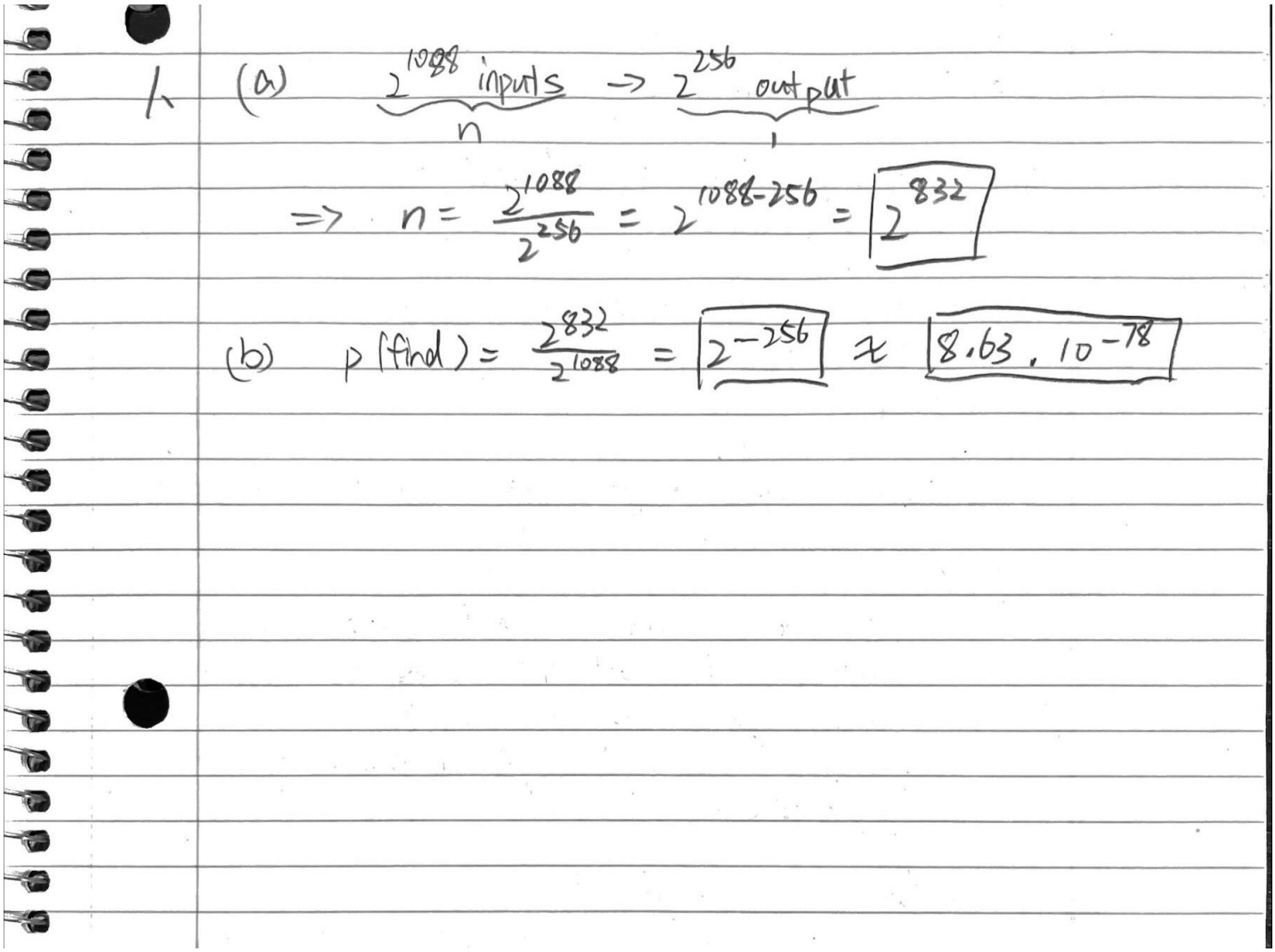
CS181 HW4
Xiaoming Huang

1. Asd



2.

