**2018網路安全專題作業Demo**

**巴斯卡平均母音換位加密法**

組員：a1045528 王彥翔

a1045518 陳佳睿

a1045526俞建玨

a1045503 趙普

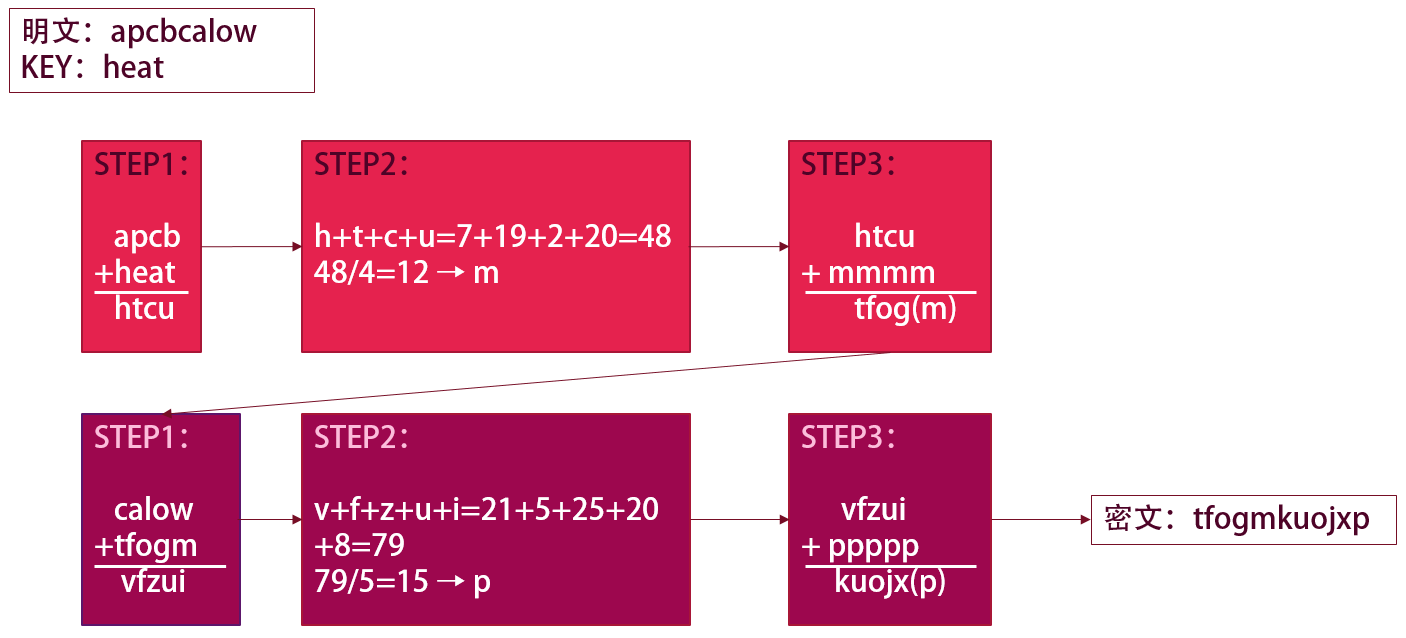
1. **加密過程：**
2. 平均部分：每一段與key作凱薩加密的密文換算數字算一次平均數，如有小數就無條件捨去，結果作為標準將密文做一次平移，並將該數放至加密結果後方做為下一次加密的key，依此類推。例如：

明文：apcbcalow

key：heat

1. 先將apcd與heat相加，結果為htcu
2. 並且將htcu進行平均算出為12，為m
3. 將加密出來的結果htcu再平移m，並且將m加入密文最後一位元
4. 再將後半部明文calow與tfogm相加，算出為vfzui
5. 並且將vfzui進行平均算出為15，為p
6. 將加密出來的結果vfzui再平移p，並且將p加入密文最後一位元
7. 得出密文：tfogmkuojxp

(步驟如下圖所示)



1. 母音換位：設立一個flag，其值可能為0或1，初始設值為0，當遇到母音時將flag值翻轉一次，在flag=1的區塊內，將其區域內依照開頭母音去母音換位表查看相對應數字N，並且以N個字元為一組進行反轉。例如：

假設密文為：abcdefkkjk

經過換位後將會變成：acbdefkkjk

(步驟如下圖所示)



