

Abbreviations
$\sim X_1 = (\sim M_1, 1, a, \text{enc}(a_1, \sim M), \text{hmac}(\text{enc}(a_1, \sim M), 1, a, \sim M))$ $=$ $(\text{sci_A_3}, 1, a, \text{enc}(a_1, \text{kdf}(\text{szk_3}, 1)), \text{hmac}(\text{enc}(a_1, \text{kdf}(\text{szk_3}, 1)), 1, a, \text{kdf}(\text{szk_3}, 1))))$

A trace has been found.

