12

- Unauthenticated key agreement
  - Susceptible to Man-in-the-Middle (MitM) attack

g, N **K**

- If Eve knows and captures 6,9 it is difficult* to calculate

$$K = 3$$

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

$$K = B^{a} \% N$$

$$K = 9^{5} \% 13$$

$$K = 3$$

$$K = A^{b} \% N$$

$$K = 6^{8} \% 13$$

$$K = 3$$

$$b = 8$$

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

$$B = 2^{8} \% 13$$

$$B = 9$$

$$a = 5$$

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

$$A = 2^{5} \% 13$$

$$A = 6$$

$$g = 2, \; N = 13$$

Diffie–Hellman

Diffie–Hellman

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

	Chuck		Sara	
Random	$a = 5$		$b = 8$	Random
Computes	$A = g^a \% N$		$B = g^b \% N$	Computes
	$A = 2^5 \% 13$		$B = 2^8 \% 13$	
	$A = 6$		$B = 9$	
		$6 \longrightarrow$		
		$\longleftarrow 9$		
	$\mathrm{K} = B^a \% N$		$\mathrm{K} = A^b \% N$	
	$\mathrm{K} = 9^5 \% 13$		$\mathrm{K} = 6^8 \% 13$	
	$\mathrm{K} = 3$		$\mathrm{K} = 3$	

- Chuck and Sara *establish* $\mathrm{K} = 3$ via *key agreement*
- If Eve knows g, N and captures 6,9 it is difficult* to calculate K
- Unauthenticated key agreement
  - Susceptible to Man-in-the-Middle (MitM) attack

* The DH problem is linked to the discrete logarithm problem

RSA (simplified)