

ABSTRACT

There were many cryptography algorithms that associated with high-performance CPU had designed without concerned and full appreciation about its performance at low-level software implementation and microprocessors.

Logically, to achieve an optimal processing speed on low level software implementation to accomplish computerized problems, the best solution is to use a better new tech hardware and operating system or to use a lower level programming language such as *assembler*.

Then with an assumption that hard to achieved all of the optimization solution above, so on cases of cryptography algorithms optimization at its implementation which based on math theories, needed optimization techniques and methods that more efficient, that can reduce the complexity and the computation of the algorithms so can perform better speed execution time and perform a bigger throughput processing value.

Java™ that identical with its Java Virtual Machine (JVM) and the image of slow language adding with un optimized cryptography algorithms implementation make it more like it really so slow.

To achieved that performance based on the two paragraphs above, this final project studied, implemented and analyzed optimization techniques for cryptography algorithms implementation based Java, later hoped it produce more tight optimization techniques and achieved better performance.