Clie	ent Ser	ver
	ClientHello ServerHello	1. Client sends 256-bit random number R_b and supported ciphers
(501.022	2. Server sends 256-bit random number R_s and chosen cipher
	Certificate	3. Server sends certificate
*	ServerKeyExchange	4. DH: Server sends $\{g, p, g^a \mod p\}_{K_{\text{server}}^{-1}}$
	ServerHelloDone	5. Server signals end of handshake
+	${ m Client}{ m Key}{ m Exchange}$	6. DH: Client sends $g^b \mod p$ RSA: Client sends $\{PS\}_{K_{\text{server}}}$
	ChangeCipherSpec, Finished	Client and server derive cipher keys C_b, C_s and integrity keys I_b, I_s from R_b, R_s, PS
		7. Client sends $MAC(dialog, I_b)$
	ChangeCipherSpec, Finished	8. Server sends $MAC(dialog, I_s)$
· · ·	Application Data Application Data	9. Client data takes the form $\{M_1, \text{MAC}(M_1, I_b)\}_{C_b}$ 10. Server data takes the form $\{M_2, \text{MAC}(M_2, I_s)\}_{C_s}$