Intro. to Computer Security Homework 1

Brute-force attack

1. **請設計一個暴力破解的演算法,可以列舉出所有 4 位數密碼（包含大小寫英文、數字）,並寫出該演算法的虛擬碼**

   我們可以利用四個階層的迴圈，分別列舉所有可能的字元，再將四個字元串接在一起：

   - Pseudocode -

```
Let A[1…62] = [a,b,c,d,e,f,g,h,i,j,k,l,m,n,o,p,q,r,s,t,u,v,w,x,y,z,
                A,B,C,D,E,F,G,H,I,J,K,L,M,N,O,P,Q,R,S,T,U,V,W,X,Y,Z,
                0,1,2,3,4,5,6,7,8,9]
for h = 1…62
    for i = 1…62
        for j = 1…62
            for k = 1…62
                output concatenation of A[h] A[i] A[j] A[k]
```

   - Python example -

```
import string
A = string.ascii_letters + string.digits
for h in A:
    for i in A:
        for j in A:
            for k in A:
                print h+i+j+k
```

2. **請說明如何防範暴力破解法？**

   暴力破解法是透過愈來愈強大的電腦運算，以求快速嘗試所有密碼來進行破解。若要防範，可以透過延長時間，讓嘗試所有可能無法在短時間內完成，或者可以阻止不斷嘗試的行為。

   - 加長密碼長度，使所有組合數變多。
   - 增加密碼的字元種類，使所有組合數變多。
   - 輸入錯誤後延遲一段時間才可再次嘗試，甚至可以把延遲時間不斷延長。
   - 若多次密碼錯誤，則可加入 CAPTCHA 等驗證碼，防止自動嘗試，並延長時間。
   - 定期更換密碼，在所有組合被試完前，密碼就改變了。
   - 網站登入錯誤多次則封鎖 IP 一段時間。
   - 輸入錯誤多次則封鎖帳號一段時間，或者甚至要求用人工方法重啟帳號。
   - 限制只能從特定 IP 登入你的帳號。
   - 除了密碼之外，增加其他比較難暴力破解的驗證。如 Google 的 2-step verification，每次登入前還得輸入從簡訊傳來的驗證碼。