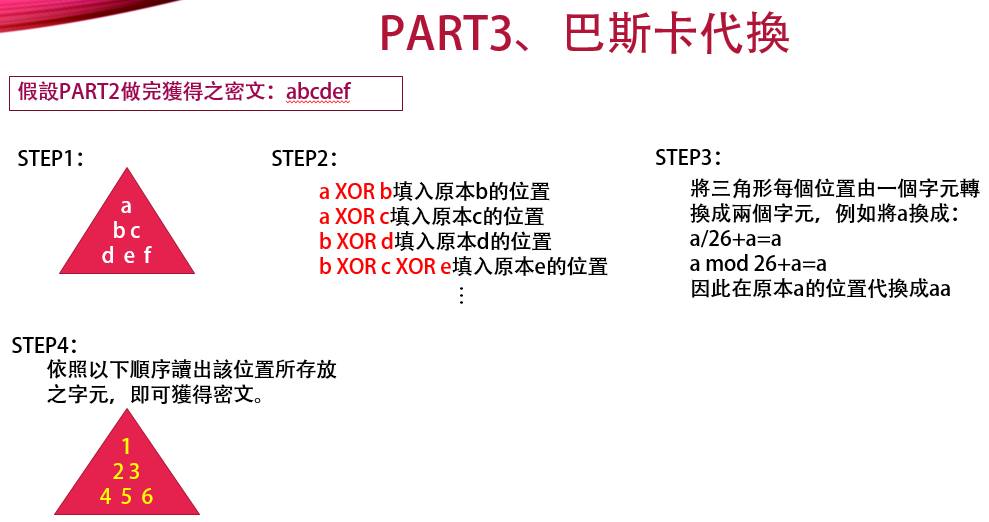
1. 巴斯卡三角形

* 巴斯卡三角形(舊)：把原文填入巴斯卡三角形，上下分支作XOR，結果取代下位，依序做至三角形底層，為避免XOR導致overflow(超過26)，因此在XOR後會存成/26以及mod26的兩個英文字母，而第一位的(最上層)為了加密的一致性,直接進行除以26以及mod26。例如：

假設密文為：abcdef

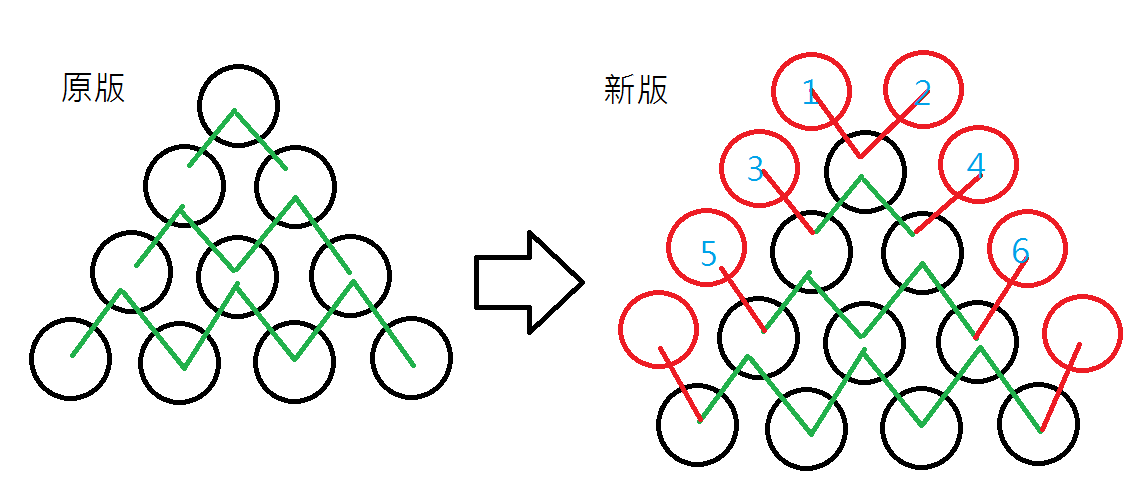
經過代換後將會變成：aaabacafaaah

(步驟如下圖所示)



* 巴斯卡三角形(新)：把原文填入巴斯卡三角形，外圍圍上key，確保每個元素都會XOR2次，結果存成/26以及mod26的兩個英文字母，依序做至三角形底層

(新版巴斯卡三角形加密圖示如下)



註:黑圈為明文，紅圈為KEY，KEY的順序為1.2.3.…..key.size()

1. **加密原理**

* 平均部分：原始的auto key加密方式最常見破解方式就是利用同一位置不同輪迴區域做重複的判定，對此則利用平均數加長密文，使其不易找出key的位元數，也不好定位同位置不同輪迴的位元。
* 母音換位：尋找兩個標記(母音)，把其之間字元依照對照表分類互換，達到換位效果。
* 巴斯卡三角形(舊)： 利用跳位元的形式密文間XOR，打亂密文內容、順序。
* 巴斯卡三角形(新)：利用跳位元並混雜key加密的形式XOR密文，可使攻擊方不意建立原始三角形，且需猜測key為何才能進行原始三角形重建。

