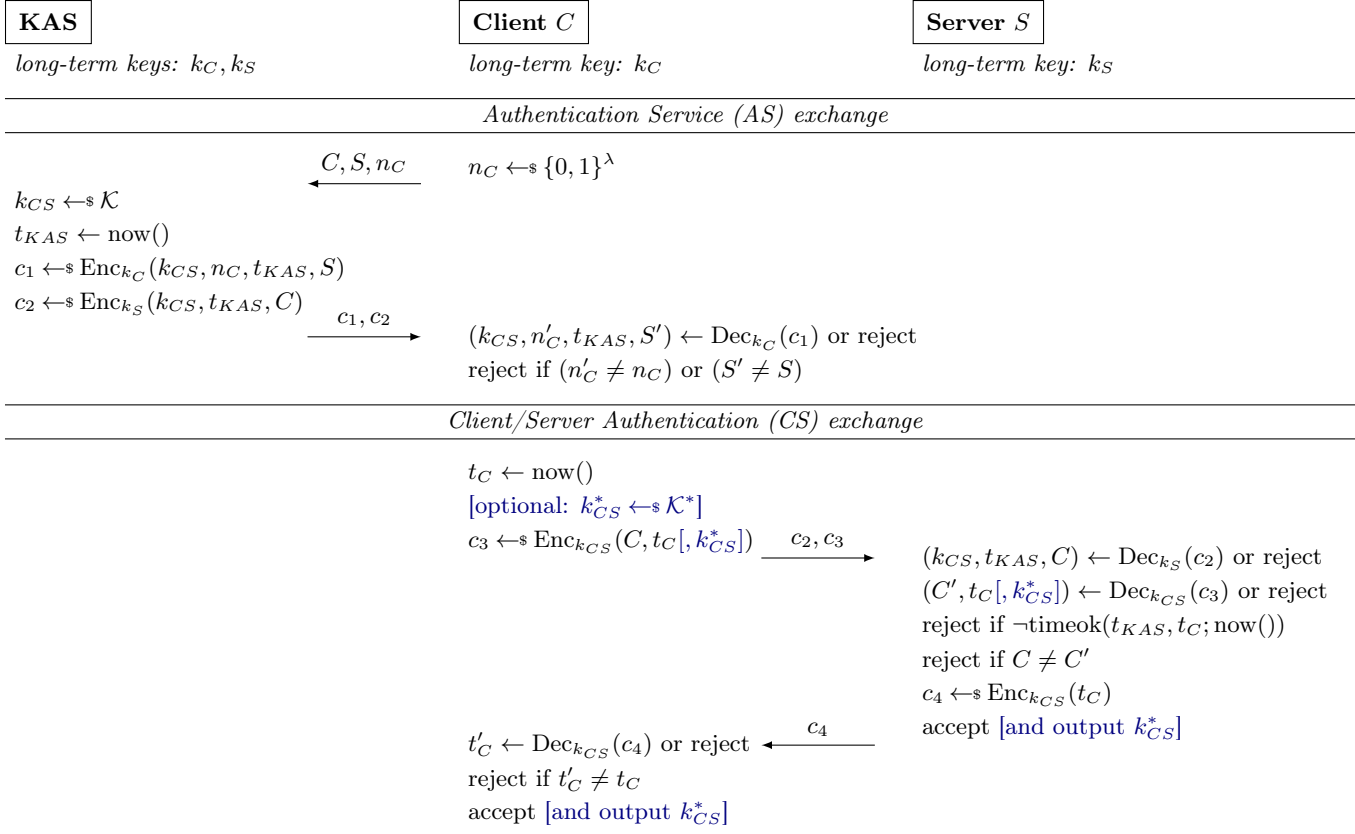
KAS
Client C
Server S
long-term keys: k_C, k_S
long-term key: k_C
long-term key: k_S
Authentication Service (AS) exchange
C, S, n_C
$n_C \leftarrow\!\!\$\ \{0,1\}^\lambda$
$k_{CS} \leftarrow\!\!\$\ \mathcal{K}$
$t_{KAS} \leftarrow \text{now}()$
$c_1 \leftarrow\!\!\$\ \text{Enc}_{k_C}(k_{CS}, n_C, t_{KAS}, S)$
$c_2 \leftarrow\!\!\$\ \text{Enc}_{k_S}(k_{CS}, t_{KAS}, C)$
c_1, c_2
$(k_{CS}, n'_C, t_{KAS}, S') \leftarrow \text{Dec}_{k_C}(c_1)$ or reject
reject if $(n'_C \neq n_C)$ or $(S' \neq S)$
Client/Server Authentication (CS) exchange
$t_C \leftarrow \text{now}()$
[optional: $k^*_{CS} \leftarrow\!\!\$\ \mathcal{K}^*$]
$c_3 \leftarrow\!\!\$\ \text{Enc}_{k_{CS}}(C, t_C[, k^*_{CS}])$
c_2, c_3
$(k_{CS}, t_{KAS}, C) \leftarrow \text{Dec}_{k_S}(c_2)$ or reject
$(C', t_C[, k^*_{CS}]) \leftarrow \text{Dec}_{k_{CS}}(c_3)$ or reject
reject if $\neg\text{timeok}(t_{KAS}, t_C; \text{now}())$
reject if $C \neq C'$
$c_4 \leftarrow\!\!\$\ \text{Enc}_{k_{CS}}(t_C)$
accept [and output k^*_{CS}]
c_4
$t'_C \leftarrow \text{Dec}_{k_{CS}}(c_4)$ or reject
reject if $t'_C \neq t_C$
accept [and output k^*_{CS}]