**BÁO CÁO THỰC HÀNH**

**Môn học: Mật mã học**

**Kỳ báo cáo: Buổi 05-06 (Lab 05-06)**

**Tên chủ đề:**

**Hash Functions - Collision and length extension attacks on Hash functions**

*GVHD: Nguyễn Ngọc Tự*

*Ngày báo cáo: 14/12/2021*

1. **THÔNG TIN CHUNG:**

*(Liệt kê tất cả các thành viên trong nhóm)*

Lớp: NT209.M11.ATCL

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Họ và tên** | **MSSV** | **Email** |
| 1 | Nguyễn Khải Đăng | 19521317 | 19521317@gm.uit.edu.vn |
|  |  |  |  |

1. **NỘI DUNG THỰC HIỆN:[[1]](#footnote-1)**

|  |  |  |
| --- | --- | --- |
| **STT** | **Task** |  |
| 1 | Hash Functions |  |
| 2 | MD5 collision attacks |  |
| 3 | Length extension attacks on MAC using SHA256 in form: SHA256(k || m), k is secret key |  |
|  |  |  |
|  |  |  |

**Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của em thực hiện.**

**BÁO CÁO CHI TIẾT**

# [ WINDOWS ] Task 5: Hash Functions

## Report your hardware resources

Ảnh có chứa văn bản

Mô tả được tạo tự động

1. Phần cứng laptop

## Report computation performance for all operations

### SHA224

Kết quả

Ảnh có chứa văn bản

Mô tả được tạo tự động

1. Kết quả Hash SHA224

Name: SHA-224

Digest size: 28

Block size: 64

Message: Đăng Nguyễn

Digest: 6291B0AA544D6B90FE45060E85B7767756DA37722323C2D007960E07

Báo cáo hiệu xuất

Total time for 10.000 rounds: 7 ms

Execution time: 0.0007 ms

### SHA256

Kết quả

Ảnh có chứa văn bản

Mô tả được tạo tự động

1. Kết quả Hash SHA256

Name: SHA-256

Digest size: 32

Block size: 64

Message: đăng nguyễn

Digest: 87B81945E5B2884A01BFB354F01D64F73D4E4DA6C28480F73446F84290AD4724

Báo cáo hiệu xuất

Total time for 10.000 rounds: 8 ms

Execution time: 0.0008 ms

### SHA384

Kết quả

Ảnh có chứa văn bản

Mô tả được tạo tự động

1. Kết quả Hash SHA384

Name: SHA-384

Digest size: 48

Block size: 128

Message: đăng nguyễn

Digest: 64517A63CFEB6977B6572939F93DEE17D52F7C34814968A451B28530C5F2244FC50A3A5158E0397704CD0D19BF929D71

Báo cáo hiệu xuất

Total time for 10.000 rounds: 9 ms

Execution time: 0.0009 ms

### SHA512

Kết quả

Ảnh có chứa văn bản

Mô tả được tạo tự động

1. Kết quả Hash SHA512

Name: SHA-512

Digest size: 64

Block size: 128

Message: đăng nguyễn

Digest: 9BD5595E75FA78DEA592C1A01E2F2D2CE5AAF76A93B2DE13A27C46B96E9A720D679D885BA9C506CF838492AAD73A6FFE1124D055D43E18C935AB71C733FC7C52

