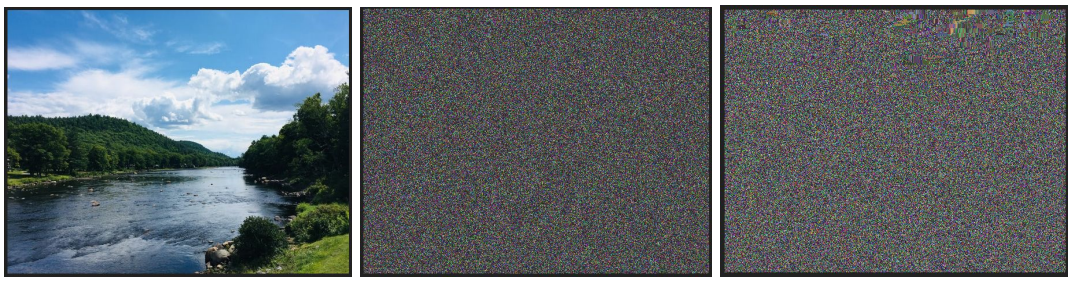
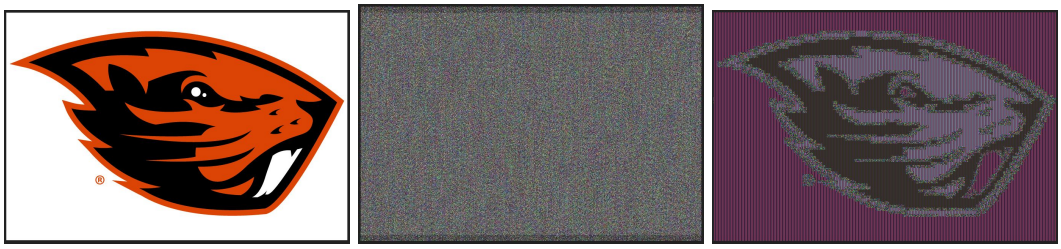
Max Franz

10/27/20

3.1:



The image of my choice was just a nice picture of some nature. The original is the leftmost image above. The middle image was encrypted using CBC mode and the rightmost image was encrypted using ECB mode. There is no visible useful information in either of the encrypted images. Both of the encrypted images also seem kind of blurry.



The beaver logo is above. The original is the leftmost image above. The middle image was encrypted using CBC mode and the rightmost image was encrypted using ECB mode. There is no visible useful information in the CBC encrypted image, however the shape of the beaver logo is visible in the ECB encrypted image. Both of the encrypted images also seem kind of blurry.

3.2:

The key is: 'median ' (with 10 trailing zeros)

I hope there isn't supposed to be any other observations here, the only thing the assignment sheet says is "Your goal is to write a program to find out this key".

3.3:

1. It takes, on average, about 4000 trials in order to break weak collision resistance by brute-forcing.
2. It takes, on average, about 80 trials in order to break strong collision resistance by brute-forcing.
3. Strong collision resistance is much easier to break based on the data I've gathered. From 80 trials to 4000 trials is a huge jump, so it's clear that strong collision resistance is easier to break.
4. I believe the large difference is based on the two properties themselves. With weak collision resistance we're given an arbitrary input and its resulting hash output and have to find another random input that gives the same resulting hash output. This takes longer because it's bound on one end. With strong collision resistance, there are no bounds because both inputs in our case are different and random so it's easier to find a match.