MIDN ANDRES
SY308 - 4001
HW02

(5 pts) Read the course notes from Probability through Perfect Indistinguishability. Honestly declare one of the following:
(0 pt) I didn't read the notes.
(2 pts) I just skimmed the notes.
(3 pts) I read the notes, but I skipped a couple of difficult topics.
(5 pts) I read the notes very carefully and thoroughly.

D

(5 pts) Solve the quiz candidate problems in the notes from Probability through Perfect Indistinguishability.
Honestly declare one of the following:
(0 pt) I did nothing.
(2 pts) I looked at the solutions, but didn't attempt to solve the problems on my own. (Recall you should get help from your instructor, if you don't understand the course material.)
(4 pts) I tried to solve some of the problems on my own, and then checked the solutions.
(5 pts) I tried to solve all problems on my own, and then checked the solutions.
Remember: Midshipmen don't lie, cheat or steal.

C

36 3

3. (10 pts: 20 mins) Consider an experiment in which two dice are rolled, and we define three random variables associated with the experiment:

- o X1 : the result of rolling the first dice
- o X2 : the result of rolling the second dice
- o S : the sum of the results of both die, i.e., S=X1+X2

Calculate the following probabilities. For each one explain your answer.

a. Pr[X1=1,X2=2]

$Pr[X1=1, X2=2] = Pr[X1=1] \cdot Pr[X_2=2] = \frac{1}{6} \cdot \frac{1}{6} = \frac{1}{36}$

$\frac{1}{36}$

b. Pr[X1=1 | X2=2] $= \frac{Pr[X1=1, X2=2]}{Pr[X2=2]} = \frac{\frac{1}{6} \cdot \frac{1}{6}}{\frac{1}{6}} = \frac{1}{6}$

These are independent events, so the results of the second roll do not effect The results of the first roll and vice versa.

c. Pr[S=5]

X1	X2	S
1	4	5
2	3	5
3	2	5
4	1	5

There are 36 total outcomes an 4 outcomes in which the sum is equal to 4. $\therefore Pr[S=5] = \frac{4}{36} = \frac{1}{9}$

Or $\frac{1}{36} + \frac{1}{36} + \frac{1}{36} + \frac{1}{36} = \frac{1}{9}$

d. Pr[S=5 | X1=3] $= \frac{Pr[S=5, X1=3]}{Pr[X1=3]} = \frac{\frac{1}{9} \cdot \frac{1}{6}}{\frac{1}{6}} = \frac{\frac{1}{36}}{\frac{1}{6}} = \frac{1}{6}$

e. Pr[X1=3 | S=5] $= \frac{Pr[X1=3, S=5]}{Pr[S=5]} = \frac{Pr[S=5 | X1=3] \cdot Pr[X1=3]}{Pr[S=5]}$

$= \frac{\frac{1}{6} \cdot \frac{1}{6}}{\frac{1}{9}} = \frac{\frac{1}{36}}{\frac{1}{9}} = \frac{1}{4}$

f. Pr[X2=1 | S=5] $= \frac{Pr[X2=1, S=5]}{Pr[S=5]} = \frac{Pr[S=5 | X_2=1] \cdot Pr[X2=1]}{Pr[S=5]}$

$Pr[X2=1] = \frac{1}{6}$

$Pr[S=5] = \frac{1}{9}$

$Pr[S=5 | X2=1] = \frac{Pr[S=5, X_2=1]}{Pr[X_2=1]} = \frac{\frac{1}{9} \cdot \frac{1}{9}}{\frac{1}{6}} = \frac{1}{6}$

$= \frac{\frac{1}{6} \cdot \frac{1}{6}}{\frac{1}{9}} = \frac{1}{4}$

X1	X2	S
3	4	7
3	5	8
3	6	9

$\frac{3}{36} = \frac{1}{12}$

(1,6) (3,6) (5,2) (6,1)
(2,5) (4,3) (5,3) (6,2)
(2,6) (4,4) (5,4) (6,3)
(3,4) (4,5) (5,5) (6,4)
(3,5) (4,6) (5,6) (6,5)
(6,6) (4,6) (5,6) (6,6)

G.