Báo cáo hiệu xuất

Total time for 10.000 rounds: 10 ms

Execution time: 0.001 ms

### SHA3-224

Kết quả

Ảnh có chứa văn bản

Mô tả được tạo tự động

1. Kết quả Hash SHA3-224

Name: SHA3-224

Digest size: 28

Block size: 144

Message: đăng nguyễn

Digest: 41806561893BB7B3186771A59B76826B8C64CD8937767B58EA71DE26

Báo cáo hiệu xuất

Total time for 10.000 rounds: 11 ms

Execution time: 0.0011 ms

### SHA3-256

Kết quả

Ảnh có chứa văn bản

Mô tả được tạo tự động

1. Kết quả Hash SHA3-256

Name: SHA3-256

Digest size: 32

Block size: 136

Message: đăng nguyễn

Digest: F92A29607F3D328921451133087D960356BE21973585D626049A35A94B5DEDD8

Báo cáo hiệu xuất

Total time for 10.000 rounds: 11 ms

Execution time: 0.0011 ms

### SHA3-384

Kết quả

Ảnh có chứa văn bản

Mô tả được tạo tự động

1. Kết quả Hash SHA3-384

Name: SHA3-384

Digest size: 48

Block size: 104

Message: đăng nguyễn

Digest: EEE8CF82C83F6040EFFBB41C35AF36AA3213659E90B3ABA62EED370733175C3188A3C6D7AEBDA389AA5F2E9AEAC44922

Báo cáo hiệu xuất

Total time for 10.000 rounds: 10 ms

Execution time: 0.001 ms

### SHA3-512

Kết quả

Ảnh có chứa văn bản

Mô tả được tạo tự động

1. Kết quả Hash SHA3-512

Name: SHA3-512

Digest size: 64

Block size: 72

Message: đăng nguyễn

Digest: 4BDB0DC081A7FA3716EC202265930322F9C1B32DB095575EFBA095715866811672BF2569BD62FBE0228A5404B1A3DD4436E070D849ADF5DC1BD37A979DA38A66

Báo cáo hiệu xuất

Total time for 10.000 rounds: 12 ms

Execution time: 0.0012 ms

### SHAKE128

Kết quả

Ảnh có chứa văn bản

Mô tả được tạo tự động

1. Kết quả Hash SHAKE128

Name: SHAKE-128

Digest size: 100

Block size: 168

Message: đăng nguyễn

Digest: 209E479818E80D9D1A89F1FBE131F27BE8C86E87BFD1EA0A12C7F01CAC1561B0B11AE2D15F1CF72536F597EDD91AE88965F3F97BE03FFFA3692C0DD7F075912067F95CB8735A4D629075EB08EA2F57B3403A536E6F00FFD814103C783BC305238D6770C0

Báo cáo hiệu xuất

Total time for 10.000 rounds: 11 ms

Execution time: 0.0011 ms

### SHAKE256

Kết quả

Ảnh có chứa văn bản

Mô tả được tạo tự động

1. Kết quả Hash SHAKE256

Nhập độ dài >0: 100

Name: SHAKE-256

Digest size: 100

Block size: 136

Message: đăng nguyễn

Digest: A05601D6B2967D9196C466EF7A02508726E477BCB7FC3C910CBDDA1A611545FCE1E23D39CC2C9458DE33976E67CD8C439E6733EEBB33BF34CC82AA0B00B3E9D16D6936C686135329CC3FB2864FECB3CBE072377E7633A5149ED543E56165180CC1B2AEF8

