Cryptograpy Engineering Quiz 4

Problem Description

- Total four questions, and please provide explaination of the answer you give.
- Submission: `{YOUR_STUDENT_ID}.pdf` with the answer to each question and the corresponding explaination for why you opt to the choices you made.

Question

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
   B) The order does not matter -- either one is fine
   C) The order does not matter -- neither one will conpress the data
   D) Encrypt then compress

2. Let $G : 0,1^n$ be a secure PRG. Which of the following is a secure PRG (there is more than one correct answer):
   A) $G'(k) = G(k)||0$ **(Here** $||$ **denotes concatenation)**
   B) $G'(k) = G(k)||G(k)$ **(Here** $||$ **denotes concatenation)**
   C) $G'(k) = G(0)$
   D) $G'(k) = G(k \oplus 1^1)$
   E) $G'(k) = G(k) \oplus 1^n$
   F) $G'(k) = \text{reverse}(G(k))$**, where reverse(x) the string x so that the first bit of x is the last bit of reverse(x). The second bit of x is the second to last bit of reverse(x). And so on.**

3. Let $G : K \to 0,1^n$ b a secure PRG. Define $G'(k_1, k_2) = G(k_1)\hat{}G(k_2)$ where ^ is the bit-wise AND function. Consider the following statistical test A on $0,1^n$. $A(x)$ 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.

```
Note: Please enter the advantage as a decimal between 0 and 1 with a leading 0. If
the advantage is 3/4, you should enter it as 0.75
```

4. Let E, D be a one-time semantically secure cipher with key space $K = 0,1^l$. A bank wishes to split a decryption key $k \in 0,1^l$ into two pieces p_1 and p_2 so that both are needed for decryption. The piece p_1 can be given to one executive and p_2 to another so that both must contribute their pieces for decryption to proceed.
   The bank generates random k_1 in $0,1^l$ and sets $k' \leftarrow k \oplus k_1$. The bank can give k_1 to one executive and k'_1 to another. Both must be present for decryption to proceed since, by itself, each piece contains no information about the secret key k (note that each piece is a one-time pad encryption of k).
   Now, suppose the bak wants to split k into three pieces $p_1,\ p_2,\ p_3$ so that any two of the pieces enable decryption using k. This ensures that even if one executive is out sick, decruption can still succeed. To do so the bank generates two random pairs $(k_1,\ k'_1)$ and $(k_2,\ k'_2)$ as in the previous

paragraph so that $k_1 \oplus k_1' = k_2 \oplus k_2'$. How should the bank assign pieces so that any two pieces enable decryption using k, but no single piece can decrypt?

A) $p_1 = (k_1, k_2),\ p_2 = (k_1'),\ p_3 = (k_2')$

B) $p_1 = (k_1, k_2),\ p_2 = (k_2, k_2'),\ p_3 = (k_2')$

C) $p_1 = (k_1, k_2),\ p_2 = (k_1', k_2),\ p_3 = (k_2')$

D) $p_1 = (k_1, k_2),\ p_2 = (k_1', k_2'),\ p_3 = (k_2')$

E) $p_1 = (k_1, k_2),\ p_2 = (k_1, k_2),\ p_3 = (k_2')$