Pr[X1=3,S>6]

$\boxed{\frac{1}{12}}$

$Pr[X1=3] = \frac{1}{6}$

$Pr[S>6] = \frac{21}{36}$

$Pr[S>6 \mid X1=3] = \frac{1}{2}$

$Pr[X1=3, S>6] = Pr[X1=3] \cdot Pr[X_2=4,5,6]$

$= \frac{1}{6} \cdot \frac{3}{6}$

$= \boxed{\frac{1}{12}}$

H.

Pr[S=5 | X1>3]

X2	S
4	5
3	5
2	5
1	5

X1
1
2
3
4
5
6

$= Pr[X1=4 \mid X1>3] \times Pr[X2=1]$

$= \frac{1}{3} \times \frac{1}{6} = \frac{1}{18}$

$\boxed{\frac{1}{18}}$

$Pr[S=5] = \frac{1}{9}$

(TRUE/FALSE) X1 and X2. are independently distributed.

TRUE

These are independent events, so the results of the second roll do not The results of the first roll and vice versa.

(TRUE/FALSE) X1. and SS are independently distributed.

FALSE

The Sum depends on the result of X1 and X2

4. (10 pts: 20 mins) Consider a variant of Vegenere Cipher $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ that considers only two-letter words as keys, that is, the key space is $\mathcal{K} = \{AA, AB, \ldots, ZZ\}$.

   a. We will show the scheme is not perfectly indistinguishable. In order to do so, we should give an adversary that distinguishes between the following experiments EXP_0 and EXP_1. Recall the experiments are defined as follows (In the lecture notes, the experiments are given in a figure. Here we describe the same experiments in texts).

> Experiment EXP_b, where $b = 0$ or 1:
> 1. Choose $K \leftarrow \mathsf{Gen}$.
> 2. Receive M_0 and M_1 from the adversary A.
> 3. Compute $C \leftarrow \mathsf{Enc}_K(M_b)$ and send C to A.

Now, to show that the encryption scheme is not perfectly indistinguishable. We give the following adversary A.

> Adversary A:
> 1. Choose $M_0 = AAA$ and $M_1 = ABC$.
> 2. Receive ciphertext C (from the experiment). Let $C = C_1C_2C_3$; that is, C_i is the i-th letter in C.
> 3. If $C_1 = C_3$ output 0; otherwise output 1.

Calculate the following probabilities. **Briefly explain your answer.**

i. (5 pts) $\Pr[A \text{ outputs } 1 \text{ in } EXP_0]$

ii. (5 pts) $\Pr[A \text{ outputs } 1 \text{ in } EXP_1]$

Pr[A outputs 1 in Exp0]
= Pr[C1=C3, A outputs 1] + Pr[C1≠C3, A outputs 1]
= 0 + Pr[C1≠C3, A=1]
= Pr[C1≠C3] · Pr[A=1 | C1≠C3]
= Pr[C1≠C3] · 1
= Pr[EncK(M0)=1] in EXP0 message 0 is Encrypted
= Pr[Len(K)=3, K[0]≠K[2]]
= 0 → Every odd C will have the same shift, so if you Plug in the same 3 letters, The first and the 3rd will always be the same. ∴ C1=C3 and A outputs 0

Pr[A outputs 1 in Exp1]
= Pr[C1=C3, A outputs 1] + Pr[C1≠C3, A outputs 1]
= 0 + Pr[C1≠C3, A=1]
= Pr[C1≠C3] · Pr[A=1 | C1≠C3]
= Pr[C1≠C3] · 1
= Pr[EncK(M1)=1] in EXP1 message 1 is Encrypted
= Pr[K=1]
= 1 → Again every odd C will have the same shift, so if you Plug in ABC, C1 will never equal C3 ∴ C1≠C2 and A outputs 1

|0-1| = 1 ∴ The Advantage of A is 1

5. (20 pts: 20 mins) Consider another variant of Vegenere Cipher $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ where the key generation is defined as follows:

50/50

Gen :
1. Choose the key length $\ell \leftarrow \{1, 2\}$. The key length ℓ is 1 with probablity 1/2 and 2 with probability 1/2.
2. For $i = 1$ to ℓ: $K_i \leftarrow \{A, \ldots, Z\}$. — 26 possibilities
3. Output K_1 if $\ell = 1$ or $K_1 K_2$ if $\ell = 2$.
4. Phrased another way, this is the Vigenere cipher where 50% of the time the key is length 1 and 50% of the time it is length 2.

a. (2 pts) What is $\Pr[K = AA \mid \ell = 2]$?

b. (2 pts) What is $\Pr[K = A]$? Keep in mind that there is a 1/2 chance of picking a key of length 1 and then on top of that a 1/26 chance of picking a particular single-length shift value.

c. (2 pts) What is $\Pr[K = AA]$?

d. (2 pts) What is $\Pr[C = CC \mid M = AA]$? Hint: you have to consider that 50% of the time the key will be length 1 and 50% of the time it will be length 2. How many keys are there of length 1 that would cause this encryption to happen? How many of length 2?

e. (2 pts) What is $\Pr[C = CC \mid M = AB]$?

