## Questions

1. Etablissez un graphe illustrant les performances de votre programme multi-threadé en variant le nombre de threads.

Pour le mot de passe encrypté par le hash « 431pugYzZc5QM » et le salt « 43 ».

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Nb threads | Temps (s) | Temps (en h) |  | Nb threads | Temps (s) | Temps (en h) |
| 1 | 48483 | 13,5 | Ccccczdzdcc | 16 | 11622 | 3,2 |
| 2 | 24301 | 6,8 |  | 32 | 11397 | 3,2 |
| 4 | 15476 | 4,3 |  | 64 | 12553 | 3,5 |
| 8 | 11376 | 3,2 |  |  |  |  |

1. Que remarquez-vous ? Le gain de vitesse est-il linéaire avec le nombre de threads ?

Nous remarquons, que lors du passage d’un seul thread, à 2 threads, le temps est presque divisé par deux. Alors que lors du passage de 4 thread à 8 threads, nous ne gagnons même pas 1/3 du temps. Enfin dès les 8 threads nous nous rendons compte qu’il n’y a plus de gain de temps.

Par conclusion, nous pouvons déduire que c’est une décroissance exponentielle, avec une stabilisation autour des 3h, et non pas un gain de temps linéaire en fonction du nombre de threads.

1. Bonus: quel est l’impact de l’hyper-threading (coeurs logiques) sur les performances ?

L’hyper-threading permet sur les performances, de gagner à peu près 1/3 du temps. Cependant, ce gain de temps n’est pas aussi remarquable que lorsque le changement s’effectue sur des ajouts de cœurs physiques.

De plus, lorsque le double de cœurs physiques est dépassé, à ce moment le temps ne diminue plus réellement.

1. Test de la linéarité du temps de crack d’un mot de passe simple :

Afin d’avoir un temps qui soit valable, nous avons pris pour chaque nombre de thread, 10 mesures de temps et ensuite fait une moyenne géométrique de celles-ci.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Nb de threads | Temps (en s) |  | Nb de threads | Temps (en s) |
| 1 | 9,354001862 |  | 17 | 1,885979667 |
| 2 | 3,336424858 |  | 18 | 2,06196622 |
| 3 | 3,207627473 |  | 19 | 1,89478297 |
| 4 | 2,360850706 |  | 20 | 1,9542113 |
| 5 | 2,32294803 |  | 21 | 1,870230473 |
| 6 | 1,97110683 |  | 22 | 1,869741889 |
| 7 | 1,976521582 |  | 23 | 1,907557053 |
| 8 | 1,959614282 |  | 24 | 1,851781798 |
| 9 | 1,931083442 |  | 25 | 1,960728318 |
| 10 | 1,897580626 |  | 26 | 2,020192701 |
| 11 | 1,892958299 |  | 27 | 1,957157347 |
| 12 | 1,796366899 |  | 28 | 1,935775151 |
| 13 | 1,826250238 |  | 29 | 1,984064876 |
| 14 | 1,817931748 |  | 30 | 1,996195508 |
| 15 | 1,815408367 |  | 31 | 1,888339349 |
| 16 | 1,825210609 |  | 32 | 1,936622358 |

Nous remarquons, que contrairement à ce que donnait l’impression lors des premières mesures, que la relation n’est pas réellement linéaire et mais la différence est vraiment minime lors d’un grand nombre de threads.