Sabe-se que fatorar um número é uma tarefa custosa. Fatorar números grandes é demorado até mesmo para computadores. A condição de um número ser grande para um dado computador fatorar é relativo ao poder de processamento desta máquina.

Existem algoritmos de criptografia, como o RSA, cuja segurança está na incapacidade de se fatorar, em tempo viável, números muito grandes.

Este trabalho apresenta um estudo sobre abordagens diferentes para se fatorar um número. Foram feitos experimentos com um programa sequencial, um programa paralelizado em multiplos núcleos e um programa utilizando múltiplos processadores, isto é, fazendo uso de clusters. O programa paralelizado em multiplos núcleos foi desenvolvido utilizando a biblioteca OpenMP com a linguagem de programação C. O programa utilizando clusters foi feito utilizando a biblioteca MPI com a linguagem de programação C.

Como os computadores utilizados possuem uma arquitetura de 32 bits, portanto suportando um inteiro de no máximo 4294967295, tivemos a necessidade de estar utilizando uma biblioteca que oferecesse suporte para números grandes (big numbers). A biblioteca utilizada para esta finalidade foi a biblioteca GMP (GNU Multiple Precision Arithmetic Library) sob licensa LGPL.

| Tamanho do Número | Número | Tempo (segundos) |
|---|---|---|
| 1 | 2 | 0.000028 |
| 1 | 3 | 0.000026 |
| 1 | 4 | 0.000132 |
| 1 | 5 | 0.000027 |
| 1 | 8 | 0.000038 |
| 3 | 100 | 0.000049 |
| 3 | 200 | 0.000050 |
| 10 | 7077186818 | 0.000071 |
| 10 | 7713785683 | 0.000100 |
| 15 | 748730246741887 | 0.008447 |
| 15 | 712191023103097 | 0.003103 |
| 19 | 7509091499908239241 | 4.295326 |
| 20 | 63056345867926987482 | 0.046040 |
| 20 | 43505976633682201943 | 31.335534 |
| 20 | 79370243920946960584 | 2.313705 |
| 20 | 34085147142693443881 | 11.659095 |
| 20 | 10512918099255099743 | 0.021995 |
| 23 | 76612731218754443279598 | 1.075590 |
| 23 | 53733513486651165795013 | 76.632444 |
| 24 | 386043875567031301229623 | 199.081966 |

| | | |
|---|---|---|
| 25 | 6069251140313796740041954 | 2.166276 |
| 25 | 2431895588423462563250705 | 0.025406 |
| 25 | 1892988417346241674822433 | 0.156842 |
| 25 | 1723902935037510516386411 | 14.511825 |
| 25 | 5536851585286553139257421 | 25.917943 |
| 30 | 74283440703184202673975499258 8 | 271.223744 |
| 30 | 60574076178784763775723278650 4 | 0.478688 |
| 30 | 20302664841296779652626793491 3 | 3.801269 |
| 30 | 84047108222201417803636281327 5 | 0.491431 |
| 30 | 19575195916023965356056856392 8 | 9.965011 |
| 30 | 54724568497016652329363681164 4 | 58.221045 |
| 30 | 16099133920701076407277776226 3 | 31.539890 |
| 30 | 59812683790911772145709578190 9 | 268.850703 |
| 35 | 29134039946418465813179755474790791 | 529.752063 |
| 35 | 95065745812250451258471902299179898 | 100.304532 |
| 35 | 94983115177474781105509523256790062 | 36.820591 |

| Tamanho do Número | Número | Tempo (segundos) |
|---|---|---|
| 1 | 2 | 0.000006 |
| 1 | 3 | 0.000011 |
| 1 | 4 | 0.000054 |
| 1 | 5 | 0.000261 |
| 1 | 8 | 0.000058 |
| 3 | 100 | 0.000363 |
| 3 | 200 | 0.000301 |
| 10 | 7077186818 | 0.002194 |
| 10 | 7713785683 | 0.000516 |
| 15 | 748730246741887 | 0.008383 |
| 15 | 712191023103097 | 0.003004 |
| 19 | 7509091499908239241 | 3.086130 |
| 20 | 63056345867926987482 | 0.044060 |
| 20 | 43505976633682201943 | 20.343292 |
| 20 | 79370243920946960584 | 2.349894 |
| 20 | 34085147142693443881 | 10.477237 |

| | | |
|---|---|---|
| 20 | 10512918099255099743 | 0.021844 |
| 23 | 76612731218754443279598 | 1.586285 |
| 23 | 5373351348665116579 5013 | 56.763360 |
| 24 | 386043875567031301229623 | 141.669845 |
| 25 | 6069251140313796740041954 | 2.295430 |
| 25 | 2431895588423462563250705 | 0.045793 |
| 25 | 189298841734624167 4822433 | 0.140478 |
| 25 | 172390293503751051 6386411 | 14.051887 |
| 25 | 5536851585286553139257421 | 43.981444 |
| 30 | 74283440703184202673975 4992588 | 409.438065 |
| 30 | 60574076178784763775723 2786504 | 0.826654 |
| 30 | 20302664841296779652626 7934913 | 3.443465 |
| 30 | 84047108222201417803636 2813275 | 0.484033 |
| 30 | 19575195916023965356056 8563928 | 1.476104 |
| 30 | 54724568497016652329363 6811644 | 42.752348 |
| 30 | 16099133920701076407277 7762263 | 48.949888 |
| 30 | 59812683790911772145709 5781909 | 216.152001 |
| 35 | 29134039946418465813179755474790791 | 402.684744 |
| 35 | 95065745812250451258471902299179898 | 74.151530 |
| 35 | 94983115177474781105509523256790062 | 25.706148 |

