Abbreviations
~X_1 = FIN(tls12_prf(tls12_prf(zero,master_secret,(~M_7939, a_7816)),server_finished,(((((CH(~M_7939,a_7819), SH(a_7816,nego(TLS12,RSA(a_7820),a_7821,a_7814, a_7822))),CRT(~M_8044)),CCS(change_cipher_spec)), CKE(rsa_enc(~M_8044,zero))),FIN(tls12_prf(tls12_prf(zero,master_secret,(~M_7939,a_7816)),client_finished, (~M_7939,a_7816)))))) = FIN(tls12_prf(tls12_prf(zero,master_secret,(cr_7825,a_7816)),server_finished, (((((CH(cr_7825,a_7819),SH(a_7816,nego(TLS12,RSA(a_7820),a_7821,a_7814,a_7822))),CRT(pk(k_7829))), CCS(change_cipher_spec)),CKE(rsa_enc(pk(k_7829), zero))),FIN(tls12_prf(tls12_prf(zero,master_secret, (cr_7825,a_7816)),client_finished,(cr_7825,a_7816))))))
~M_8197 = aead_enc(a_7814,b2ae(tls12_prf(tls12_prf(zero,master_secret,(cr_7825,a_7816)),client_key_expansion, (a_7816,cr_7825))),a_7817,a_7818,secretC2S)

A trace has been found.