7402 Asn 5 Report

“Tastes like a Caesar”

Isaac Morneau; A00958405
John Agapeyev; A00928238

Figures

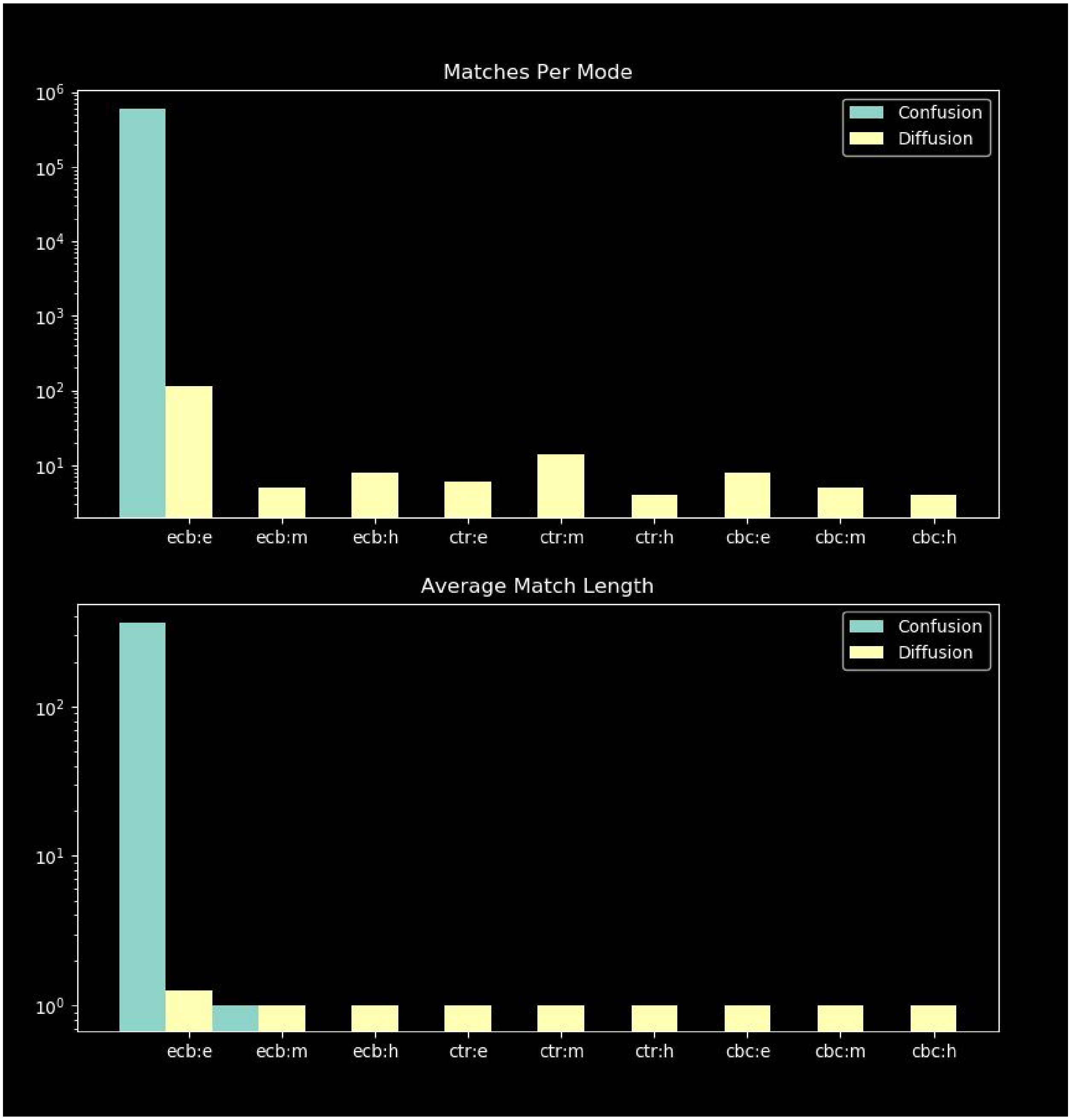
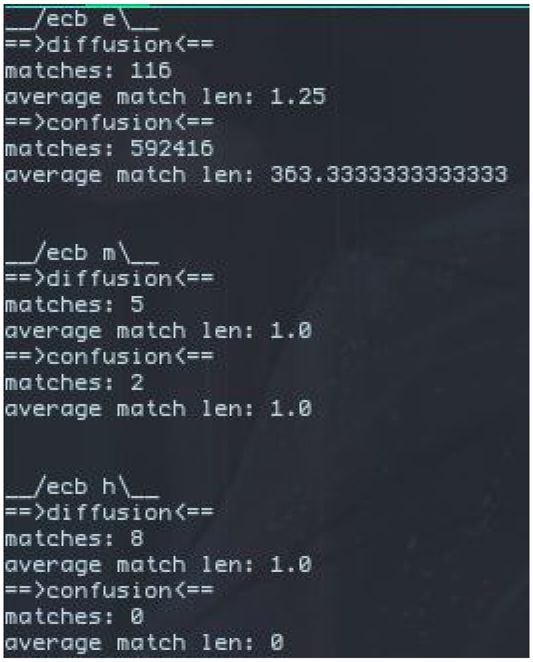
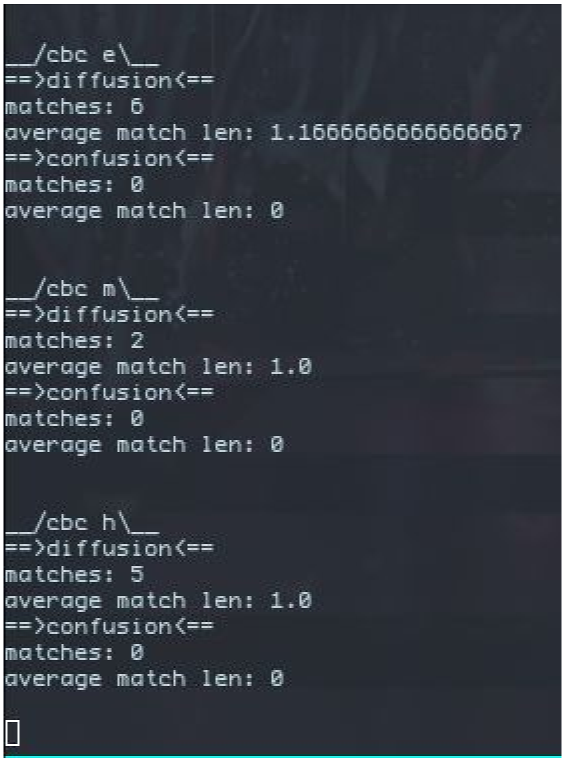