Algumas amostras da execução do programa de fatoração usando um cluster com 9 processadores.

| Tamanho do Número | Número | Tempo (segundos) |
|---|---|---|
| 3 | 101 | 0.375663 |
| 5 | 36352 | 0.312026 |
| 10 | 9763325716 | 0.345695 |
| 10 | 5082586720 | 0.408552 |
| 10 | 8681666825 | 0.411655 |
| 15 | 115424559575241 | 0.545306 |
| 15 | 443783428613476 | 0.375577 |
| 20 | 79370243920946960584 | 1.530122 |
| 20 | 43505976633682201943 | 16.434937 |
| 20 | 10512918099255099743 | 0.440172 |
| 20 | 14613182581679137689 | 0.362169 |

| | | |
|---|---|---|
| 20 | 34085147142693443881 | 6.527642 |
| 23 | 53733513486651165795013 | 39.445539 |
| 24 | 386043875567031301229623 | 95.953669 |
| 25 | 3326866823752185958438354 | 2.074929 |
| 25 | 5491270739766741699364882 | 10.880183 |
| 25 | 3911140541452410602756228 | 127.127205 |
| 25 | 1723902935037510516386411 | 12.373954 |
| 29 | 67134594397575527200200935420 | 18.640374 |
| 30 | 59812683790911772145709578 1909 | 177.891607 |
| 30 | 160991339207010764072777762263 | 102.855715 |
| 30 | 54724568497016652329363681 1644 | 29.903860 |
| 35 | 29134039946418465813179755474790791 | 234.280416 |
| 35 | 95065745812250451258471902299179898 | 50.101438 |
| 35 | 94983115177474781105509523256790062 | 21.110983 |

Algumas amostras da execução do programa de fatoração usando um cluster com 24 processadores.

| Tamanho do Número | Número | Tempo (segundos) |
|---|---|---|
| 1 | 2 | 0.022114 |
| 1 | 3 | 0.624308 |
| 1 | 4 | 0.006507 |
| 1 | 5 | 0.335170 |
| 1 | 8 | 0.009956 |
| 3 | 100 | 0.412505 |
| 3 | 200 | 0.380989 |
| 10 | 7077186818 | 0.665389 |
| 10 | 7713785683 | 0.632166 |
| 15 | 748730246741887 | 0.686632 |
| 15 | 712191023103097 | 0.691787 |
| 19 | 7509091499908239241 | 1.510260 |
| 20 | 63056345867926987482 | 0.632454 |
| 23 | 76612731218754443279598 | 1.083079 |
| 23 | 53733513486651165795013 | 15.531813 |
| 24 | 386043875567031301229623 | 36.956390 |
| 25 | 60692511403137967400419 54 | 2.451667 |

| | | |
|---|---|---|
| 25 | 2431895588423462563250705 | 0.555968 |
| 25 | 1892988417346241674822433 | 0.481169 |
| 25 | 1723902935037510516386411 | 8.202594 |
| 25 | 5536851585286553139257421 | 125.166787 |
| 30 | 74283440703184202673975499258 8 | 189.174654 |
| 30 | 60574076178784763775723278650 4 | 1.589574 |
| 30 | 20302664841296779652626793491 3 | 1.417595 |
| 30 | 84047108222201417803636281327 5 | 0.770357 |
| 30 | 19575195916023965356056856392 8 | 3.853850 |
| 30 | 54724568497016652329363681164 4 | 11.800279 |
| 30 | 16099133920701076407277776226 3 | 73.981350 |
| 30 | 59812683790911772145709578190 9 | 97.527965 |
| 35 | 29134039946418465813179755474790791 | 107.532448 |
| 35 | 95065745812250451258471902299179898 | 19.484942 |

Uma breve comparação entre os tempos de execução do programa de fatoração usando um cluster de 9 processadores e o mesmo usando um cluster de 24 processadores.

| Tam. | Número | Tempo 9 proc. (s) | Tempo 24 proc. (s) |
|---|---|---|---|
| 23 | 53733513486651165795013 | 39.445539 | 15.531813 |
| 24 | 386043875567031301229623 | 95.953669 | 36.956390 |
| 25 | 1723902935037510516386411 | 12.373954 | 8.202594 |
| 30 | 59812683790911772145709578190 9 | 177.891607 | 97.527965 |
| 30 | 16099133920701076407277776226 3 | 102.855715 | 73.981350 |
| 30 | 54724568497016652329363681164 4 | 29.903860 | 11.800279 |
| 35 | 95065745812250451258471902299179898 | 50.101438 | 19.484942 |
| 35 | 29134039946418465813179755474790791 | 234.280416 | 107.532448 |

Uma breve comparação entre os tempos de execução do programa de fatoração usando apenas uma máquina de multiplos núcleos (2 núcleos) e o mesmo usando um cluster de 24 processadores.

| Tam. | Número | Tempo 2 núcleos (s) | Tempo 24 proc. (s) |
|---|---|---|---|
| 23 | 53733513486651165795013 | 56.763360 | 15.531813 |
| 24 | 386043875567031301229623 | 141.669845 | 36.956390 |
| 25 | 1723902935037510516386411 | 14.051887 | 8.202594 |

| | | | |
|---|---|---|---|
| 30 | 59812683790911772145709578190 9 | 216.152001 | 97.527965 |
| 30 | 160991339207010764072777762263 | 48.949888 | 73.981350 |
| 30 | 54724568497016652329363681164 4 | 42.752348 | 11.800279 |
| 35 | 95065745812250451258471902299179898 | 74.151530 | 19.484942 |
| 35 | 29134039946418465813179755474790791 | 402.684744 | 107.532448 |