Lab3-2

資工四 B04902103 蔡昀達

1. Intermediate 選最後一步的 Add Round Key。Ciphertext⊕Last Round Key。
2. Reverse key schedule. K43-40 為已知，k39=k43⊕k42 以此類推，每四步做一次 Sbox 和 Round Constant 的非線性轉換。
3. 使用 numpy 計算兩矩陣 columnwise correlation 達到加速，並沒有使用平行或 gpu 加速。