**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。