2. to show if f has weakly collision resistant property, then f has one way property.

proof by contrapositive:

Assume f is not a one way function.
then given $y \in Y$, we are able to find some $x \in Y$ such that $f(x) = y$.

which means if we know $y = f(x)$., $x \in X$, $y \in Y$

we can find $x' \in X$ such that $f(x) = y$.

Also notice that $|x|/|X|$ is large, set that to be n. that means that
$p(x' = x) = \frac{1}{n}$, which is super small

Since f is n to 1, and we will hit on x with $\frac{1}{n}$ chance.

so $p(x' \neq x) = 1 - \frac{1}{n} \approx 1$

So it's highly likely to find an $x' \in X$ and $f(x') = y = f(x)$ with almost 100% chance that $x' \neq x$
i.e. f is not weakly collision resistant.

Hence, by contrapositive, if f has weakly collision property, then it also has the one-way property

∎

3.

inputSHA3() is in *345.cpp*

4.

outputSHA3() is in *345.cpp*

Testing result:

```
Question 3 and 4:
the text:
00110001001100100011001100110100001101010011011000110111001110000011100100110000001100010011
00100011001100110100001101010011011000110111001110000011100100110000001100010011001000110011
00110100001101010011011000110111001110000011100100110000001100010011001000110011001101000011
01010011011000110111001110000011100100110000001100010011001000110011001101000011010100110110
00110111001110000011100100110000001100010011001000110011001101000011010100110110001101110011
10000011100100110000001100010011001000110011001101000011010100110110001101110011000001110001
00110000001100010011001000110011001101000011010100110110001101110011100000111001001100000011
00010011001000110011001101000011010100110110001101110011100000111001001100000011000100110010
00110011001101000011010100110110001101110011100000111001001100000011000100110010001100110011
01000011010100110110001101110011100000111001001100000011000100110010001100110011010000110101
00110110001101110011100000111001001100000011000100110010001100110011010000110101001101100011
01110011100000111001001100000011000100110010001100110011010000110101001101100011100000111000
00111001001100000011000100110010001100110011010000110101001101100011101110011100000111001011
00000011000100110010001100110011010000110101001101100011101110011100000111001001100000011000
00110010001100110011010000110101001101100011101110011100000111001001100000011000100110010011
00110011010000110101001101100011101110011100000111001001100000011000100110010001100110011010
00110101001101100011011100111000001110010011000000110001001100100011001100110100001101010011
01100011011100111000001110010011000
```

```
output of outputSHA3:
00110001001100100011001100110100001101010011011000110111001110000011100100110000001100010011
00100011001100110100001101010011011000110111001110000011100100110000001100010011001000110011
00110100001101010011011000110111001110000011100100110000001100010011001000110011001101000011
01010011011000110111001110000011100100110000001100010011001000110011001101000011010100110110
00110111001110000011100100110000001100010011001000110011001101000011010100110110001101110011
10000011100100110000001100010011001000110011001101000011010100110110001101110011000001110001
00110000001100010011001000110011001101000011010100110110001101110011100000111001001100000011
00010011001000110011001101000011010100110110001101110011100000111001001100000011000100110010
00110011001101000011010100110110001101110011100000111001001100000011000100110010001100110011
01000011010100110110001101110011100000111001001100000011000100110010001100110011010000110101
00110110001101110011100000111001001100000011000100110010001100110011010000110101001101100011
01110011100000111001001100000011000100110010001100110011010000110101001101100011100000111000
00111001001100000011000100110010001100110011010000110101001101100011101110011100000111001011
00000011000100110010001100110011010000110101001101100011101110011100000111001001100000011000
00110010001100110011010000110101001101100011101110011100000111001001100000011000100110010011
00110011010000110101001101100011101110011100000111001001100000011000100110010001100110011010
00110101001101100011011100111000001110010011000000110001001100100011001100110100001101010011
01100011011100111000001110010011000
```

5.

theta() is in *345.cpp*

calculated value for a_out[4][3][9....18]: 0011011000
calculated value for a_out[3][1][15...24]: **0000101001**