

Abbreviations
$\sim X_1 = (a_3, \text{encxor}((a_4, \sim M_4, \text{edhoc_kdf}(\text{hkdfextract}(\text{hash}((a_3, \text{hash}((\text{method_four}, a, \sim M_{10}, a_1, a_2))))), \text{kemdecap}(a_3, \sim M_{13})), \text{sfour}, (\sim M_4, \text{hash}((a_3, \text{hash}((\text{method_four}, a, \sim M_{10}, a_1, a_2))))), \sim M_5, a_5, \text{hash_length}), a_5), \text{edhoc_kdf}(\text{hkdfextract}(\text{hash}((a_3, \text{hash}((\text{method_four}, a, \sim M_{10}, a_1, a_2))))), \text{kemdecap}(a_3, \sim M_{13})), \text{stwo}, \text{hash}((a_3, \text{hash}((\text{method_four}, a, \sim M_{10}, a_1, a_2))))), \text{plaintext_length})))$ $= (a_3, \text{encxor}((a_4, \text{id}(\text{pk}(\text{sk}_5), \text{ltdh}_3, \text{kempk}(\text{sk_auth_kem}_3)), \text{edhoc_kdf}(\text{hkdfextract}(\text{hash}((a_3, \text{hash}((\text{method_four}, a, \text{kempk}(X_1), a_1, a_2))))), \text{kemdecap}(a_3, X_1)), \text{sfour}, (\text{id}(\text{pk}(\text{sk}_5), \text{ltdh}_3, \text{kempk}(\text{sk_auth_kem}_3)), \text{hash}((a_3, \text{hash}((\text{method_four}, a, \text{kempk}(X_1), a_1, a_2))))), \text{pk}(\text{sk}_5), a_5, \text{hash_length}), a_5), \text{edhoc_kdf}(\text{hkdfextract}(\text{hash}((a_3, \text{hash}((\text{method_four}, a, \text{kempk}(X_1), a_1, a_2))))), \text{kemdecap}(a_3, X_1)), \text{stwo}, \text{hash}((a_3, \text{hash}((\text{method_four}, a, \text{kempk}(X_1), a_1, a_2))))), \text{plaintext_length})))$

A trace has been found.

