Symmetric key cryptography

- The communication channel is insecure. How can we settle on the key to be used for cryptography over this insecure channel?
- Diffie-Hellman key exchange algorithm (1976)
- p, g: prime numbers. a, b: random numbers

Alice				**Bob**		
Secret	Public	Calculates	Sends	Calculates	Public	Secret
a	p, g		$p,g \longrightarrow$			b
a	p, g, A	$g^a \bmod p = A$	$A \longrightarrow$		p, g	b
a	p, g, A		$\longleftarrow B$	$g^b \bmod p = B$	p, g, A, B	b
a, **s**	p, g, A, B	$B^a \bmod p = s$		$A^b \bmod p = s$	p, g, A, B	b, **s**