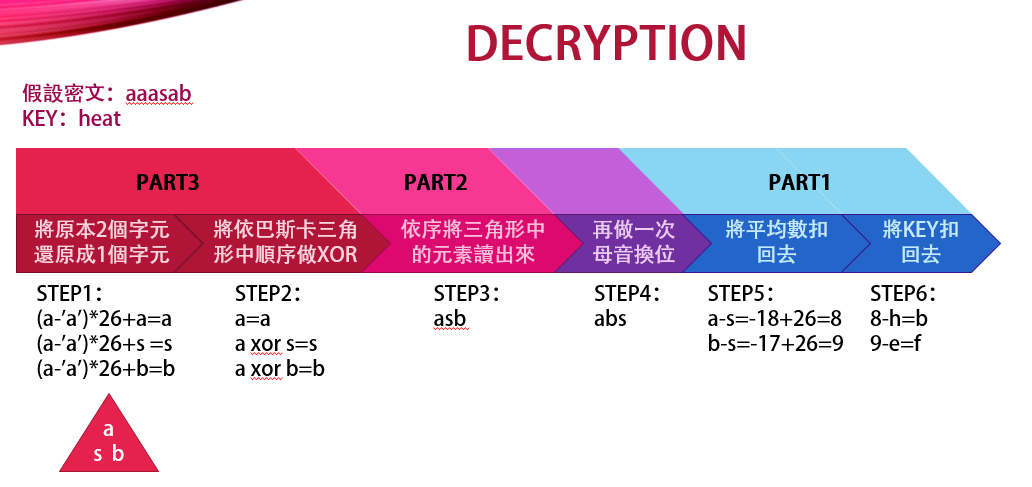
1. **解密過程**

* 平均部分：從最前面開始，先把作為標記的平均數拿去減密文，再把結果減去key，下一段也是類似做法，先減去平均，再把前一段密文拿來減這段密文取得明文，依此類推至結束。
* 母音換位：跟加密方式一樣，再做一次同步驟。
* 巴斯卡三角形：將密文2個一組合併後與key填至增大版三角形，從由上而下XOR

解密原理

* 平均部分：其實就是把原先的結果反著做回來，加key的地方變減key，加平均變減平均，並移除作為標記的平均數使位元數回歸正常。
* 母音換位：尋找兩個標記(母音)，把其之間字元依照對照表分類互換。
* 巴斯卡三角形：加密從上至下加密，依舊由上而下解密

(如下圖所示)



1. **範例：**

M：sayhellotohimforme

K：noproblem

加密結果：

(old)atarasaoafabakaaavaoavazamaxazatalaeawar

(new)aqbeadaaafaaabaaavakazazamaxaubdalaeawar

1. **加解密系統評估：**

* space：字元加會逐漸增加，正相關於K與M的比值，
* time：

1. 第一個平均的部分在O(n)的時間便可以完成加密。
2. 第二個部分先經過一次flag轉換花費O(n)，接著再跟據flag進行換位，平均時間落在O(n)，故第二階段也只需要O(n)+O(n)=O(n)的時間複雜度。
3. 第三個部分只要遍歷過一次array，每到一個點判斷其要填入自己與他點的XOR值為多少，整體時間複雜度為O(n)。

綜合以上三點，整體時間複雜度為O(n)。

* key：key的長度為固定值，且不需要很長，因為會重複利用密文當作key不斷進行加密，方便使用者記憶。

1. **創造程度：方法有3種分3層**

* 平均部分：似auto key加密方式，但有根據它的缺點進行改進，以增加破解難度。
* 母音換位：透過英文文本處理啟發，來想出此換位。
* 巴斯卡三角形：由數學上二項式係數表示法獲得靈感，進而依照此結構進行加密，將密文2個一組合併後與key填至增大版三角形，從由上而下XOR。

1. **安全性：**

* 運用代換-換位交錯加密，確保最基礎之安全性質。
* (舊版本)在未知加密方式下須破解三層；如已經知道加密方式，則只需考慮平均數部分，利用平均數加長密文，使其不易找出key的位元數，也不好定位同位置不同輪迴的位元，迴避直接攻擊同一位置的方式，但若猜測到key的長度，仍然可以利用密文兩字源之間數字對照的差值進行分析，找到同一位元來推出整個明文。
* (新版本)前半部如舊版本所述，但巴斯卡三角形部分密文與key再做XOR，將原本密文與key混雜創造出新的密文，增加攻擊難度。