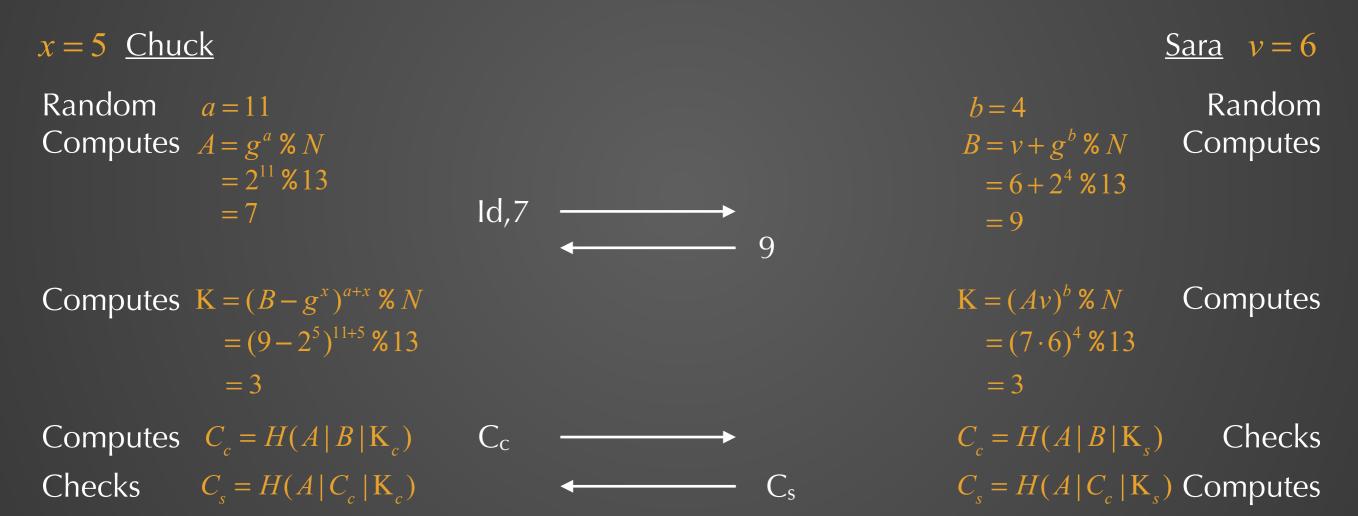
g = 2, N = 13

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)



• Chuck and Sara establish K = 3 via key agreement

Structure