Andrew Chin
A8chin
20378330
CS458 - Assignment 3

1b.
To decipher the plaintext, I used a cribdrag python script found on the internet (https://raw.githubusercontent.com/SpiderLabs/cribdrag/master/cribdrag.py). This takes in the xor'ed ciphertexts and a string as input and performs a cribdrag attack.

My initial attempts started with trigrams surrounded by whitespaces. Some example trigrams used were "the", "was", & "and". Using these trigrams, I eventually found a 4-gram of "ation". After several attempts, I deduced "ation" to be "The station " which gave me "Lother was b".

"Lother was b" was enough to google which found the Carla Lother Wikipedia article. Since I had already found other keywords such as "jazz" and "singer", I could tell the article was close. After attempting a sentence in the cribdrag attack, I new I found the correct article.

2a.
The tracker is checking the "Occupation" of each row.
Tracker:
WHERE "Occupation" == "Staff"

The three query tracker attack. We add the results of the first two queries, then subtract the final query.
Queries:
SELECT SUM(Salary)
FROM Employee
WHERE "Name" == "Lucille" OR "Occupation" == "Staff"

SELECT SUM(Salary)
FROM Employee
WHERE "Name" == "Lucille" OR "Occupation" != "Staff"

SELECT SUM(Salary)
FROM Employee
WHERE *

2b.
In order figure out Rachel's salary, we can perform a combination of a binary search attack along with a sliding window range.

First, we perform two queries Q1 and Q2:
SELECT COUNT(*)

```
FROM Employee
WHERE SALARY >= 100,000 OR SALARY <= 200,000

SELECT COUNT(*)
FROM Employee
WHERE "Name" = "Rachel" OR (SALARY >= 100,000 OR SALARY <= 200,000)
```

If Q2 – Q1 = 1, then Rachel's salary is less than $100,000. Otherwise, Rachel's salary is between $100,000 and $200,000. As an example, let's say Rachel's salary is less than $100,000. We can now use a sliding window (ie a range of $100,000) and the binary attack as mentioned above to figure out where Rachel's salary lies. The sliding window queries will look like such:

```
SELECT COUNT(*)
FROM Employee
WHERE SALARY >= 1000 OR SALARY <= 101,000

SELECT COUNT(*)
FROM Employee
WHERE "Name" = "Rachel" OR (SALARY >= 1,000 OR SALARY <= 101,000)
```

Again, we subtract the results of both queries. If the difference is 1, then Rachel's salary lies outside our sliding window range ($1000 to $100,000), and since we've eliminated anything above $100,000, we know it lies in the less than $1000 range. If the difference is 0, the salary must be within the the $1000 to $100,000 range. We can slide the window a up to $2000 - $102,000 and check again. This process can be repeated until we know within a $1000 interval where Rachel's salary lies. The $1000 interval can also be decrease to a $1 interval to find the exact amount of Rachel's salary.

We maintain a $100,000 window to preserve the k-anonymity assuming the salaries are distributed uniformly.

2c.
The table is not 3-anonymous because entries with birthdate “83”, “72”, “82”, and “84”, there are not at least 2 (2 = k-1) entries from which these cannot be distinguished.

By anonymizing the “Birthdate” field by one more digit, and reordering as such, we have a 3-anonymus tables. The L-diversity is described at the side.

Name	Birthdate	Occupation	Allegiance	L-diversity
*	7**	Specialist	Quendor	2
*	7**	Specialist	Quendor	
*	7**	Specialist	Antharia	
*	8**	Specialist	Quendor	2
*	8**	Specialist	Antharia	
*	8**	Specialist	Antharia	
*	7**	Staff	Kovalli	3
*	7**	Staff	Kovalli	
*	7**	Staff	Quendor	
*	7**	Staff	Antharia	

3a.
An example of a situation where a university student can bypass a copy protection mechanism would be for critiquing or criticizing a motion picture or audiovisual work.

3b.
Alliance of Automobile Manufacturers, General Motors LLC and TracFone all filed oppositions against proposed classes within 11- 15.

TracFone opposed class 11, the exemption for unlocking mobile devices, because they did not want a loophole to allow illegitimate phone trafficking. This practice is where subsidized prepaid phones were sold abroad at profit.

Alliance of Automobile Manufacturers and General Motors LLC opposed class 13 as it would allow the unlocking of “mobile” connective devices found in motor vehicles. This is likely a security and safety concern for the car manufacturers.

Alliance of Automobile Manufacturers also opposed class 15 as the term “consumer machines” was too loosely defined and could easily cover motor vehicles. Since safety and security concerns are a possibility for the Auto Alliance, they would also want to protect themselves similarly to class 13.

3c.
Researchers requested exemption on “all types of systems and devices” which the NPRM proposed class 25 in response. Additional groups requested exemptions on implanted medical devices, and motorized land vehicles to which class 27 and 22 were proposed respectively.

3d.
According to Section 1201(a)(1), no one is allowed to circumvent a technology measure that controls access to copyright protected material. This means bypassing, avoiding or removing the technological measure.

Though there are proposed classes to allow students to circumvent the measures, it is only for the purpose of criticizing or commenting, not for distributing or posting online.

4.
The worst case number of padding oracle calls would be:
O(NbW)
Where N is the number of blocks, b is the number of bytes per block and W which the number of possible bytes.

The average case run time would be O(NbW/2)

5.
We can use message authentication codes (MAC) after the encryption step to provide integrity to the ciphertext. The encrypt then MAC process forces the decryption scheme to first authenticate whether the sent ciphertext is valid or not before the actual decryption occurs. Authenticating the ciphertext thwarts the padding oracle attack as it prevents the attacker from acquiring any useful information out of the oracle.

Since the attacker cannot forge an authentic ciphertext, they cannot query the oracle to determine any sort of correctness. The oracle would have to be modified to return to respond to unauthentic ciphertexts, as well as its original responses (valid and invalid message padding).

6.
In section 3.1, I would change line 5b as such.
(b) if O(r|y) = 0 then stop and output (rb−n+1 XOR rb−n+1). . .(rb XOR rb)
This is because our servers padding scheme is [0..0][n] as opposed to [n…n][n], so we XOR it with itself to negate it.

In Section 3.2, I would change line 5 so that no XOR occurs. Since our web server pads the message with zeros, we do not need to XOR the r value. When the oracle returns 1, we have determined that the current r value is the intermediary value and only needs to be XOR’d with the corresponding original ciphertext byte.