Q1

a. 2^40 / 2^20 = 2^20
   = 1,048,576s
   ≈ 17,476.26min
   ≈ 291.27h
   ≈ 12days
   ∴ At most 12days
b. 2^80 / 2^20 = 2^60
   = 1,152,921,504,606,846,976s
   ≈ 19,215,358,410,114,116.27min
   ≈ 320,255,973,501,901.94h
   ≈ 13,343,998,895,912.58days
   ≈ 36,558,901,084.69years
   ∴ At most ↑ years

Q2

The client generates a random nonce and sends it to the server along with its public key. After receiving the request, the server generates a fresh session key and a timestamp, then uses symmetric encryption to encrypt the long message together with the anti-replay fields, and computes a MAC. Next, the server encrypts the session key with the client's public key and returns the response. After receiving the response, the client decrypts the session key using its private key, verifies the MAC, decrypts the ciphertext using the session key, and performs anti-replay checks.