**Tên: Nguyễn Ngọc Trưởng**

**MSSV: 19522440**

**Mã lớp: NT219.L21.ATTN**

**Lab5: Hash Functions**

* Report your hardware resources

|  |  |
| --- | --- |
| **Processor** | Intel® Core™ i7-8565U CPU @ 1.80GHz 1.99 GHz |
| **RAM** | 8,00 GB (7,89 GB usable) |
| **OS type** | 64-bit |
| **Graphics** | Intel® UHD Graphics 620 (WHL GT2) |
| **OS** | * Ubuntu 18.04.5 LTS * Windows 10 Home Single Language (20H2) |

* Report computation performance for all operations on both Windows and Linux

Thời gian băm plain-text.txt, được đo bằng microsecond

(được tính bằng cách tính trung bình 1000 vòng lặp)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Window 10 | | Ubuntu 18.04 | |
| (4.911 bytes) | (8.279 bytes) | (4.911 bytes) | (8.279 bytes) |
| [0] : SHA224 | 53 | 40 | 26 | 44 |
| [1] : SHA256 | 54 | 55 | 31 | 45 |
| [2] : SHA384 | 21 | 43 | 27 | 33 |
| [3] : SHA512 | 64 | 83 | 26 | 37 |
| [4] : SHA3\_224 | 55 | 99 | 30 | 42 |
| [5] : SHA3\_256 | 85 | 174 | 31 | 42 |
| [6] : SHA3\_384 | 50 | 217 | 39 | 53 |
| [7] : SHA3\_512 | 90 | 234 | 48 | 69 |
| [8] : SHAKE128 (d=256) | 70 | 66 | 39 | 40 |
| [9] : SHAKE256  (d=256) | 37 | 57 | 42 | 51 |

**Lab6: Collision and length extension attacks on Hash functions**

6.1 MD5 collision attacks (có file đính kèm)

+) Two collision messages have the same prefix string  
 - Generate yourself prefix string  
 - Compute the two output files that have the same MD5 digest

Ảnh có chứa văn bản

Mô tả được tạo tự động

+) Two different C++ programs but have the same MD5;  
 - Code yourself two short C++ programs  
 - Compiler your codes code1, code2  
 - Run hashclash to generate two program with the same MD5 digest

Ảnh có chứa văn bản

Mô tả được tạo tự động