

<p>I → R: CKY_I, OK_KEYX, GRP, g^x, EHAO, NIDP, ID_I, ID_R, N_I, S_{KI}[ID_I ID_R N_I GRP g^x EHAO]</p>
<p>R → I: CKY_R, CKY_I, OK_KEYX, GRP, g^y, EHAS, NIDP, ID_R, ID_I, N_R, N_I, S_{KR}[ID_R ID_I N_R N_I GRP g^y g^x EHAS]</p>
<p>I → R: CKY_I, CKY_R, OK_KEYX, GRP, g^x, EHAS, NIDP, ID_I, ID_R, N_I, N_R, S_{KI}[ID_I ID_R N_I N_R GRP g^x g^y EHAS]</p>

Notation:

I = Initiator
 R = Responder
 CKY_I, CKY_R = Initiator, responder cookies
 OK_KEYX = Key exchange message type
 GRP = Name of Diffie-Hellman group for this exchange
 g^x, g^y = Public key of initiator, responder; g^{xy} = session key from this exchange
 EHAO, EHAS = Encryption, hash, authentication functions, offered and selected
 NIDP = Indicates encryption is not used for remainder of this message
 ID_I, ID_R = Identifier for initiator, responder
 N_I, N_R = Random nonce supplied by initiator, responder for this exchange
 S_{KI}[X], S_{KR}[X] = Indicates the signature over X using the private key (signing key) of initiator, responder

Figure 6.11 Example of Aggressive Oakley Key Exchange