CO21BTECH11002
Aayush Kumar

Method:

A for loop is run in range 0 to 1<<20. In each iteration, a key is generated using the expandKey function. In ith iteration, i is shifted left by 4 bits (since last 4 bits are ignored for key generation) and used as input in the expandKey function. Then for each iteration, we check if encryption of the given message using the key is the same as the given cipher text. If they are the same, then we have found the key, hence, we break the loop.

Results:

Key = 8e94635ae87bde371e30e71d3b6b516e

Secret Message = mediumaquamarine