Problem 0

1. Name: Jubeen Shah
2. Graduate Student
3. What is your experience/comfort with:
   (a) **Mathematical proofs:** Not ver comfortable
   (b) **Elementary probability theory:** Comfortable
   (c) **Analysis of algorithms:** Taking the algorithms course this semester
   (d) **Complexity theory, including big-O notation and NP completeness:** Taking the algorithms course this semester which should help later

Problem 1: Perfect Security and One-time Pad

1. Let $M = \{0, 1, 2, 3\}$ (messages are uniform). The key space is K (chosen uniformly) from $K = \{0, 1, 2, 3, 4\}$.

$$Enc(k, m) = k + m \mod 4$$

$$Dec(k, c) = c - k \mod 4$$

Is this correct and perfectly secure?

Solution 1.1: Messages along with the key used, the encrypted cipher text and the message decrypted is given below.

Message: 0	Key: 0	Cipher : 0	Message: 0
Message: 0	Key: 1	Cipher : 1	Message: 0
Message: 0	Key: 2	Cipher : 2	Message: 0
Message: 0	Key: 3	Cipher : 3	Message: 0
Message: 0	Key: 4	Cipher : 0	Message: 0
Message: 1	Key: 0	Cipher : 1	Message: 1
Message: 1	Key: 1	Cipher : 2	Message: 1
Message: 1	Key: 2	Cipher : 3	Message: 1
Message: 1	Key: 3	Cipher : 0	Message: 1
Message: 1	Key: 4	Cipher : 1	Message: 1
Message: 2	Key: 0	Cipher : 2	Message: 2
Message: 2	Key: 1	Cipher : 3	Message: 2
Message: 2	Key: 2	Cipher : 0	Message: 2
Message: 2	Key: 3	Cipher : 1	Message: 2
Message: 2	Key: 4	Cipher : 2	Message: 2
Message: 3	Key: 0	Cipher : 3	Message: 3
Message: 3	Key: 1	Cipher : 0	Message: 3
Message: 3	Key: 2	Cipher : 1	Message: 3
Message: 3	Key: 3	Cipher : 2	Message: 3
Message: 3	Key: 4	Cipher : 3	Message: 3

For a Encryption Scheme *(Gen, Enc, Dec)* to be perfectly secure, there are a few conditions that need to be met.

1. $Pr[C = c|M = m] = Pr[C = c]$
2. $Pr[C = c|M = m_0] = Pr[C = c|M = m_1]$
3. $Number\ of\ Keys \geq Number\ of\ Message \geq Number\ of\ Cipher\ Text$; or

4. *Number of Keys = Number of Message = Number of Cipher Text* (Shannon's Theorem)

(c) condition is met, since we have
$M = \{0, 1, 2, 3\}$
$K = \{0, 1, 2, 3, 4\}$
$C = \{0, 1, 2, 3\}$

Looking at the output of the *cipher text* and *messages* it can be said that for any given value of the *cipher text* or *message* both conditions (a) and (b) are met. i.e., the probability of cipher text c_x being of m_0 or m_1 or m_2 or m_3 is equal.

Since, conditions (a), (b), and (c) are met with, and every pair of $(cipher\ text, message)$ has a unique key, we can say that the encryption scheme is **perfectly secure**.

2. Suppose we have a variation of the one-time pad in which the message space $M = \{0,1\}^n$ but the key space K is limited to all n-bit strings with an even number of 1's. Give an example of an n, m_0, m_1 for which, given c, anyone may determine whether m_0 or m_1 was encrypted.

Solution 1.2: Let's assume, the following values for $n,\ m_0,\ m_1$, and c respectively.

$n = 3$
$m_0 = 100$
$m_1 = 101$
$c = 111$

So if we XOR the the messages with the cipher text, we should get some key k_0 and k_1

$k_0 = m_0 \oplus c = 100 \oplus 111 = 011$
$k_1 = m_1 \oplus c = 101 \oplus 111 = 010$

The key thus be either be *011* or *010*. That is, both (k_0, m_0, c) and (k_1, m_1, c) have equal probability of being the key used to encrypt message m1 and m2.

