Quiz4

Department: 資工系 **Student ID:110550126** **Name:**曾家祐

1. Data compression is often used in data storage and transmission. Suppose you want to use data compression in conjunction with encryption. Does it make more sense to:

A) Compress then encrypt

壓縮的基本原理是將文件中重複出現的位元(文字)，以新的代碼表示，並將這些代碼和原本的位元編成 dictionary，以此達到壓縮文件的效果，但若是先進行加密，可能會讓編碼相比於加密前更加無序混亂，使得壓縮時，無法找到夠多重複出現的位元，讓壓縮得效果不好。而先壓縮後，並不會對加密造成太大的影響。

因此，先進行加密再壓縮是較為合理的作法。

2. Let G:01^n be a secure PRG. Which of the following is a secure PRG (there is more than one correct answer):

D) G'(k) = G(k ⊕1^1)　把 keyword 先 inverse 不會影響安全性

E) G'(k) = G(k) ⊕ 1^n　把結果 inverse 不會影響安全性

F) G'(k) = reverse(G(k)) 把 keyword 相反不會影響安全性

Secure PRG 必須要是不可預測的，因為原本的 G(k)是 secure PRG，所以以上三個也都會是不可預測的 secure PRG。

而下面三個則是有規律而非隨機，因此可以被預測，所以不是 secure PRG。

A) G'(k) = G(k)||0　如果 LSB 被攻擊者得知，它們可以選擇一個 receiver 來解密

B) G'(k) = G(k)||G(k) 重複出現不符合 secure PRG 的規則

C) G'(k) = G(0)　keyword = 0 可以被攻擊者得知，因此並不安全

3. Let b a secure PRG. Define where ^ is the bit-wise AND function. Consider the following statistical test A on . outputs LSB(x), the last significant bit of x. What is Adv PRG [A,G']? You may assume that LSB[G(k)] is 0 for exactly half the seeds k in K.

Ans:0.25

Since LSB[G(k)] = 0 is 0.5 → LSB[G(K)] = 1 is 1-0.5= 0.5.
LSB[G(k1)] and LSB[G(k2)] both be 1 is 0.5*0.5 = 0.25

4. Ans: C) p1 = (k1,k2), p2 = (k1', k2), p3 = (k2')

p1 and p2 can use k1 and k1' to derive k to decrypt
p2 and p3 can use k2 and k2' to derive k to decrypt
p1 and p3 can use k2 and k2' to derive k to decrypt

other 4 can't be the solution since:

A) Can't derive k with p2 = (k1') and p3 = (k2')
B) P2 = (k2,k2') p2 can derive k by itself
D) Can't derive k with p2 = (k1',k2') and p3 = (k2')
E) Can't derive k with p1 = (k1,k2) p2 = (k1,k2)