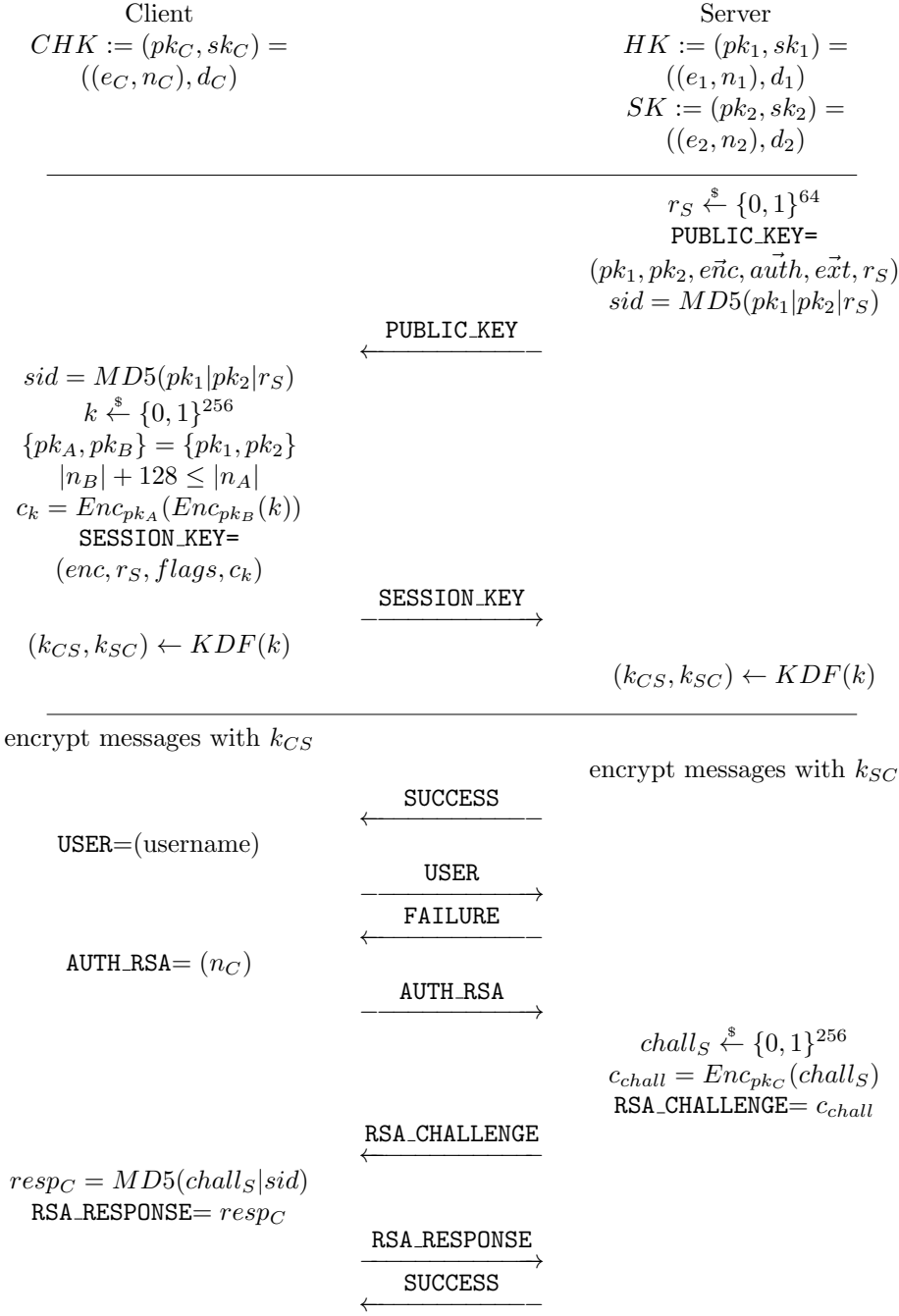
Client
$CHK := (pk_C, sk_C) = ((e_C, n_C), d_C)$
Server
$HK := (pk_1, sk_1) = ((e_1, n_1), d_1)$
$SK := (pk_2, sk_2) = ((e_2, n_2), d_2)$
$r_S \xleftarrow{\$} \{0,1\}^{64}$
PUBLIC_KEY=
$(pk_1, pk_2, \vec{enc}, \vec{auth}, \vec{ext}, r_S)$
$sid = MD5(pk_1|pk_2|r_S)$
PUBLIC_KEY
$sid = MD5(pk_1|pk_2|r_S)$
$k \xleftarrow{\$} \{0,1\}^{256}$
$\{pk_A, pk_B\} = \{pk_1, pk_2\}$
$|n_B| + 128 \leq |n_A|$
$c_k = Enc_{pk_A}(Enc_{pk_B}(k))$
SESSION_KEY=
$(enc, r_S, flags, c_k)$
SESSION_KEY
$(k_{CS}, k_{SC}) \leftarrow KDF(k)$
$(k_{CS}, k_{SC}) \leftarrow KDF(k)$
encrypt messages with k_{CS}
encrypt messages with k_{SC}
SUCCESS
USER=(username)
USER
FAILURE
AUTH_RSA= (n_C)
AUTH_RSA
$chall_S \xleftarrow{\$} \{0,1\}^{256}$
$c_{chall} = Enc_{pk_C}(chall_S)$
RSA_CHALLENGE= c_{chall}
RSA_CHALLENGE
$resp_C = MD5(chall_S|sid)$
RSA_RESPONSE= $resp_C$
RSA_RESPONSE
SUCCESS