---

f. We will show the scheme is not perfectly indistinguishable. We give the following adversary A that distinguishes EXP_0 and EXP_1 defined above.

Adversary A:
1. Choose $M_0 = AA$ and $M_1 = AB$.
2. Receive ciphertext C (from the experiment). Let $C = C_1 C_2$; that is, C_i is the i-th letter in C.
3. If $C_1 = C_2$ output 0; otherwise output 1.

Calculate the following probabilities. **Briefly explain your answer.**

i. (5 pts) $\Pr[A \text{ outputs } 1 \text{ in } EXP_0]$

ii. (5 pts) $\Pr[A \text{ outputs } 1 \text{ in } EXP_1]$

a. (2 pts) What is $\Pr[K = AA \mid \ell = 2]$? $= \Pr[K = AA]$ Because they are independent

$26 \cdot 26 = 676$ possibilities

$K_1 = 26$ possibilities

$K_2 = 26$ possibilities

$\Pr[K = AA] = \boxed{\frac{1}{676}}$

b. (2 pts) What is $\Pr[K = A]$? Keep in mind that there is a 1/2 chance of picking a key of length 1 and then on top of that a 1/26 chance of picking a particular single-length shift value.

$\Pr[K = A] = \Pr[\ell = 1, K = A] + \Pr[\ell = 2, K = A] = 0 + \frac{1}{2} \cdot \frac{1}{26} = \boxed{\frac{1}{52}}$

c. (2 pts) What is $\Pr[K = AA]$? $= \Pr[\ell = 2, K = AA] = \frac{1}{2} \cdot \frac{1}{676} = \boxed{\frac{1}{1352}}$

d. (2 pts) What is $\Pr[C = CC \mid M = AA]$? Hint: you have to consider that 50% of the time the key will be length 1 and 50% of the time it will be length 2. How many keys are there of length 1 that would cause this encryption to happen? How many of length 2?

$\Pr[\ell = 1, K = C] + \Pr[\ell = 2, K = CC]$

$\frac{1}{2} \cdot \frac{1}{26} + \frac{1}{2} \cdot \frac{1}{676} = \frac{26}{1352} + \frac{1}{1352} = \boxed{\frac{27}{1352}}$

e. (2 pts) What is $\Pr[C = CC \mid M = AB]$?

$\Pr[K = CB]$

$= \boxed{\frac{1}{676}}$

i. (5 pts) $\Pr[A \text{ outputs 1 in } EXP_0]$ $M_0 = AA$ 3. If $C_1 = C_2$ output 0; otherwise output 1.

$\Pr[A \text{ outputs 1 in Exp0}]$
$= \Pr[C_1 = C_2, A \text{ outputs 1}] + \Pr[C_1 \neq C_2, A \text{ outputs 1}]$
$= 0 + \Pr[C1 \neq C_2, A = 1]$
$= \Pr[C_1 \neq C_2] \cdot \Pr[A = 1 \mid C_1 \neq C_2]$
$= \Pr[C_1 \neq C_2] \cdot 1$
$= \Pr[Enc_K(M_0) = 1]$ in EXP0 message 0 is Encrypted
$= \Pr[l = 2, K_1 \neq K_2]$
$= \frac{1}{2} \cdot \frac{25}{26} = \frac{25}{52}$

$\Pr[K_1 \neq K_2]$
$= 1 - \Pr[K_1 = K_2]$
$1 - \frac{26}{676} = \frac{25}{26}$

If the adversary sends the message AA or when Plaintext 1 = Plaintext 2, and our key length is 1, then C1 = C2 thus the adversary will output 0 so at least half of the time the adversary will output 0. Also, if our key length is 2 and K1=K2 then C1=C2 and the adversary will output 0. The rest of the time the adversary will output 0, meaning that C1 != C2 and thus when K1 != K2.

