EECS 4980:805 Inside Cryptography

DES Analysis Project - CBC

David Carek

Analysis of DES CBC Mode

In this analysis we will compare the DES in electronic code book (ECB) mode with cipher block chaining (CBC) mode. We will compare statistics and graphs of both CBC and ECB modes to try to find any patterns in the CBC mode. Since CBC mode XORs the previous encrypted 8-byte block with the unencrypted data of the next 8-byte block we hope to see all potential patterns removed as well as frequencies of characters, di-grams, tri-grams, and octets kept beneath a normal noise ratio.

First we will look at the byte statistics in figure 1a. Since the focus of this analysis is on the comparison between ECB and CBC we will not discuss the unencrypted frequency much. Even though ECB mode raises the minimum and lowers the maximum byte frequencies by 18,924 and 765,031 respectively, CBC does a better job of evening out

Figures

|  |  |  |  |
| --- | --- | --- | --- |
| **Byte Statistics** | **Unencrypted Frequency** | **Encrypted ECB Frequency** | **Encrypted CBC Frequency** |
| Min | 0 | 18924 | 19424 |
| Max | 767104 | 20723 | 20043 |
| Range | 767104 | 1799 | 619 |
| Median | 0.00 | 19691.50 | 19741.50 |
| Mean | 19740.14 | 19740.19 | 19740.22 |
| Standard Deviation | 70869.18 | 372.75 | 131.15 |

Figure 1a.

|  |  |  |  |
| --- | --- | --- | --- |
| **Di-gram Statistics** | **Unencrypted Frequency** | **Encrypted ECB Frequency** | **Encrypted CBC Frequency** |
| Min | 1 | 27 | 42 |
| Max | 183790 | 358 | 121 |
| Range | 183789 | 331 | 79 |
| Median | 267.00 | 74.00 | 77.00 |
| Mean | 2840.63 | 77.11 | 77.11 |
| Standard Deviation | 9405.39 | 21.22 | 8.73 |

Figure 1b.

|  |  |  |  |
| --- | --- | --- | --- |
| **Tri-gram Statistics** | **Unencrypted Frequency** | **Encrypted ECB Frequency** | **Encrypted CBC Frequency** |
| Min | 2 | 2 | 2 |
| Max | 67523 | 242 | 6 |
| Range | 67521 | 240 | 4 |
| Median | 368.06 | 3.49 | 2.11 |
| Mean | 41.00 | 2.00 | 2.00 |
| Standard Deviation | 1565.19 | 4.65 | 0.33 |

Figure 1c.

|  |  |  |  |
| --- | --- | --- | --- |
| **Octet Statistics** | **Unencrypted Frequency** | **Encrypted ECB Frequency** | **Encrypted CBC Frequency** |
| Min | 1 | 1 | 1 |
| Max | 241 | 241 | 1 |
| Range | 240 | 240 | 0 |
| Median | 1.62 | 1.62 | 1.00 |
| Mean | 1.00 | 1.00 | 1.00 |
| Standard Deviation | 2.80 | 2.80 | 0.00 |

Figure 1d.

Figure 2a.

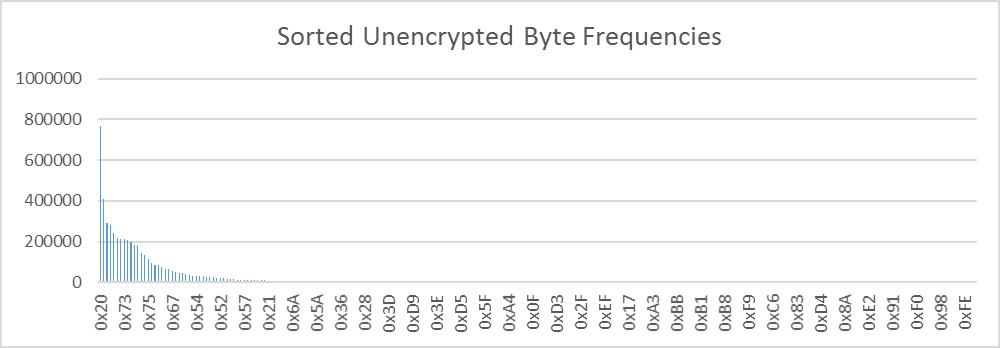


Figure 2b.

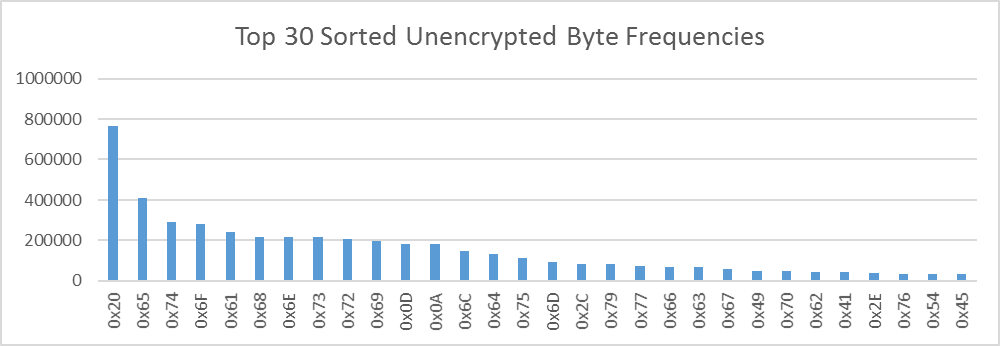


Figure 2c.