Báo cáo hiệu xuất

Total time for 10.000 rounds: 11 ms

Execution time: 0.0011 ms

# [ LINUX ] Task 5: Hash Functions

## Report your hardware resources

Ảnh có chứa văn bản, ảnh chụp màn hình, màn hình

Mô tả được tạo tự động

1. Cấu hình linux

## Report computation performance for all operations

### SHA224

Kết quả

1. Kết quả Hash SHA224

Name: SHA-224

Digest size: 28

Block size: 64

Message: Đăng Nguyễn

Digest: 6291B0AA544D6B90FE45060E85B7767756DA37722323C2D007960E07

Báo cáo hiệu xuất

Total time for 10.000 rounds: 7 ms

Execution time: 0.0007 ms

### SHA256

Kết quả

1. Kết quả Hash SHA256

Name: SHA-256

Digest size: 32

Block size: 64

Message: đăng nguyễn

Digest: 87B81945E5B2884A01BFB354F01D64F73D4E4DA6C28480F73446F84290AD4724

Báo cáo hiệu xuất

Total time for 10.000 rounds: 8 ms

Execution time: 0.0008 ms

### SHA384

Kết quả

1. Kết quả Hash SHA384

Name: SHA-384

Digest size: 48

Block size: 128

Message: đăng nguyễn

Digest: 64517A63CFEB6977B6572939F93DEE17D52F7C34814968A451B28530C5F2244FC50A3A5158E0397704CD0D19BF929D71

Báo cáo hiệu xuất

Total time for 10.000 rounds: 9 ms

Execution time: 0.0009 ms

### SHA512

Kết quả

1. Kết quả Hash SHA512

Name: SHA-512

Digest size: 64

Block size: 128

Message: đăng nguyễn

Digest: 9BD5595E75FA78DEA592C1A01E2F2D2CE5AAF76A93B2DE13A27C46B96E9A720D679D885BA9C506CF838492AAD73A6FFE1124D055D43E18C935AB71C733FC7C52

Báo cáo hiệu xuất

Total time for 10.000 rounds: 10 ms

Execution time: 0.001 ms

### SHA3-224

Kết quả

1. Kết quả Hash SHA3-224

Name: SHA3-224

Digest size: 28

Block size: 144

Message: đăng nguyễn

Digest: 41806561893BB7B3186771A59B76826B8C64CD8937767B58EA71DE26

Báo cáo hiệu xuất

Total time for 10.000 rounds: 11 ms

Execution time: 0.0011 ms

### SHA3-256

Kết quả

1. Kết quả Hash SHA3-256

Name: SHA3-256

Digest size: 32

Block size: 136

Message: đăng nguyễn

Digest: F92A29607F3D328921451133087D960356BE21973585D626049A35A94B5DEDD8

Báo cáo hiệu xuất

Total time for 10.000 rounds: 11 ms

Execution time: 0.0011 ms

### SHA3-384

Kết quả

1. Kết quả Hash SHA3-384

Name: SHA3-384

Digest size: 48

Block size: 104

Message: đăng nguyễn

Digest: EEE8CF82C83F6040EFFBB41C35AF36AA3213659E90B3ABA62EED370733175C3188A3C6D7AEBDA389AA5F2E9AEAC44922

Báo cáo hiệu xuất

Total time for 10.000 rounds: 10 ms

Execution time: 0.001 ms

### SHA3-512

Kết quả

1. Kết quả Hash SHA3-512

Name: SHA3-512

Digest size: 64

Block size: 72

Message: đăng nguyễn

Digest: 4BDB0DC081A7FA3716EC202265930322F9C1B32DB095575EFBA095715866811672BF2569BD62FBE0228A5404B1A3DD4436E070D849ADF5DC1BD37A979DA38A66

Báo cáo hiệu xuất

Total time for 10.000 rounds: 12 ms

Execution time: 0.0012 ms

### SHAKE128

Kết quả

1. Kết quả Hash SHAKE128

Name: SHAKE-128

Digest size: 100

Block size: 168

Message: đăng nguyễn

Digest: 209E479818E80D9D1A89F1FBE131F27BE8C86E87BFD1EA0A12C7F01CAC1561B0B11AE2D15F1CF72536F597EDD91AE88965F3F97BE03FFFA3692C0DD7F075912067F95CB8735A4D629075EB08EA2F57B3403A536E6F00FFD814103C783BC305238D6770C0

Báo cáo hiệu xuất

Total time for 10.000 rounds: 11 ms

Execution time: 0.0011 ms

### SHAKE256

Kết quả

1. Kết quả Hash SHAKE256

Nhập độ dài >0: 100

Name: SHAKE-256

Digest size: 100

Block size: 136

Message: đăng nguyễn

Digest: A05601D6B2967D9196C466EF7A02508726E477BCB7FC3C910CBDDA1A611545FCE1E23D39CC2C9458DE33976E67CD8C439E6733EEBB33BF34CC82AA0B00B3E9D16D6936C686135329CC3FB2864FECB3CBE072377E7633A5149ED543E56165180CC1B2AEF8

Báo cáo hiệu xuất

Total time for 10.000 rounds: 11 ms

Execution time: 0.0011 ms

**HẾT**

1. Ghi nội dung công việc, các kịch bản trong bài Thực hành [↑](#footnote-ref-1)