Discussion: 10:30 – 11:30am Fri

Team 18: League of Asians

Name: Frank Tan, Zhi Qian Seah(Thomas), Joonjae Bang

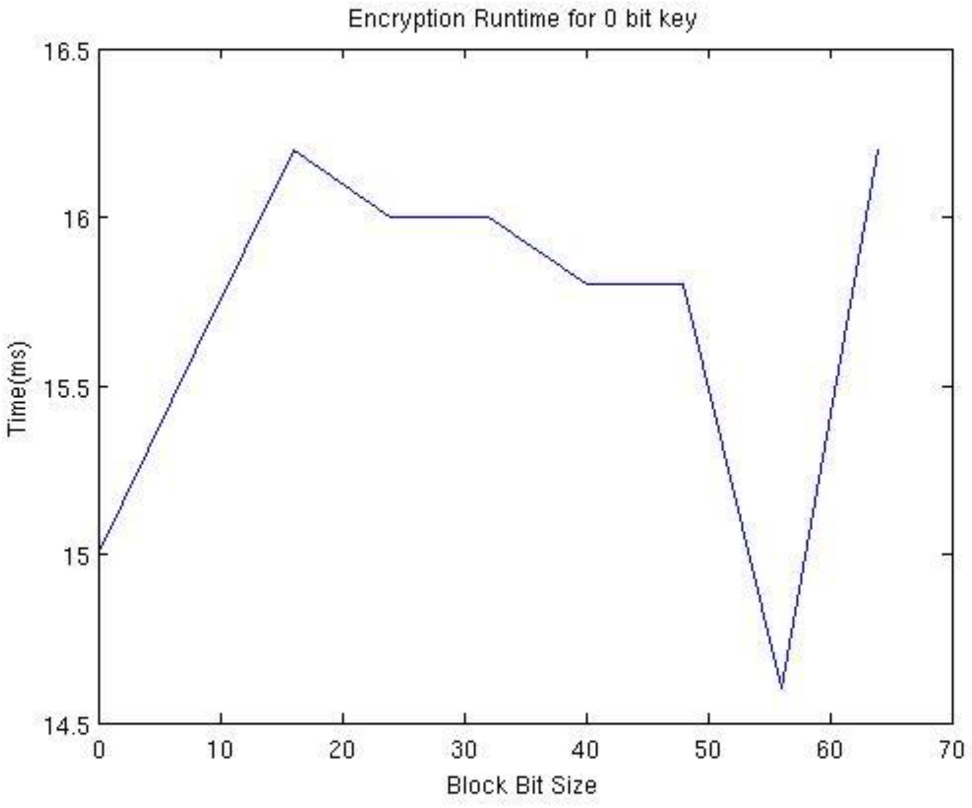
uniqnames: fstan, joonjae, zhiqian

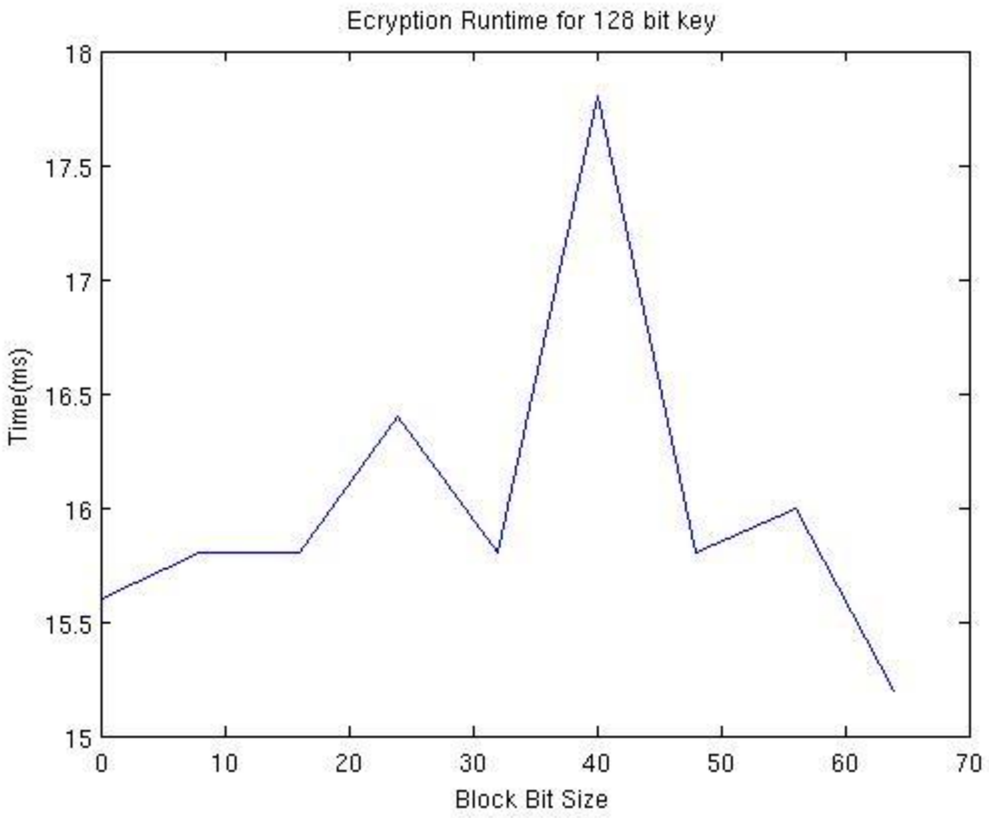
Runtime Performance Analysis of PRESENT Implementation

