Cipher block chaining with unique nonce: key = (k,k_1)

unique nonce means: (key, n) pair is used for only one message