

BÁO CÁO ĐỒ ÁN 3

KIẾN TRÚC MÁY TÍNH VÀ HỢP NGỮ



Mục lục

[I. Thông tin nhóm 2](#_Toc511588266)

[II. Phân công công việc 2](#_Toc511588267)

[III. Mô tả cách thức cài đặt các hàm quan trọng 3](#_Toc511588268)

[1. Kiểm tra ngày tháng năm hợp lệ 3](#_Toc511588269)

[2. Xuất chuỗi TIME theo đinh dạng DD/MM/YYYY 3](#_Toc511588270)

[3. Chuyễn đổi định dạng chuỗi TIME 3](#_Toc511588271)

[4. Các hàm lấy giá trị ngày, tháng, năm 4](#_Toc511588272)

[5. Hàm cho biết thứ mấy trong tuần 4](#_Toc511588273)

[6. Hàm kiểm tra năm nhuận 4](#_Toc511588274)

[7. Tính khoảng thời gian giữa hai năm 5](#_Toc511588275)

[8. Tìm năm nhuận gần nhất 5](#_Toc511588276)

[IV. Giải thích về quy tắc khi viết và gọi hàm trong MIPS 5](#_Toc511588277)

[V. Tài liệu tham khảo 6](#_Toc511588278)

# Thông tin nhóm

* MSSV: 1612348 Họ tên: Lý Vĩnh Lợi
* MSSV: 1612362 Họ tên: Trần Văn Lượn
* MSSV: 1612756 Họ tên: Nguyễn Hữu Trường

# Phân công công việc

|  |  |  |
| --- | --- | --- |
| **Công việc** | **Người phụ trách** | **Mức độ hoàn thành (%)** |
| **Các hàm chính** | | |
| Hàm Date: Xuất chuỗi TIME theo định dạng DD/MM/YYYY | Lượn | 100 |
| Hàm Convert: Chuyển đổi kiểu định dạng của chuỗi TIME | Lượn | 100 |
| Hàm Day: Lấy ngày từ chuỗi TIME | Lượn | 100 |
| Hàm Month: Lấy tháng từ chuỗi TIME | Lượn | 100 |
| Hàm Year: Lấy năm từ chuỗi TIME | Lượn | 100 |
| Xuất menu, lựa chọn | Lượn | 100 |
| Hàm LeapYear: Kiểm tra năm nhuận với tham số truyền vào là chuỗi TIME | Trường | 100 |
| Hàm LeapYear: Kiểm tra năm nhuận với tham số truyền vào là một số nguyên (năm) | Trường | 100 |
| Hàm GetTime: Tính khoảng thời gian cách biệt giữa 2 chuỗi TIME | Trường | 100 |
| Hàm Weekday: Cho biết chuỗi TIME tương ứng thứ mấy trong tuần | Trường + Lợi | 100 |
| Hàm tìm hai năm nhuận gần nhất | Trường | 100 |
| Hàm kiểm tra ngày tháng năm hợp lệ với tham số truyền vào là các chuỗi ngày, tháng, năm | Lợi | 100 |
| **Các hàm phụ** | | |
| Hàm chuyển đổi một số nguyên sang chuỗi | Lợi | 100 |
| Hàm chuyển đổi một chuỗi sang số nguyên | Lợi | 100 |
| Hàm chuyển đổi một chữ số sang số | Lợi | 100 |
| Hàm chuyển đổi một số (dương, nhỏ hơn 10) sang chữ số | Lợi | 100 |
| Hàm tính độ dài chuỗi | Lợi | 100 |
| Hàm đảo ngược mảng | Lợi | 100 |

# Mô tả từng bước thuật toán phát sinh key

## File Crackme 2.2

### Tiền xử lý

* File 2.2.exe ban đầu đã được nén, vì sau khi run trong OllyDbg không xuất hiện thông tin của từng dòng lệnh

A screenshot of a social media post

Description generated with very high confidence

* Sau đó đưa vào PEID để kiểm tra

A screenshot of a cell phone

Description generated with very high confidence

* Sử dụng UPX [1] để giải nén chương trình

A screenshot of a computer screen

Description generated with very high confidence

* Sau đó đưa chương trình đã được giải nén vào OllyDbg và run

A screenshot of a social media post

Description generated with very high confidence

### Chương trình 1

Để nhanh chóng, đặt các breakpoint vào sau các dòng lệnh được gom nhóm và chạy (F9), ta sẽ thấy sự thay đổi của đường dẫn

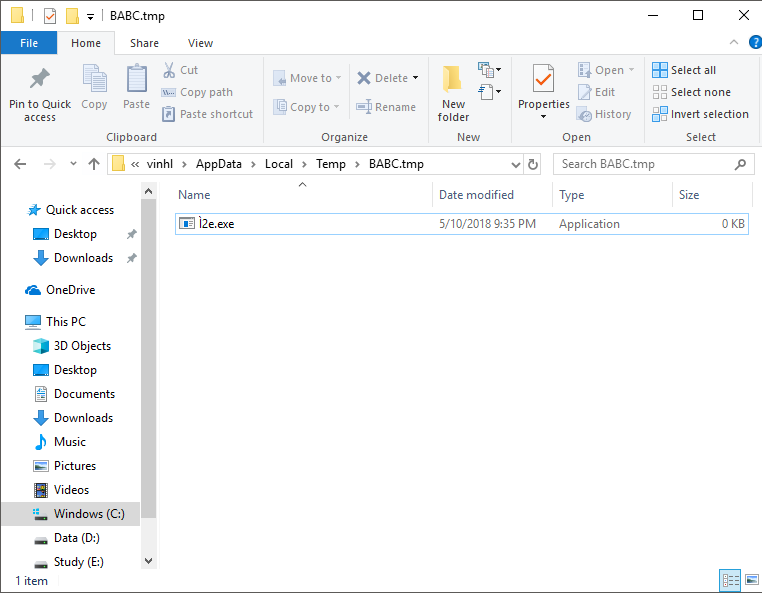
A screenshot of a social media post

Description generated with very high confidence

A screenshot of a social media post

Description generated with very high confidence

Sau khi chạy đến breakpoint tại dòng 0040115A, 1 file exe với tên được sinh ngẫu nhiên



