1. 凱薩加密法(Caesar Cipher)

凱薩加密法是一種非常簡單的加密技術,將 A-Z 用 1-26 表示,平移一個距離後就會得到密文。

例如明文為:

THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG 平移量為 1 時密文為:

UIF RVJDL CSPXO GPY KVNQT PWFS UIF MBAZ EPH 解密只需將平移量改為-1,即可得到明文:

THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG

現在我們希望將這個密碼破解難度上升,利用一組數字當作加密,

假設金鑰為: "20180109"

每個字元(包含空格)的平移量依序為 2, 0, 1, 8, 0, 1, 0, 9, ... 一直循環到文字結束。

明文:

THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG 經過"20180109"加密後:

VHF QVILM CZOXN HOY JVMYU PDES CJE TAAY FOH 每個字元的平移量為:

2018010920180109201801092018010920180109201

現在用你的學號當作金鑰,加密一段只包含大寫 A-Z 與空白的英文句子並能解密。