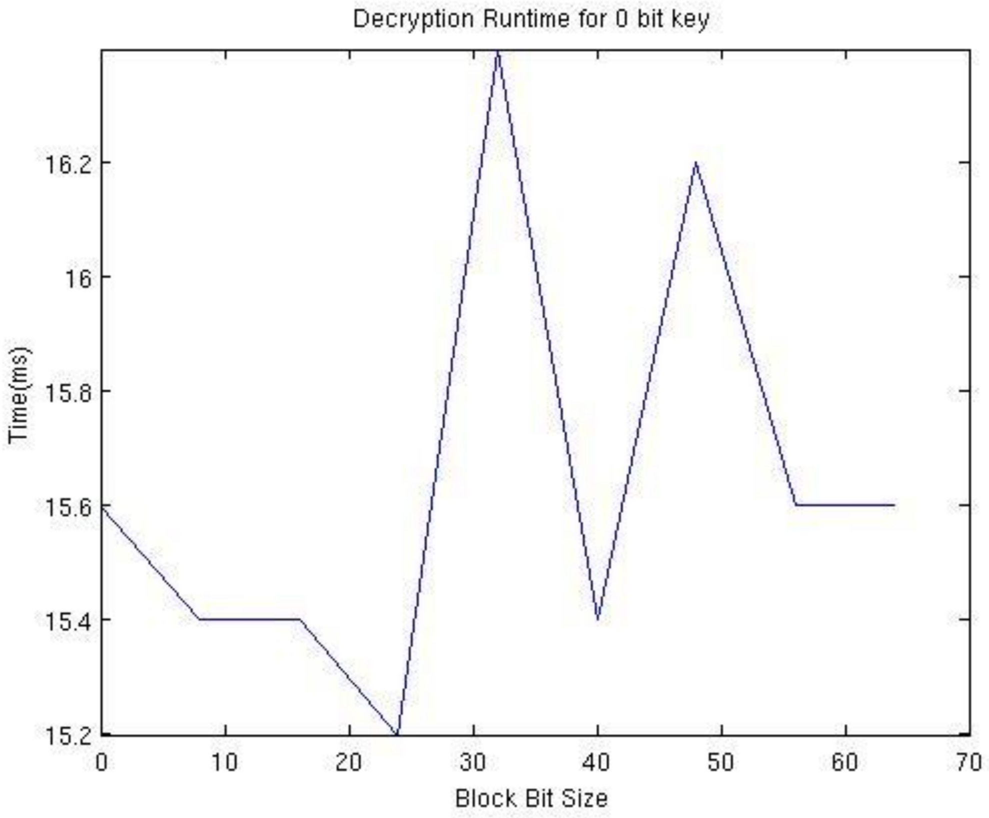
From a theoretical analysis, PRESENT encryption/decryption block cipher should exhibit a constant runtime since the bit size of the block or the key does not factor into the amount of computation required for each encryption/decryption.

