Alice		Bob
x_A - private key		x_B - private key
$y_A = g^{x_A}$ - public key		$y_B = g^{x_B}$ - public key
$cert_A$ - certificate for y_A		$cert_B$ - certificate for y_B
	MAIN PROCEDURE	
choose a at random		choose b at random
$h_A := H(a)$		$h_B := H(b)$
$c_A := g^{h_A}$	$\xrightarrow{c_A}$	$c_B := g^{h_B}$
	$\xleftarrow{c_B}$	
$K := c_B^{h_A}$		$K := c_A^{h_B}$
$K_A := H(K, 1), K_B := H(K, 2)$		$K_A := H(K, 1), K_B := H(K, 2)$
$K'_A := H(K, 3), K'_B := H(K, 4)$		$K'_A := H(K, 3), K'_B := H(K, 4)$
$r_A := H(c_B^{x_A}, K'_A)$		
	$\xrightarrow{Enc_{K_A}(cert_A, r_A)}$	check $cert_A$, proceed with random values if $r_A \neq H(y_A^{h_B}, K'_A)$
	$\xleftarrow{Enc_{K_B}(cert_B, r_B)}$	$r_B := H(c_A^{x_B}, K'_B)$
check $cert_B$, proceed with random values if $r_B \neq H(y_B^{h_A}, K'_B)$		
$K_{session} := H(K, 5)$		$K_{session} := H(K, 5)$