Initiator
(sk_I, pk_I)

Responder
(sk_R, pk_R)

Negotiation

$\mathsf{cky_I}|0, m_1 = (\overrightarrow{SA})$ $\longrightarrow$

$\longleftarrow$ $\mathsf{cky_I}|\mathsf{cky_R}, m_2 = (SA)$

Key Agreement/Authentication

$\mathsf{cky_I}|\mathsf{cky_R}, m_3 = (g^x, n_I, aux_I)$ $\longrightarrow$

$\longleftarrow$ $\mathsf{cky_I}|\mathsf{cky_R}, m_4 = (g^y, n_R, aux_R)$

Key Derivation

derive k, k_0, k_1, k_2

Encrypted Authentication and Key Confirmation

$\mathsf{cky_I}|\mathsf{cky_R}, c_5$ $\longrightarrow$

$\longleftarrow$ $\mathsf{cky_I}|\mathsf{cky_R}, c_6$