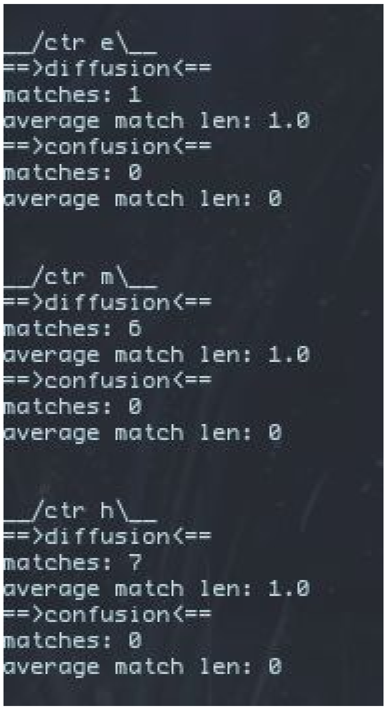
Figure 1



```
__/ecb e\__
==>diffusion<==
matches: 116
average match len: 1.25
==>confusion<==
matches: 592416
average match len: 363.3333333333333


__/ecb m\__
==>diffusion<==
matches: 5
average match len: 1.0
==>confusion<==
matches: 2
average match len: 1.0


__/ecb h\__
==>diffusion<==
matches: 8
average match len: 1.0
==>confusion<==
matches: 0
average match len: 0
```



```
__/cbc e\__
==>diffusion<==
matches: 6
average match len: 1.1666666666666667
==>confusion<==
matches: 0
average match len: 0


__/cbc m\__
==>diffusion<==
matches: 2
average match len: 1.0
==>confusion<==
matches: 0
average match len: 0


__/cbc h\__
==>diffusion<==
matches: 5
average match len: 1.0
==>confusion<==
matches: 0
average match len: 0
```



```
__/ctr e\__
==>diffusion<==
matches: 1
average match len: 1.0
==>confusion<==
matches: 0
average match len: 0


__/ctr m\__
==>diffusion<==
matches: 6
average match len: 1.0
==>confusion<==
matches: 0
average match len: 0


__/ctr h\__
==>diffusion<==
matches: 7
average match len: 1.0
==>confusion<==
matches: 0
average match len: 0
```

Figured 2

Analysis

Note: all figures, including the graphs, has been generated by the tool itself.

Confusion

Finding the highest confusion spike in figure 1 we see that ECB in easy mode has the poorest difference resulting in the most matches and the highest match rate. Conversely in hard mode CTR and CBC performed equally well in our simple analysis. These numbers can be compared exactly in figure 2 though it is so much worse than the other modes its not worth doing so.

Diffusion

Finding the highest diffusion spike in figure 1 we see that it's again ECB in easy mode. Looking at the raw data output in figure 2 we see that there is a high degree of data that was not damaged by the encryption and was able to be matched. This tells us that it had very poor diffusion. Likewise the lack of matches in something like CBC hard mode indicates that it has very good diffusion.