## The Intruder-in-the-Middle Attack

Alice	Eve	Bob
a	e	b
$p_A = \alpha^a$	$p_E = \alpha^e$	$p_B = \alpha^b$
$p_A$	$p_A p_B \leftarrow p_A$	$p_B$
$p_E$ $\blacksquare$	$p_E$ $p_E$	$p_E$
$p_E{}^a = \alpha^{ea}$		$p_E{}^b = \alpha^{eb}$
K	$K_1 \equiv p_A^e = \alpha^{ae}  K_2 \equiv p_B^e = \alpha^{be}$	