

Abbreviations
$\sim X_1 = \text{aenc}(\text{aenc}((\text{pk}(a_1), \sim M_2), \sim M_1), \sim M_1) = \text{aenc}(\text{aenc}(\text{pk}(a_1), \text{aenc}(\text{aenc}((\text{pk}(\text{ska_1}), \text{aenc}(n, \text{pk}(\text{skb_1}))), \text{pk}(\text{skb_1}))), \text{pk}(\text{skb_1}))), \text{pk}(\text{skb_1})), \text{pk}(\text{skb_1}))$
$\sim X_2 = \text{aenc}(\text{aenc}((\text{pk}(a_3), \text{adec}(\sim M_3, a_1)), \sim M_1), \sim M_1) = \text{aenc}(\text{aenc}((\text{pk}(a_3), \text{aenc}((\text{pk}(\text{ska_1}), \text{aenc}(n, \text{pk}(\text{skb_1}))), \text{pk}(\text{skb_1}))), \text{pk}(\text{skb_1}))), \text{pk}(\text{skb_1})), \text{pk}(\text{skb_1}))$
$\sim X_3 = \text{aenc}(\text{aenc}((\text{pk}(a_5), 2\text{-proj-2-tuple}(\text{adec}(\sim M_4, a_3))), \sim M_1), \sim M_1) = \text{aenc}(\text{aenc}((\text{pk}(a_5), \text{aenc}(n, \text{pk}(\text{skb_1}))), \text{pk}(\text{skb_1})), \text{pk}(\text{skb_1}))$

A trace has been found.