ii. (5 pts) $\Pr[A \text{ outputs 1 in } EXP_1]$ $M_1 = AB$

$\Pr[A \text{ outputs 1 in Exp1}]$
$= \Pr[C_1 = C_2, A \text{ outputs 1}] + \Pr[C_1 \neq C_2, A \text{ outputs 1}]$
$= 0 + \Pr[C1 \neq C_2, A = 1]$
$= \Pr[C_1 \neq C_2] \cdot \Pr[A = 1 \mid C_1 \neq C_2]$
$= \Pr[C_1 \neq C_2] \cdot 1$
$= \Pr[Enc_K(M_1) = 1]$ in EXP message 1 is Encrypted
$= \Pr[l = 2, K_1 \neq K_2] + \Pr[l = 1]$
$= \frac{1}{2} \cdot \Pr[K_1 \neq K_2 + 1] + \frac{1}{2}$
$= \frac{1}{2} \cdot \frac{25}{26} + \frac{1}{2}$
$= \frac{51}{52}$

$\Pr[K_1 \neq K_2 + 1]$
$= 1 - \Pr[K_1 = K_2 + 1]$
$= 1 - \frac{1}{26}$
$= \frac{25}{26}$

If the adversary sends the message AB or when Plaintext 1 = Plaintext 2 +1, and our key length is 1, then C1 != C2 thus the adversary will output 1 so at least half of the time the adversary will output 1. Also, if our key length is 2 and K1=K2+1 then C1=C2 and the adversary will output 0. The rest of the time the adversary will output 1 meaning that C1 != C2 and thus when K1 != K2 +1 or key length =1.

$\left| \frac{25}{52} - \frac{51}{52} \right| = \frac{1}{2}$ ∴ The Advantage of A is $\frac{1}{2}$

6. (10 pts: 25 minutes) Consider following encryption scheme.

- The message space is $\mathcal{M} = \{0, 1, \ldots, 4\}$. Algorithm Gen chooses a key from uniformly at random from the key space $\mathcal{K} = \{0, 1, \ldots, 5\}$. $\mathsf{Enc}_K(M)$ returns $(k + m) \bmod 5$ and $\mathsf{Dec}_K(c)$ returns $(c - k) \bmod 5$.

Here $a \bmod b$ computes the remainder resulting from dividing a by b, and the remainder value is at most 0 and less than b. For example, $7 \bmod 3$ is 1, since we have $7 = 2 \cdot 3 + 1$. In addition, $-1 \bmod 3$ is 2, since we have $-1 = (-1) \cdot 3 + 2$.

For example, $\mathsf{Enc}_3(4) = (3 + 4) \bmod 5 = 7 \bmod 5 = 2$.

Show that the above scheme is not perfectly indistinguishable. In particular,

a. (4 pts) Give an adversary algorithm that distinguishes between EXP_0 and EXP_1.

Adversary A:
1. Choose $M_0 =$ 0 and $M_1 =$ 4
2. Receive ciphertext C.
3. If C = 0 output 0; else output 1.

b. (3 pts) Calculate $\Pr[A \text{ outputs } 1 \text{ in } EXP_0]$ for algorithm A that you give right above.

c. (3 pts) Calculate $\Pr[A \text{ outputs } 1 \text{ in } EXP_1]$ for algorithm A that you give right above.

The above two probabilities must differ.

b.

$$
\begin{aligned}
&\Pr[A \text{ outputs } 1 \text{ in } Exp_0] \\
&= \Pr[C = 0, A \text{ outputs } 1] + \Pr[C \neq 0, A \text{ outputs } 1] \\
&= 0 + \Pr[C \neq 0, A = 1] \\
&= \Pr[C \neq 0] \cdot \Pr[A = 1 \mid C \neq 0] \\
&= \Pr[C \neq 0] \cdot 1 \\
&= \Pr[Enc_K(m_0) \neq 0] \quad \text{in } EXP_0 \text{ message 0 is Encrypted} \\
&= 1 - (\Pr[K = 0] + \Pr[K = 5]) \\
&= 1 - \left(\frac{1}{6} + \frac{1}{6}\right) \\
&= \frac{2}{3}
\end{aligned}
$$

If the adversary chooses message 0 it will be added to the value of the key, which will be itself because 0 + num = num. Thus, if the key is 0 or 5, the modulo operation will equal 0, and the message will be 0. So the adversary will output 0, this happens 1/3 of the time, thus the probability that the adversary outputs 1 is 2/3.

