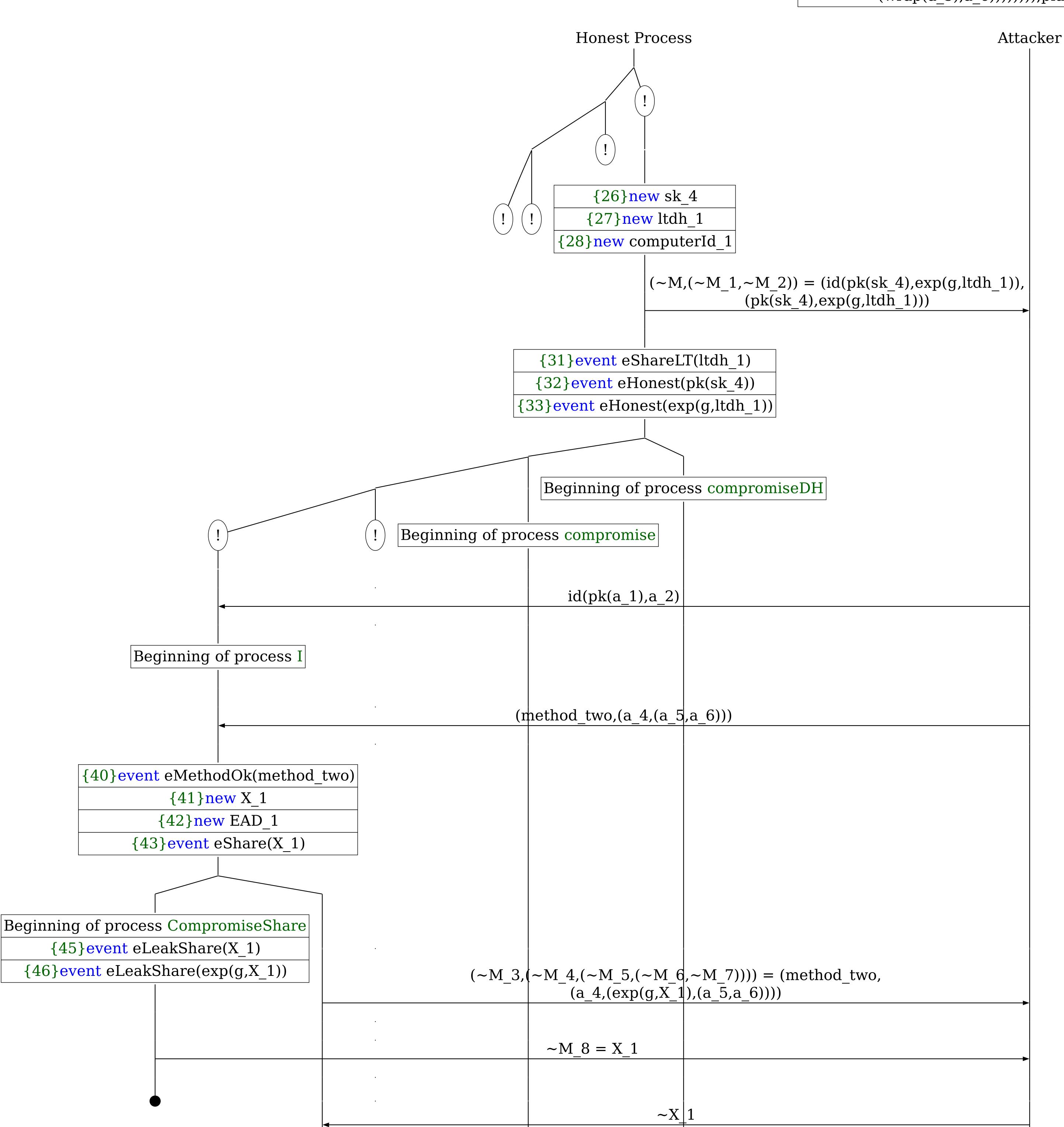
Abbreviations

~X\_1 = (a\_7,encxor((a\_8,(id(pk(a\_1),a\_2),(sign((sSignature1, (id(pk(a\_1),a\_2),(hash((wrap(a\_7),wrap(hash((wrap(method\_two),(wrap(a\_4),(wrap(~M\_5),(wrap(a\_5), a\_6))))))),(pk(a\_1),(a\_9,edhoc\_kdf(hkdfextract(hash((wrap(a\_7),wrap(hash((wrap(method\_two),(wrap(a\_4),(wrap(~M\_5),(wrap(a\_5),a\_6))))))),exp(a\_7, ~M\_8)),stwo,(id(pk(a\_1),a\_2),(hash((wrap(a\_7), wrap(hash((wrap(method\_two),(wrap(a\_4),(wrap(~M\_5), (wrap(a\_5),a\_6))))))),pk(a\_1),a\_9))),hash\_length)))))), a\_10,a\_1),a\_9))),edhoc\_kdf(hkdfextract(hash((wrap(a\_7),wrap(hash((wrap(method\_two),(wrap(a\_4),(wrap(~M\_5),(wrap(a\_5),a\_6))))))),exp(a\_7,~M\_8)),stzero, hash((wrap(a\_7),wrap(hash((wrap(method\_two),(wrap(a\_4),(wrap(a\_4),(wrap(a\_5),a\_6))))))),plaintext\_length)))

A trace has been found.



 $\{117\}$  event eDerivedIShared(exp(g,ltdh\_1),exp(a\_7, X\_1))

hàsh Tength))))), $\bar{a}$  10, $\bar{a}$  1), $\bar{a}$  9))),pk( $\bar{a}$  1), $\bar{b}$ ))

