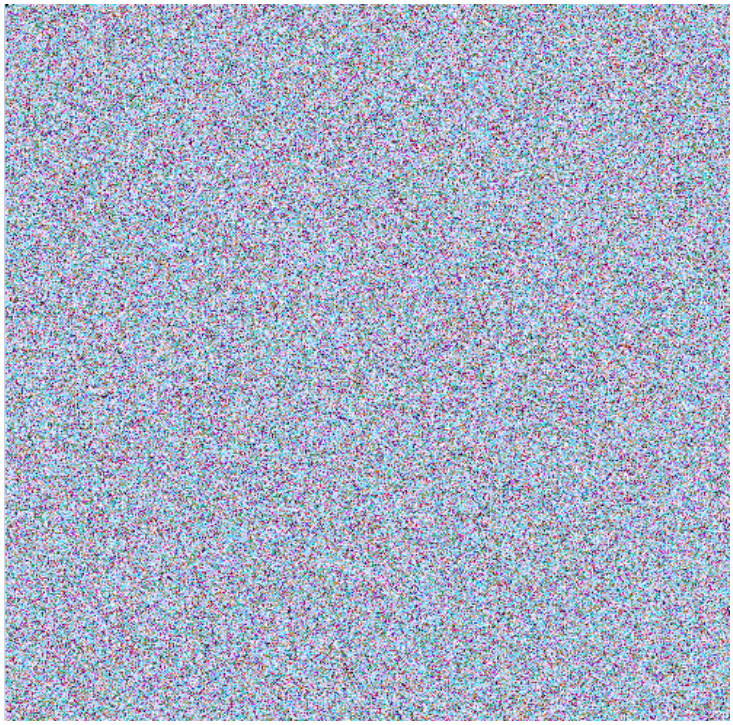
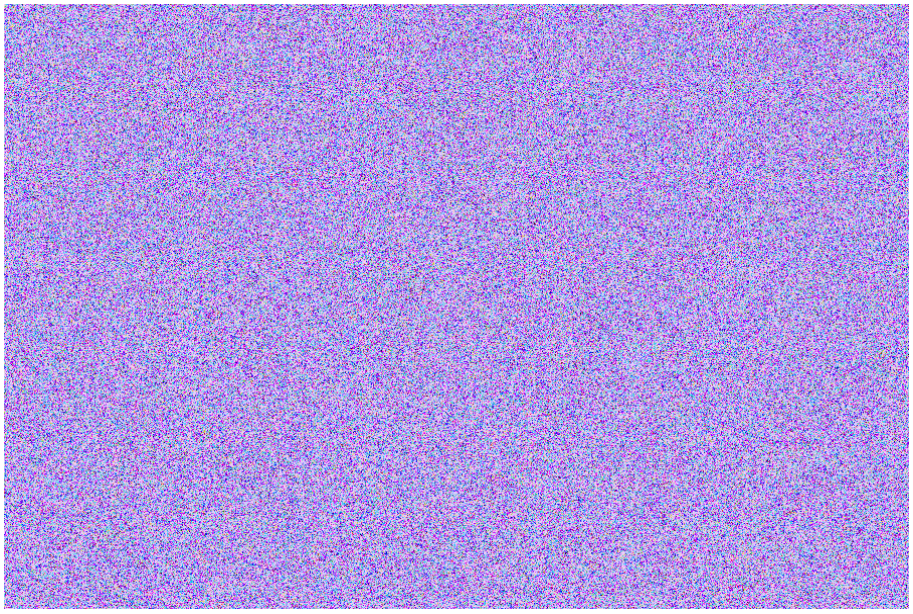
CS 370 - Programming Project 1 Writeup

3.1 - Observation Task: Encryption Modes, CBC vs ECB

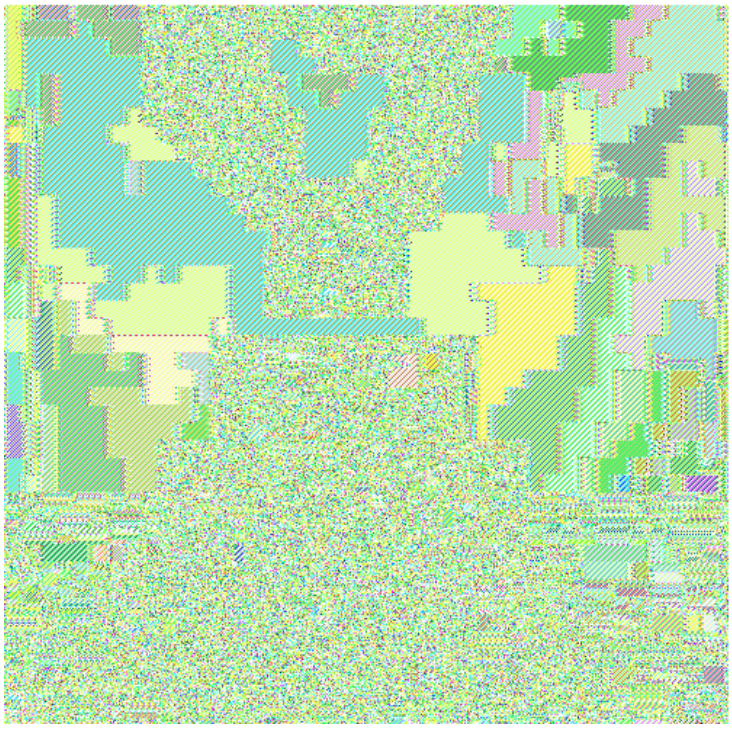
Original photos:

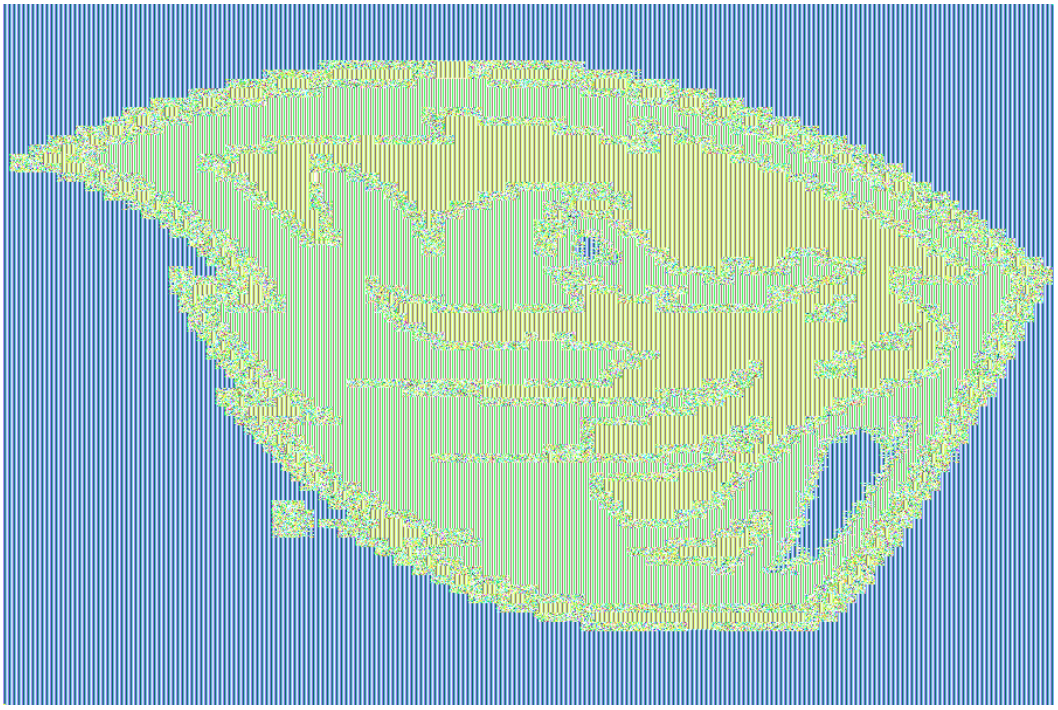
After CBC encryption:





Blocks after ECB encryption:





The images encrypted with AES-128-CBC retain some structure. A bit of information might be able to be gleaned from a CBC-encrypted image if the image was a logo or some image with high contrast/structure. The CBC encrypted images are completely indiscernible.

3.3 - Observation Task: Weak vs Strong Collision Resistance Property

1) Weak collision:

```
Weak Collision Run 1: Matched first 3 characters after 23842311 trials
Weak Collision Run 2: Matched first 3 characters after 32768123 trials
Weak Collision Run 3: Matched first 3 characters after 20230457 trials
Weak Collision Run 4: Matched first 3 characters after 27429341 trials
Weak Collision Run 5: Matched first 3 characters after 36123324 trials

After 5 trials, the total number of trials ran: 140393556
The average number of attacks to find a match for the first 3 characters was 28078711.2
```

I would think that this should take 255*255*255 attempts on average, but it seems to take a bit more than that. I'm not sure why. These trials take *extremely* long to run, so running more than 5 was not really feasible.

2) Strong collision:

```
Strong Collision Run 46: Matched first 3 characters after 9483 trials
Strong Collision Run 47: Matched first 3 characters after 3178 trials
Strong Collision Run 48: Matched first 3 characters after 2303 trials
Strong Collision Run 49: Matched first 3 characters after 1953 trials
Strong Collision Run 50: Matched first 3 characters after 2122 trials

After 50 trials, the total number of trials ran: 238256
The average number of attacks to find a match for the first 3 characters was 4765.12
```

This should take, I believe, 2^12 attempts to have a 50% chance of breaking the property. That's 4096 attempts, not too far off from the average I got.

3) The strong collision property is far easier to break via brute force method.

4) The difference in the observations is due to the fact that the weak collision program is trying to generate a hash to match a provided hash, and the strong collision program is trying to get **any** two hashes to match each other in a growing list of all the hashes the program has generated so far. This results in the strong collision property being broken well before the weak collision property.