C.

$$
\begin{aligned}
&\Pr[A \text{ outputs } 1 \text{ in } Exp_1] \\
&= \Pr[C = 0, A \text{ outputs } 1] + \Pr[C \neq 0, A \text{ outputs } 1] \\
&= 0 + \Pr[C \neq 0, A = 1] \\
&= \Pr[C \neq 0] \cdot \Pr[A = 1 \mid C \neq 0] \\
&= \Pr[C \neq 0] \cdot 1 \\
&= \Pr[Enc_K(m_0) \neq 0] \quad \text{in } EXP_1 \text{ message 1 is Encrypted} \\
&= 1 - \Pr[K = 1] \\
&= 1 - \frac{1}{6} = \frac{5}{6}
\end{aligned}
$$

If the adversary chooses message 1 it will be added the the value of the key, and take the modulo of it and return the encrypted number. Thus, if the key is 1 the modulo operation will equal 0, and the message will be 0. So the adversary will output 0, this happens 1/6 of the time, thus the probability that the adversary outputs 1 is 5/6.

$$\left| \frac{4}{6} - \frac{5}{6} \right| = \quad \therefore \text{ The Advantage of A is } \frac{1}{6}$$

7. (10 pts) Consider the following encryption scheme with key space $\mathcal{K} = \{0, 1, 2, 3, 4\}$, and message space $\mathcal{M} = \{0, 1, 2\}$.

- $\mathsf{Gen}()$: $K \leftarrow \mathcal{K}$, and output K.
- $\mathsf{Enc}_K(M)$: output $(M + K) \bmod 3$.
- $\mathsf{Dec}_K(C)$: output $(C - K) \bmod 3$.

Show that the above scheme is not perfectly indistinguishable. In particular,

a. (4 pts) Give an adversary algorithm that distinguishes between EXP_0 and EXP_1.

Adversary A:

1. Choose $M_0 =$ 0 and $M_1 =$ 1.
2. Receive ciphertext C.
3. If C = 0 output 0; else output 1.

b. (3 pts) Calculate $\Pr[A \text{ outputs } 1 \text{ in } EXP_0]$ for algorithm A that you give right above.

c. (3 pts) Calculate $\Pr[A \text{ outputs } 1 \text{ in } EXP_1]$ for algorithm A that you give right above.

The above two probabilities must differ.

b. $\Pr[A \text{ outputs } 1 \text{ in } Exp_0]$
$= \Pr[C = 0, A \text{ outputs } 1] + \Pr[C \neq 0, A \text{ outputs } 1]$
$= 0 + \Pr[C \neq 0, A = 1]$
$= \Pr[C \neq 0] \cdot \Pr[A = 1 \mid C \neq 0]$
$= \Pr[C \neq 0] \cdot 1$
$= \Pr[Enc_K(m_0) \neq 0]$ in Exp_0 message 0 is Encrypted
$= 1 - \Pr[K = 0] + \Pr[K = 3]$
$= 1 - \frac{1}{5} + \frac{1}{5}$
$= \frac{3}{5}$

If the adversary chooses message 0 it will be added the the value of the key, which will be itself because 0 + num = num. Thus, if the key is 0 or 3, the modulo operation will equal 0, and the message will be 0. So the adversary will output 0, this happens 2/5 of the time, thus the probability that the adversary outputs 1 is 3/5.

C. $\Pr[A \text{ outputs } 1 \text{ in } Exp_1]$
$= \Pr[C = 0, A \text{ outputs } 1] + \Pr[C \neq 0, A \text{ outputs } 1]$
$= 0 + \Pr[C \neq 0, A = 1]$
$= \Pr[C \neq 0] \cdot \Pr[A = 1 \mid C \neq 0]$
$= \Pr[C \neq 0] \cdot 1$
$= \Pr[Enc_K(m_0) \neq 0]$ in Exp_1 message 1 is Encrypted
$= 1 - \Pr[K = 2]$
$= 1 - \frac{1}{5} = \frac{4}{5}$

If the adversary chooses message 1 it will be added the the value of the key, and take the modulo of it and return the encrypted number. Thus, if the key is 2 the modulo operation will equal 0, and the message will be 0. So the adversary will output 0, this happens 1/5 of the time, thus the probability that the adversary outputs 1 is 4/5.