{133}event eAcceptI(computerId 1,method two,exp( g,ltdh 1),pk(a  $\bar{1}$ ),hkdfextract( $\bar{h}$ ash((wra $\bar{p}$ (a 7), wrap(hash((wrap(method two),(wrap(a 4),(wrap(exp( $g,X_1)$ ,  $(wrap(a_5),a_6))))))), <math>exp(a_7,X_1)$ ),  $hkdfextract(a_5)$ edhoc kdf(hkdfextract(hash((wrap(a 7), wrap(hash( (wrap(method two),(wrap(a 4),(wrap(exp(g,X 1)), $(wrap(a 5),a^{\overline{6}})))))))),exp(\overline{a} 7,X 1)),sfive,hash($  $(wrap(hash(wrap(a_7), wrap(hash(wrap(method_two),$ (wrap(a 4),(wrap(exp(g,X 1)),(wrap(a 5),a 6)))))))))((a 8,(id(pk(a 1),a 2),(sign((sSignature1,(id(  $pk(a^{-1})$ , a 2),  $(hash((wrap(a^{-7}), wrap(hash((wrap(a^{-7}), wrap(hash((wrap(hash((wrap(a^{-7}), wrap(hash((wrap(a^{-7}), wrap(hash((wrap(a), wrap(hash((wrap(a), wrap(hash((wrap(a), wrap(hash((wrap(a), wrap(hash((wrap(a), wrap(hash((wrap(a), wrap(hash((wrap(a), wrap(hash((wrap(a), wrap(hash((wrap(hash((wrap(hash((wrap(hash((wrap(hash((wrap(hash((wrap(hash((wrap(hash((wrap(hash((wrap(hash((wwa)), wrap(hash((wwa)), wrap(hash((wwa)), wr$ method two), (wrap(a 4), (wrap(exp(g,X 1)), (wrap(exp(g,X 1))))hash((wrap(a\_7), wrap(hash((wrap(method\_two), (wrap(  $a_4$ ),  $(wrap(exp(g,X_1)), (wrap(a_5), a_6))))))),$  $\exp(a_7,X_1)$ ),stwo, $(id(pk(a_1),a_2)$ , $(hash((wrap(a_1),a_2))$ a 7), wrap(hash((wrap(method two), (wrap(a 4), (wrap(  $\exp(g,X_1),(wrap(a_5),a_6)))))),(pk(a_1),a_9))),$  $\overline{hash} \overline{length}))))), \overline{a} 10, \overline{a} 1), a 9)), pk(\overline{a} 1))),$ hash length), exp(a 7,ltdh 1)), edhoc kdf(hkdfextract( edhoc kdf(hkdfextract(hash((wrap(a 7), wrap(hash(  $(wrap(method two),(wrap(a_4),(wrap(exp(g,X_1)),$  $(wrap(a 5),a^{-}6))))))),exp(\bar{a} 7,X 1)),sfive,hash($ (wrap(hash((wrap(a 7), wrap(hash((wrap(method two)), wrap(hash((wrap(method two))), wrap(hash((wrap(method two)), wrap(hash((wrap(method two)), wrap(hash((wrap(method two)), wrap(hash((wrap(method two)), wrap(hash((wrap(method two)), wrap(hash((wrap(method two)), wrap(hash((ww))), wrap(hash((ww)), wrap(hash((ww))), $(wrap(a_4),(wrap(exp(g,X 1)),(wrap(a 5),a 6)))))))))$  $(\bar{a} \ \bar{8}, (id(pk(\bar{a} \ 1), \bar{a} \ 2), \bar{(sign((sSignature1), id()))})$  $pk(a^{-1})$ ,  $a^{-2}$ ,  $(hash((wrap(a^{-7}), wrap(hash((wrap(a^{-7}), wrap(hash((wrap(a), wrap(hash((wrap(a), wrap(a), wrap(hash((wrap(a), wrap(hash((wrap(a), wrap(hash((wrap(a), wrap(hash((wrap(a), wrap(hash((wrap(a), wrap(hash((wrap(a), wrap(hash((wrap(a), wrap(hash((wrap(hash((wrap((wrap((wrap((wrap((wrap((wrap((wrap((wrap((wrap((w), wrap((w), wrap((w), wrap((w),$  $method_two)$ ,(wrap(a\_4),(wrap(exp(g,X\_1)),(wrap( a 5),a 6))))))),(pk(a 1),(a 9,edhoc kdf( $\overline{h}$ kdfextract( hash((wrap(a\_7),wrap(hash(wrap(method\_two),(wrap( a = 4,  $(wrap(exp(g,X 1)), (wrap(a_5), a_6))))))),$  $\exp(a 7, X 1)$ , stwo, (id(pk(a 1), a 2), (hash((wrap(a 1), a 2), (hash((wrap(a 1), a 2), a 2)))a 7), wrap(hash((wrap(method two), (wrap(a 4), (wrap( hash  $\overline{\text{length}}))))), \overline{\text{a}} 10, \overline{\text{a}} 1), a 9)), pk(\overline{\text{a}} 1), )),$ hash length), exp(a 7,1tdh 1)), sseven, hash((wrap( hash((wrap(hash((wrap(a 7), wrap(hash((wrap(method two), $(wrap(a_4),(wrap(exp(g,X_1)),(wrap(a_5),a_6))))))))$  $((a \ 8,(id(pk(a \ 1),a \ 2),(sign((sSignature1,(id(a \ 1),a \ 2),(sign((sSignature1),(id(a \ 1),a \ 2),(sign((sSignature1),(id(a \ 1),a \ 2),(sign((sSignature1),(id(a \ 1),a \ 2),(sign((sSignature1),(id(a \ 1),a \ 2),(id(a \ 1),a \ 2),(sign((sSignature1),(id(a \ 1),a \ 2),(id(a \ 1),a \ 2),(id(a$ pk(a 1),a 2),(hash((wrap(a 7),wrap(hash((wrap( method two),(wrap(a 4),(wrap(exp(g,X\_1)),(wrap( hash((wrap(a 7), wrap(hash((wrap(method\_two), (wrap(  $a_4$ ),  $(wrap(exp(g,X_1)), (wrap(a_5),a_6))))))),$  $\exp(a 7, X 1)$ , stwo, (id(pk(a 1), a 2), (hash((wrap(a 1), a 2), (hash((wrap(a 1), a 2), a 2)))a 7), wrap(hash((wrap(method two), (wrap(a 4), (wrap(  $\exp(g,X 1)),(wrap(a 5),a 6)))))))))))(pk(a 1),a 9))),$ hash  $[ength])))), \overline{a} 10, \overline{a} 1), a 9)), pk(\overline{a} 1)))),$ ((id(pk(sk 4),exp(g,ltdh 1)),(edhoc kdf(hkdfextract( edhoc kdf(hkdfextract(hash((wrap(a\_7), wrap(hash(  $(wrap(method\ two),(wrap(a\ 4),(wrap(exp(g,X\ 1)),$  $(wrap(a 5),a^{-}6))))))),exp(\overline{a}_{7},X_{1}),sfive,hash($ (wrap(a 4),(wrap(exp(g,X 1)),(wrap(a 5),a 6))))))))) $((a \ 8,(id(pk(a \ 1),a \ 2),\overline{(sign((sSignature 1,(id(s)),a)))}))$ pk(a 1),a 2),(hash((wrap(a 7),wrap(hash((wrap( method two),(wrap(a 4),(wrap(exp(g,X\_1)),(wrap( hash((wrap(a 7), wrap(hash((wrap(method two), (wrap(  $a_4$ ),(wrap(exp(g,X\_1)),(wrap(a\_5),a\_6))))))),  $\exp(a 7, X 1)$ , stwo, (id(pk(a 1), a 2), (hash(wrap(a 7), wrap(hash((wrap(method two), (wrap(a 4), (wrap(  $\exp(g,X 1)),(wrap(a 5),a 