Quiz 8

309552026

鄭偉丞

1. 三種 key 長度不同的 AES 加密法除了使用的密鑰長度不同，會造成破解難度的差異，key 越長越難破解。除此之外，加密迴圈的次數也有差異，128 bits: 10 次，192 bits: 12 次，256 bits: 14 次，加密迴圈的次數越多，安全性越高，但執行加解密所需的時間越長。目前 AES 加密還沒有被破解，但一些高機密的政府資料等，均不建議使用 128 bits 的 AES 演算法。

2. EXTRA CREDIT:
   在加密迴圈次數相同的情況下，使用的密鑰長度越長，安全性越高，但密鑰長度過長會導致加解密所花的時間過長，若因此而降低加密迴圈的次數，則較長的密鑰的安全性並不一定比較高。