$\left| \frac{3}{5} - \frac{4}{5} \right| =$ ∴ The Advantage of A is $\frac{1}{5}$

8. (10 pts) Consider the following encryption scheme with key space $\mathcal{K} = \{0,1,2,3,4,5\}$, and message space $\mathcal{M} = \{0,1,2\}$.

   - $\mathsf{Gen}()$: $K \leftarrow \mathcal{K}$, and output K.
   - $\mathsf{Enc}_K(M)$: output $(M + K) \bmod 3$.
   - $\mathsf{Dec}_K(C)$: output $(C - K) \bmod 3$.

   (10 pts) Show that the above encryption scheme **is perfectly indistinguishable**. In particular, prove that no adversary can exist that wins the distinguishing game with a non-zero advantage.

Adversary A :
1. Choose M0 = 0, M1 = 1, and M2=2 .
2. Receive ciphertext C .
3. If C=0 output 0; Else output 1 .

M0

$$
\begin{aligned}
&Pr[A \text{ outputs } 1 \text{ in } Exp_0] \\
&= Pr[C = 0, A \text{ outputs } 1] + Pr[C \neq 0, A \text{ outputs } 1] \\
&= 0 + Pr[C \neq 0, A = 1] \\
&= Pr[C \neq 0] \cdot Pr[A = 1 \mid C \neq 0] \\
&= Pr[C \neq 0] \cdot 1 \\
&= Pr[Enc_K(m_0) \neq 0] \quad \text{in } Exp_0 \text{ message } 0 \text{ is Encrypted} \\
&= 1 - Pr[K = 0] + Pr[K = 3] \\
&= 1 - \left(\frac{1}{6} + \frac{1}{6}\right) \\
&= \frac{4}{6}
\end{aligned}
$$

M1

$$
\begin{aligned}
&Pr[A \text{ outputs } 1 \text{ in } Exp_1] \\
&= Pr[C = 0, A \text{ outputs } 1] + Pr[C \neq 0, A \text{ outputs } 1] \\
&= 0 + Pr[C \neq 0, A = 1] \\
&= Pr[C \neq 0] \cdot Pr[A = 1 \mid C \neq 0] \\
&= Pr[C \neq 0] \cdot 1 \\
&= Pr[Enc_K(m_0) \neq 0] \quad \text{in } Exp_1 \text{ message } 1 \text{ is Encrypted} \\
&= 1 - (Pr[K = 2] + Pr[K = 5]) \\
&= 1 - \frac{1}{6} - \frac{1}{6} = \frac{4}{6}
\end{aligned}
$$

M2

$$
\begin{aligned}
&Pr[A \text{ outputs } 1 \text{ in } Exp_2] \\
&= Pr[C = 0, A \text{ outputs } 1] + Pr[C \neq 0, A \text{ outputs } 1] \\
&= 0 + Pr[C \neq 0, A = 1] \\
&= Pr[C \neq 0] \cdot Pr[A = 1 \mid C \neq 0] \\
&= Pr[C \neq 0] \cdot 1 \\
&= Pr[Enc_K(m_0) \neq 0] \quad \text{in } Exp_2 \text{ message } 2 \text{ is Encrypted} \\
&= 1 - (Pr[K = 1] + Pr[K = 4] \\
&= 1 - \left(\frac{1}{6} + \frac{1}{6}\right) = 4/6
\end{aligned}
$$

If m_0 and m_1 are chosen $\left|\frac{4}{6} - \frac{4}{6}\right| = 0$ $\therefore$ The Advantage of A is 0

If m_0 and m_2 are chosen $\left|\frac{4}{6} - \frac{4}{6}\right| = 0$ $\therefore$ The Advantage of A is 0

If m_1 and m_2 are chosen $\left|\frac{4}{6} - \frac{4}{6}\right| = 0$ $\therefore$ The Advantage of A is 0

If the adversary chooses any message it will be added the the value of the key, and take the modulo of it and return the encrypted number. In the steps above I proved that regardless of which message the adversary chooses, each time there is a 1/3 chance that the ciphertext will return as a 0 because the key and message set each have two compliments that when added together and modded by 3 equal 0. So in each experiment the adversary has the same advantage in each and if you pair that with any other experiment, the net advantage will be equivalent, thus 0. So this encryption scheme is perfectly indistinguishable.