We can eliminate one of the tuple (k_0, m_0, c) or the tuple (k_1, m_1, c) because as per the question we have that the key has **even number of 1s**, therfore *010* cannot be the key and know that m_0 was encrypted.

Problem 2: PRG

Let G be a pseudorandom generator with expansion factor $\ell(n) > 2n$. In each of the following cases, say whether G' is a PRG. If yes, show a proof. If no, show a counterexample.

1. $G'(s) = G(s_1, \ldots, s_{\lfloor n/2 \rfloor})$ where $s = s_1, \ldots, s_n$.

Solution 2.1 We have the following Pseudo-Random Generator

$$G'(s) = G(s_1, \ldots, s_{\lfloor n/2 \rfloor}) \text{ where } s = s_1, \ldots, s_n$$

Theorem: If G is a PRG, then $G'(s) = G(s_1, \ldots, s_{\lfloor n/2 \rfloor})$ is a PRG.

Proof: Assume that G' is not a PRG. Then $\exists$ PPT algorithm D who distinguishes

$$|Pr[D(y) = 1 | y \leftarrow G'(s)] - Pr[D(y) = 1 | y \leftarrow_{\$} \{0,1\}^n]| = \varepsilon(n)$$

Where $\varepsilon(n)$ is a non-negligible function.
Now we will create a distinguisher D' which will simulate D.

1. Given input y to D', $|y| = \{0,1\}^{\ell(\lfloor \frac{n}{2} \rfloor)}$, where the expansion factor $\ell(\lfloor \frac{n}{2} \rfloor)$ can be assumed to be Z
2. Give y to D to distinguish
3. Output $D(y)$. That is, output whatever D outputs on y as input.

Case Analysis: For when $y = G'(s)$ and $y = \{0,1\}^n$

1. If $y = G'(s)$ for some seed s for $s \in \{0,1\}^{\lfloor \frac{n}{2} \rfloor}$, since D' outputs the same as D we have the following:

   $$Pr[D'(s) = 1 | T \leftarrow G'(s) | s \in \{0,1\}^Z]$$

   We have that

   $G(s_0, s_1, \ldots, s_{\lfloor \frac{n}{2} \rfloor})$ where input length is $\dfrac{n}{2}$ means that $G(s_0, s_1, \ldots, s_{\lfloor \frac{n}{2} \rfloor})$ is of length Z

   We also have that

   $G'(s_0, s_1 \ldots, s_n) = G(s_0, s_1, \ldots, s_{\lfloor \frac{n}{2} \rfloor})$ which means that $G'(s_0, s_1 \ldots, s_n)$ is of length Z.

Therefore we can write that

$$Pr[D'(s) = 1 | T \leftarrow G'(s) | s \in \{0,1\}^Z] = Pr[D'(y) = 1 | y \leftarrow G(s) | s \in \{0,1\}^n] \tag{1}$$

2. If $y \leftarrow_{\$} \{0,1\}^n$ then y will be taken from a truly random distribution. Therefore we have that

$$Pr[D'(y) = 1 | y \leftarrow_{\$} \{0,1\}^n] \tag{2}$$

Thus, the difference in Equation *2* and *1* gives us

$$|Pr[D'(y) = 1 | y \leftarrow G(s) | s \in \{0,1\}^n] - Pr[D'(y) = 1 | y \leftarrow_{\$} \{0,1\}^n]| = \varepsilon(n)$$

Since we assumed that $\varepsilon(n)$ was a non-negligible function this would mean that D' is a distinguisher for G that distinguishes with non-negligible probability. Since G is a PRG, this would be a contradiction. Hence $G'(s) = G(s_1, \ldots, s_{\lfloor n/2 \rfloor})$ is a PRG

