William Endicott

CS370

Assignment2

3.1) for each of the photos used when encrypting with ECB as expected and discussed in lecture that shows a resemblance of the original photo. The beaver logo is very easily identifiable. The photo I picked was a rubber duck with a white background. The ECB encryption shows the outline of the duck. The identical cipher blocks occur in these photos which is why it is recognizable.

The CBC encryption looks like a static screen back when we didn’t have cable. This makes the photos completely unidentifiable.

For this portion of the assignment, I was unable to get the encrypted photos of the beaver logo to open on my computer, so I needed to use a bmp viewer. I spoke with Akshith about this issue, and he told me to attach screen shots and I’ll also attach the website I used.

<https://products.groupdocs.app/viewer/bmp>

A close-up of a brain

Description automatically generated with low confidenceA picture containing player

Description automatically generated

3.2)

The key that was used was the word median from the dict.

3.3)

1)

Table

Description automatically generated

2)For weak collision resistance with 24 bits, it should take about attempts

In 15 runs mine took on average 8934 attempts.

3)For strong collision resistance with 24 bits, it should take about attempts

In 15 runs mine took on average 3882 attempts.

4) Based on what my program produced the one that appears to be easier to break is the strong collision resistance. The birthday paradox is the perfect example for this.

5) The strong resistance requires a smaller number of comparisons because we are tracking every hash and comparing the next generated one to every single occurrence that has already happened. For the weak collision resistance we take one set hash and compare that one to evry newly generated hash.