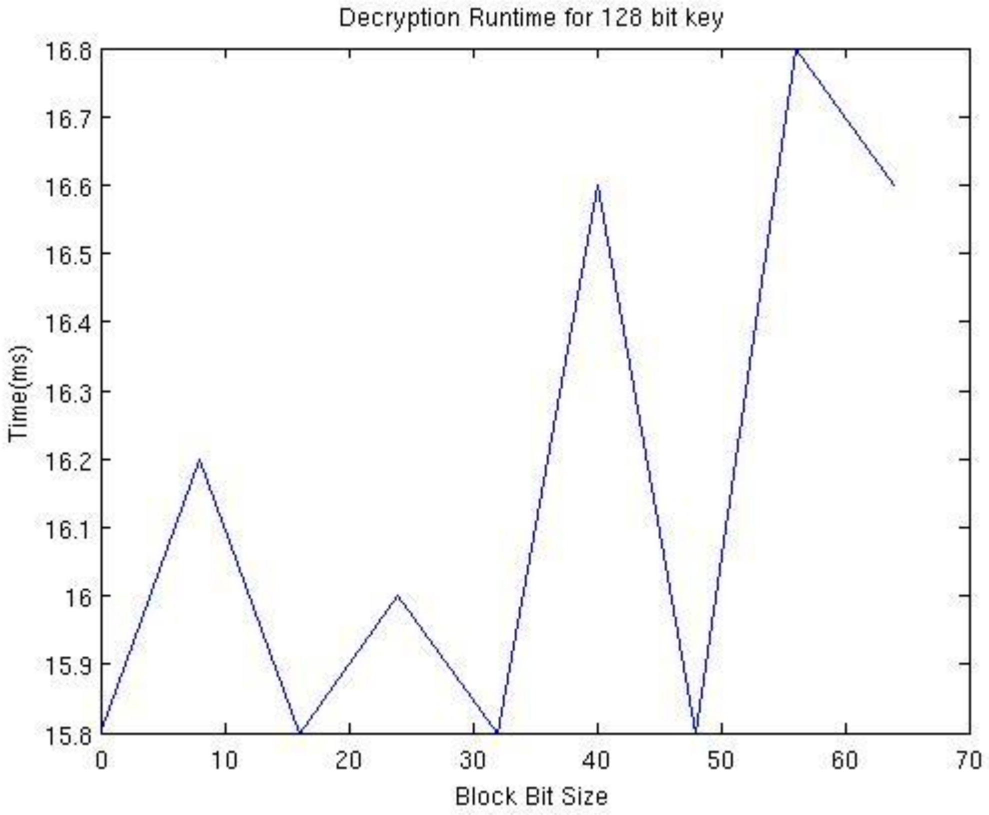
We tested both the encryption and decryption of our implementation using various bit length blocks and key length. Our findings did not contradict the theoretical analysis, and side by side comparison of all runtimes showed the runtime values to fluctuate in a 4 millisecond range, typical of most program runtimes on the CAEN environment.

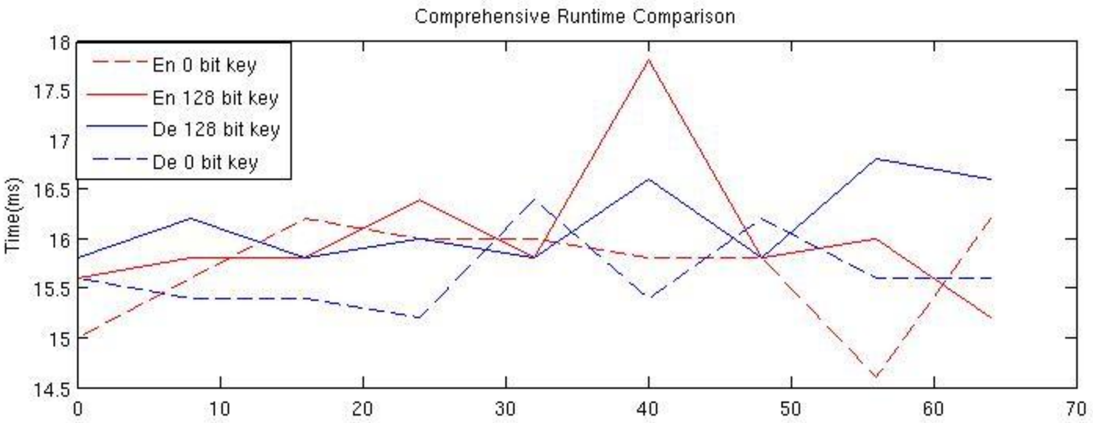
Our runtime analysis graphs are given below:




Ecryption Runtime for 128 bit key
Time(ms)
18
17.5
17
16.5
16
15.5
15
0
10
20
30
40
50
60
70
Block Bit Size


Decryption Runtime for 0 bit key
Time(ms)
16.2
16
15.8
15.6
15.4
15.2
0
10
20
30
40
50
60
70
Block Bit Size


Decryption Runtime for 128 bit key
Time(ms)
16.8
16.7
16.6
16.5
16.4
16.3
16.2
16.1
16
15.9
15.8
0
10
20
30
40
50
60
70
Block Bit Size


Comprehensive Runtime Comparison
En 0 bit key
En 128 bit key
De 128 bit key
De 0 bit key
Time(ms)
18
17.5
17
16.5
16
15.5
15
14.5
0
10
20
30
40
50
60
70