CS370_hw1

Lyon Kee

October 2023

3 Lab Environment and Tasks

3.1 [15pts] Observation Task: Encryption Mode – ECB vs. CBC

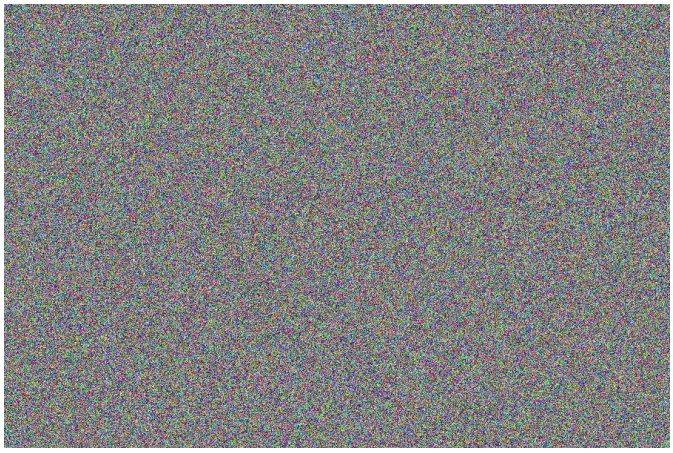

Figure 1: cbc encrypted beaverhead
No useful information can be derived because it is CBC encryption mode, each prior block affects the next.

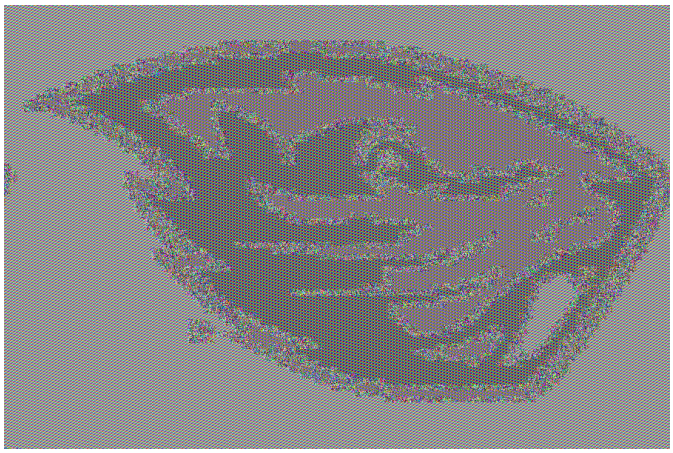

Figure 2: ecb encrypted beaverhead
We are still able to see the pattern in the encrypted data just like the original because it is ECB encryption mode. It does not mask each block with the prior so we can see blocks of data being changed and those same blocks will now have the same encrypted values.

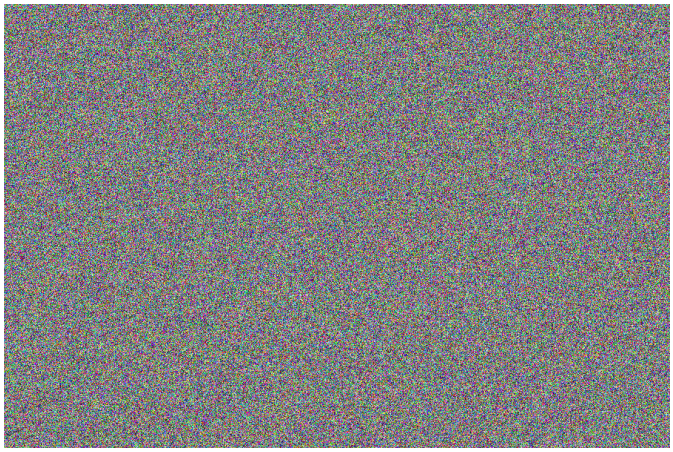

Figure 3: cbc encrypted picture of my cat
No useful information can be derived because it is CBC encryption mode, each prior block affects the next.

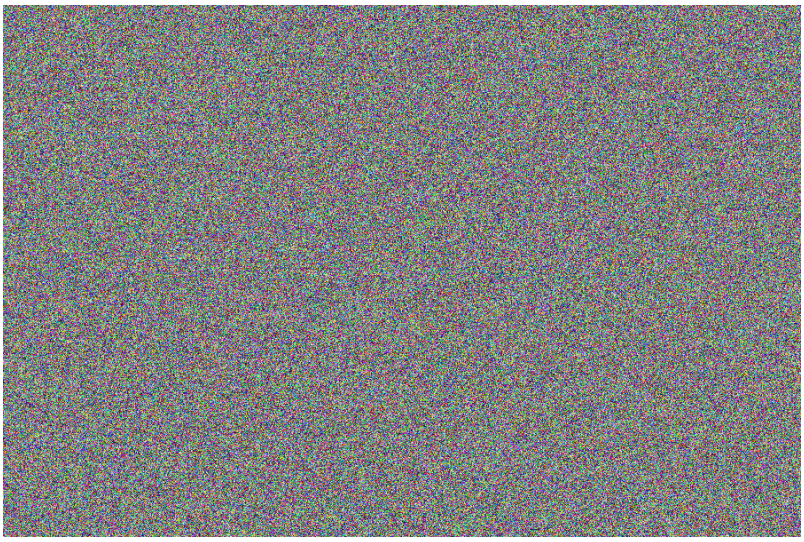

Figure 4: ecb encrypted picture of my cat
No useful information can be derived even though it is in ECB encryption mode, this is because the image has rich colors resulting in the inability to see patterns due to the lack of identical repeated blocks within the image which would hash to the same value with ECB.

3.2 [45pts] Coding Task: Encrypting with OpenSSL

```
KEY FOUND: key for (b'This is a top secret.'): b'median          '
```

3.3 [90pts] Coding Task: Weak versus Strong Collision Resistance Property

3.3.1

```
Weak collision: Average iterations for 20 runs: 15159363.55
Strong collision: Average iterations for 20 runs: 4473.75
```

3.3.2

Given that we are only checking the first 24 bits, it would take almost 2^{24} attempts to bruteforce this resistance with a minimum of 1. On average, the number of trails needed to break weak collision resistance would be:

$$
\begin{aligned}
P(n) &= 1 - \left(\frac{2^{24}-1}{2^{24}}\right)^n \\
P(n) &> 0.5 \text{ is given by:} \\
0.5 &< 1 - \left(\frac{2^{24}-1}{2^{24}}\right)^n \\
\ln 0.5 &< \ln \left(\frac{2^{24}-1}{2^{24}}\right)^n \\
\ln 0.5 &< n \ln \left(\frac{2^{24}-1}{2^{24}}\right) \\
n &> \frac{\ln 0.5}{\ln \frac{2^{24}-1}{2^{24}}} \\
n &> 11,629,079.62147161 \\
n &= 11,629,080 \text{ attempts}
\end{aligned}
$$

In 20 trial runs, we observed an average attempt of 15159363.55, which is above the predicted estimate, this is likely due to the low number of trial runs giving us a slightly inaccurate prediction of the actual population.

3.3.3

The average trails needed to break a strong collision resistance is given by $N = \sqrt{M}$ such that M are the units. We have $M = 2^24$ and thus $N = 2^{24/2} = 2^{12} = 4096$ # of tries to reach 50% collision probability. It took my code an average of 4473.75 number of trails to reach collision, this is fairly close to the estimated range.

3.3.4

A strong collision is easier to break as it suggests that there are more collisions.

3.3.5

The explanation for strong collision being easier to break is that it is more likely that something newly hashed is already something that has been hashed previously. We are matching every hash we ever made with one another instead of matching one and dropping it if it doesn't match.