

Abbreviations
$\sim X_1 = (a_7, \text{encxor}((a_8, (\text{id}(a_1, a_2), (a_9, a_{10}))), \text{edhoc_kdf}(\text{hkdfextract}(\text{hash}((\text{wrap}(a_7), \text{wrap}(\text{hash}((\text{wrap}(\text{method_two}), (\text{wrap}(a_4), (\text{wrap}(\sim M_5), (\text{wrap}(a_5), a_6))))))), \text{exp}(a_7, \sim M_8)), \text{stzero}, \text{hash}((\text{wrap}(a_7), \text{wrap}(\text{hash}((\text{wrap}(\text{method_two}), (\text{wrap}(a_4), (\text{wrap}(\sim M_5), (\text{wrap}(a_5), a_6))))))), \text{plaintext_length})))))) = (a_7, \text{encxor}((a_8, (\text{id}(a_1, a_2), (a_9, a_{10}))), \text{edhoc_kdf}(\text{hkdfextract}(\text{hash}((\text{wrap}(a_7), \text{wrap}(\text{hash}((\text{wrap}(\text{method_two}), (\text{wrap}(a_4), (\text{wrap}(\text{exp}(g_X, 1)), (\text{wrap}(a_5), a_6))))))), \text{exp}(a_7, X_1)), \text{stzero}, \text{hash}((\text{wrap}(a_7), \text{wrap}(\text{hash}((\text{wrap}(\text{method_two}), (\text{wrap}(a_4), (\text{wrap}(\text{exp}(g_X, 1)), (\text{wrap}(a_5), a_6))))))), \text{plaintext_length}))))))$

A trace has been found.

