

trojan message plaintext

length
topic
payload
padding

bytes

2

32

≤ 4030

$4030 - \text{len}(\text{payload})$

encrypt

trojan chunk

address

32

span

8

nonce

32

trojan message ciphertext

4064

headers

BMT
hash