6)))))))))))(pk(a 1),a 9))),$  $\overline{\text{hash Tength}}))))), \overline{\text{a}} 10, \overline{\text{a}} 1), \overline{\text{a}} 9)), pk(\overline{\text{a}} 1))),$ hash  $\overline{length}$ ,  $\exp(a \overline{7}, ltdh \overline{1})$ ,  $\overline{ssix}$ ,  $(\overline{id}(p\overline{k}(sk 4), \overline{ssix})$  $\exp(g, \operatorname{Itdh} 1)), (\operatorname{hash}((\operatorname{wrap}(\operatorname{hash}((\operatorname{wrap}(a 7), \operatorname{wrap}($ hash((wrap(method two),(wrap(a 4),(wrap(exp(g, X = 1),  $(wrap(a = 5), \bar{a} = 6)))))))), <math>((a = 8, (id(pk(a = 1), a = 6)))))))$ a 2),(sign((sSi $\overline{g}$ nat $\overline{u}$ re1,(id(pk( $\overline{a}$ 1),a  $\overline{2}$ ),(h $\overline{a}$ sh(  $(wrap(a_7), wrap(hash((wrap(method two), (wrap(a_4), wrap(a_7))))$ (wrap(exp(g,X 1)),(wrap(a 5),a 6))))))),(pk(a 1),(a 9,edhoc kdf(hkdfextract(hash((wrap(a 7),wrap( hash((wrap(method two),(wrap(a 4),(wrap(exp(g, X = 1),  $(wrap(a = 5), a = 6))))))), exp(<math>\bar{a} = 7, \bar{X} = 1$ ), stwo,  $(id(\bar{p}k(a 1), a^2), \bar{(}has\bar{h}((wrap(a 7), wrap(\bar{h}ash((wrap(a 7), wrap(\bar{h}ash((wrap(\bar{h}ash((wrap(\bar{h}ash((wrap(\bar{h}ash((wrap(\bar{h}ash((wrap(\bar{h}ash((wrap(\bar{h}ash((wrap(\bar{h}ash((wrap(\bar{h}ash((wrap(\bar{h}a), wrap(\bar{h}ash((wrap(\bar{h}a), wrap(\bar{h}ash((wrap(\bar{h}a), wrap(\bar{h}ash((wrap(\bar{h}a), wrap(\bar{h}ash((wrap(\bar{h}a), wrap(\bar{h}ash((wrap(\bar{h}a), wrap(\bar{h}a), wrap(\bar{h}ash((\bar{h}a), wrap(\bar{h}ash((\bar{h}a), wrap(\bar{h}ash((\bar{h}a), wrap(\bar{h}ash((\bar{h}a), wrap(\bar{h}a), wrap(\bar{h}ash((\bar{h}a), wrap(\bar{h}a), wrap(\bar{h}ash((\bar{h}a), wrap(\bar{h}a), wrap(\bar{h}ash((\bar{h}a), wrap(\bar{h}a), wrap(\bar{h}a), wrap(\bar{h}a), wrap(\bar{h}ash((\bar{h}a), wrap(\bar{h}a), wrap(\bar{h}a), wrap(\bar{h}a), wrap(\bar{h}a), wrap(\bar{h}a), wrap(\bar{h}a), wrap(\bar{h}a), wrap(\bar{h}a), wra$  $method\_two)$ ,( $wrap(a_4)$ ,( $wrap(exp(g_X_1))$ ,( $wrap(exp(g_X_1))$ ),( $wrap(exp(g_X_1))$ )),( $wrap(exp(g_X_1))$ ),( $wrap(exp(g_X_1))$ )),( $wrap(exp(g_X_1))$ ),( $wrap(exp(g_X_1))$ )),( $wrap(exp(g_X_1))$ )),( $wrap(exp(g_X_1))$ ),( $wrap(exp(g_X_1))$ )),( $wrap(exp(g_X_1))$ )) a 5),a 6))))))),(pk(a 1),a 9))),hash length))))),

 $a_10,a_1),a_9)),pk(a_1))),exp(g,ltdh_1),EAD(1)),$ 

hash length, EAD 1), exp(g, ltdh 1))), hash length),

X 1, a 7