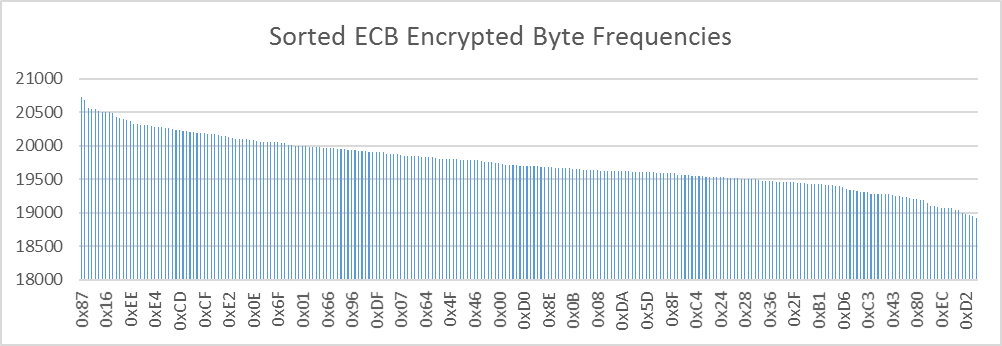


Figure 2d.

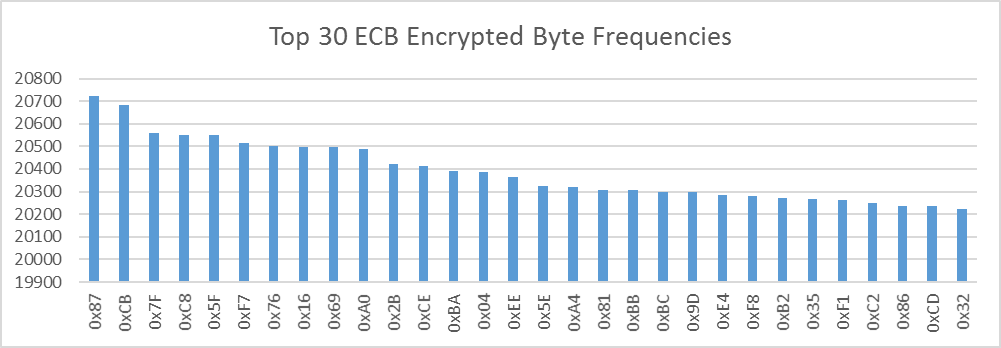


Figure 2e.

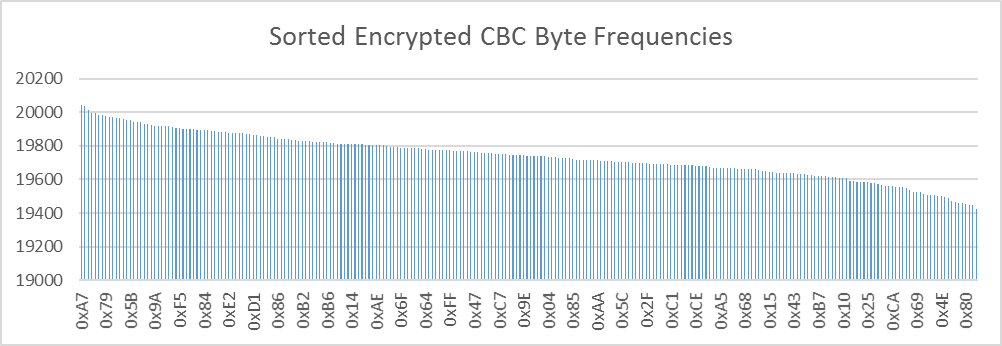


Figure 2f.

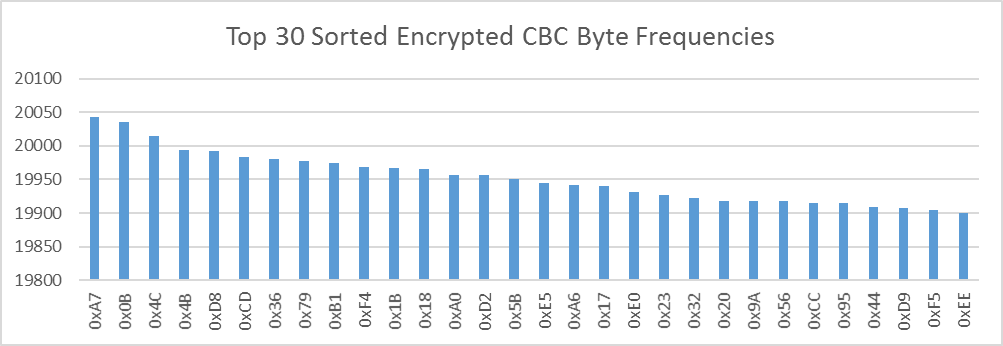


Figure 3a.