1. $G'(s) = G(s)||G(s')$, where $s' = s_1, s_2, \ldots, s_{n-1}, \bar{s}_n$ [1] [2]

Solution 2.2 We have the following Pseudo-Random Generator

$$G'(s) = G(s)||G(s') \text{ where } s' \text{ is simply } s \text{ with the last bit flipped.}$$

Preparing Input:

Proof: Assume that G' is not a PRG. Then $\exists$ PPT algorithm D who distinguishes

$$|Pr[D(y) = 1|y \leftarrow G'(s)] - Pr[D(y) = 1|y \leftarrow_{\$} \{0,1\}^n]| = \varepsilon(n)$$

Where $\varepsilon(n)$ is a non-negligible function.
Let D be a distinguisher for G' with the following algorithm:

1. On input y, parse it as $y = y_1, y_2 \ldots y_n$
2. Calculate $z = G(s)||G(s')$
3. Return

$$D(y) = \begin{cases} 1 & if\ z = y_1 \ldots y_{\frac{n}{2}-1}||y_{\frac{n}{2}} \ldots y_{n-1} \\ 0 & otherwise \end{cases}$$

This would be because, since the first $1 \ldots \frac{n}{2} - 1$ bits are equal to the *next* $\frac{n}{2} \ldots n-1$ bits, as only the last bit is being flipped.

Case Analysis: For when $y = G'(s)$ and $y = \{0,1\}^n$

1. For D to output 1, we need the Probability that the $1 \ldots \frac{n}{2} - 1$ bits are equal to the *next* $\frac{n}{2} \ldots n-1$ bits

$$Pr[D(G'(s)) = 1] = 1 - Pr[D(G'(s)) = 0] = 1 - \frac{1}{2^{\frac{n}{2}-1}} \tag{3}$$

[1] Hint: Is there a way to force a relationship between $G(s)$ and $G(s')$ for some particular G?
[2] Notation remark: s' is simply s with the last bit flipped.

2. For when y is Truly Random, we have that the

$$Pr[D(G'(s) = 1] = \frac{2^{\frac{n}{2}-1}}{2^n} = 2^{-\frac{n}{2}-1} \tag{4}$$

Thus, the difference in Equation *3* and *4* gives us

$$|Pr[D'(y) = 1|y \leftarrow G(s)||G(s')|] - Pr[D'(y) = 1|y \leftarrow 0, 1^{\ell(p(n))}]| = 1 - \frac{1}{2^{\frac{n}{2}-1}} - \frac{1}{2^{\frac{n}{2}+1}}$$

which is non-negligible. Hence we say that $G'(s) = G(s)||G(s')$ is not a secure PRG.

Problem 3: PRF

Suppose that $F : \{0,1\}^* \times \{0,1\}^* \to \{0,1\}^*$ is a pseudorandom function. Typically a key k is chosen and we are interested in $F_k = F(k, \cdot) : \{0,1\}^* \to \{0,1\}^*$. See also definition from Katz/Lindell 3.25.

Then say whether the following are a PRF or not, and prove why or show an attack.

1. $F'_k(x) = F_k(x)||F_k(\bar{x})$. The notation $\bar{x}$ means all the bits of x are flipped.

Solution 3.1 We have the Pseudo Random Function:

$$F : \{0,1\}^* \times \{0,1\}^* \to \{0,1\}^*$$

Algorithm A

Preparing Input

- $x^0 \leftarrow \{0,1\}^n$
- $x^1 \leftarrow \bar{x}$ where the notation $\bar{x}$ means all the bits of x are flipped.

We have from the definition that

$$|Pr[D^{F_k(\cdot)} \cdot (1^n) = 1] - Pr[D^{F(\cdot)} \cdot (1^n) = 1]| \leq negl(n)$$

- Query Oracle with input x^0 and x^1
- On receipt of $\mathcal{O}(x^0 = y^0)$, parse it as $y^0 = y^0_1||y^0_2$
- On receipt of $\mathcal{O}(x^1 = y^1)$, parse it as $y^1 = y^1_1||y^1_2$
- if $y^1_1 == y^0_1$, output 1. Else output 0

Analysis of A's Success
Case $\mathcal{O} = F'$

1. $\mathcal{O}(x^0) = y^0 = y^0_1||y^0_2 = F'_{k_1}(x^0)||F'_{k_2}(\bar{x}^0)$
2. $\mathcal{O}(x^1) = y^1 = y^1_1||y^1_2 = F'_{k_2}(x^1)||F'_{k_2}(\bar{x}^1)$
   - But we have that $\bar{x}^0 = x^1$
3. Then $\mathcal{O}(x^1) = F'_{k_2}(\bar{x}^0)||F'_{k_2}(x^0)$
4. Then $y^0_1 = y^1_2$ with a probability 1
5. $A^{F(\cdot)}() = 1$ with a probability 1

Case $\mathcal{O} = Truly\ Random\ Function(TF)$

1. $\mathcal{O}(x^0) = y^0 = y_1^0 || y_2^0$; where y_1^0 and y_2^0 are uniformly random
2. $\mathcal{O}(x^1) = y^1 = y_1^1 || y_2^1$; where y_1^1 and y_2^1 are uniformly random
3. Then $y_1^0 = y_2^1$ with a probability $\frac{1}{2^n}$
4. $A^{F(\cdot)}() = 1$ with a probability $\frac{1}{2^n}$

We see that

$$|Pr[A^{TF(\cdot)}() = 1] - Pr[A^{F(\cdot)}() = 1]| = |1 - \frac{1}{2^n}|$$

which is not negligible, Hence, F' is not a secure Pseudo Random Function.

2. $F'_k(x) = F_k(x) \oplus x$.

Solution 3.2 We have the Pseudo Random Function:

$$F : \{0,1\}^* \times \{0,1\}^* \rightarrow \{0,1\}^*$$

$$F_k = F(k, \cdot) : \{0,1\}^* \rightarrow \{0,1\}^*$$

Theorem: If F is a secure PRF then F' is a secure PRF.
Proof by contradiction. We will prove the following statement. *If F' is not a secure PRF then F is not a secure PRF.*

Step 1: F' is not secure; which means that $\exists$ PPT algorithm A' such that A' can distinguish between F' and a *Truly Random* function *(TF)* with a probability $\varepsilon(n)$; where $\varepsilon(n)$ is non-negligible.

Step 2: Reduction

- A gets access to the Oracle where $\mathcal{O}$ is F or a *Truly Random* Function *TF*.
- A activates A'
  1. On each query x_i by A' forwarded to $\mathcal{O}$, Receive $\mathcal{O}(x_i) = y_i$
  2. Calculate $y'_i = y_i \oplus x_i$. Forward y'_i to A'
- Finally when A' outputs b, output the same

Step 3: Analysis of success probability of the reduction of A

Case 1: $\mathcal{O} = F$

1. A gets $F_k(x_i)$ for each query x_i
2. Then $y_i = F_k(x_i) \oplus x_i$

This looks exactly like the view A' would see with $\mathcal{O} = F'$

Case 2: $\mathcal{O} = TF$

1. A gets $y_i \leftarrow_\$ \{0,1\}^n$
2. A' gets $y_i \oplus x_i$ which is also uniformly random

This looks exactly like the view A' would see with $\mathcal{O} = TF$
We know by assumption that

$$|Pr[A^F \cdot (1^n) = 1] - Pr[A^{TF} \cdot (1^n) = 1]| = \varepsilon(n)$$

We conclude that A, gives the same output as A' distinguishes with probablity $\varepsilon(n)$. However by assumption $\varepsilon(n)$ is non-negligible and A is an adversary of F, which is a PRF. This is a *contradiction* so F' must be a secure PRF.