Để khi chương trình chính kết thúc file trên vẫn còn, copy file trên ra một thư mục (chỉ copy được sau khi chạy chương trình đến breakpoint tại dòng 0040115A)

### Chương trình 2

Dùng OllyDbg mở chương trình được sinh ra ở trên

Tương tự ta đặt các breakpoint sau các nhóm lệnh quan trọng (WriteFile, CloseHandle…)

A screenshot of a social media post

Description generated with very high confidence

A screenshot of a social media post

Description generated with very high confidence

Sau đó, vào đường dẫn trong thư mục Temp của User tương tự như trên, ta tìm được file batchfile.bat. Ta copy file này ra một thư mục khác (Lưu ý chỉ copy được sau khi chạy đến breakpoint tại dòng 004014C2)

Đây là file nguồn chính của chương trình được viết bằng BashScript của Windows, nên có thể mở lên rõ rang bằng trình soạn thảo thông thường (ví dụ Notepad, Notepad++,…)

### Chương trình 3

A screenshot of a computer

Description generated with very high confidence

Theo định nghĩa các lệnh Bash của Windows

* echo: Xuất ra màn hình
* set: Đặt <tên biến>=<giá trị>
* Biến sau khi đặt bằng set, chỗ nào cần sử dụng ta ghi %<tên biến>%
* Có thể có một số thao tác xử lý (đặc biệt là chuỗi)

A screenshot of a computer

Description generated with very high confidence

|  |  |  |
| --- | --- | --- |
| Dòng | Giải thích | Ví dụ |
| 165 | Nhập username từ bàn phím và lưu vào biến N | Nếu nhập là “username” thì biến N sẽ có giá trị là “username” (không có dấu “”) |
| 166 | Đặt biến fi = %N:~2,1% nghĩa là bỏ qua 2 kí tự từ trái sang, lấy 1 kí tự trong biến N | fi = e |
| 167 | Đặt biến si = %N:~3,1% nghĩa là bỏ qua 3 kí tự từ trái sang, lấy 1 kí tự trong biến N | si = r |
| 168 | Đặt biến th = %N:~1,1% nghĩa là bỏ qua 1 kí tự từ trái sang, lấy 1 kí tự trong biến N | th = s |
| 169 | Đặt biến fo = %N:~4,1% nghĩa là bỏ qua 2 kí tự từ trái sang, lấy 1 kí tự trong biến N | fo = n |
| 170 | Đặt biến fif = %N:~0,2% nghĩa là bỏ qua 0 kí tự từ trái sang, lấy 2 kí tự trong biến N | fif = us |
| 171 | Đặt biến name=%fif%%fo%%si%%fi%%th% nghĩa là nối các chuỗi trên theo thứ tự tương ứng và lưu vào biến name | name = usnres |
|  | *Lưu ý: Nếu username nhỏ hơn 5 kí tự thì kết quả truy xuất vượt ngoài phạm vi (biến fo chẳng hạn) sẽ trả về là chuỗi rỗng* | |
| 172 | Nhập serial và lưu vào biến O | 123456789 |
| 173 | Nhập key và lưu vào biến ja | <Key này chỉ có giá trị so sánh, chúng ta cần sinh ra key này từ thuật toán> |
| 174 – 180 | Tương tự trên nhưng lấy từng kí tự một của chuỗi serial (biến O)  set one=%O:~0,1%  set two=%O:~1,1%  set three=%O:~2,1%  set four=%O:~3,1%  set five=%O:~4,1%  set six=%O:~5,1%  set seven=%O:~6,1% | One = 1  Two = 2  Three = 3  Four = 4  Five = 5  Six = 6  Seven = 7 |
| 181 | set /a m=%one%\*%two%\*%three%\*%four%\*%five%\*%six%\*%seven%\*3 lưu vào biến m giá trị của các số trên (one, two, … seven) theo công thức  m=one\*two\*three\*four\*five\*six\*seven\*3 | M = 1\*2\*3\*4\*5\*6\*7\*3 = 15120 |
| 182 | set se1=%m:~0,4% Lấy 4 kí tự đầu của biến m | Se1=1512 |
| 183 | set se2=%m:~0,2% Lấy 2 kí tự đầu của biến m | Se2=15 |
| 184 | set se4=%m:~1,3% Bỏ qua kí tự đầu, lấy 3 kí tự tiếp theo | Se4=512 |
| 185 | set se3=%m:~2,1% Bỏ qua 2 kí tự đầu, lấy 1 kí tự tiếp theo | Se3=1 |
| 186 | set se5=%se4%%th%%se3%%si%%se1%%fi%%fif%%se2% Nối các chuỗi lại theo công thức | Se5=512s1r1512eus15 |
| 187 | set la=%se5%%cra%%hac%%name% Nối chuối theo công thức | La=512s1r1512eus15admirable154usnres |
| 188 | So sánh chuỗi serial nhập vào (lưu tại biến ja) và chuỗi key được sinh ra (lưu tại biến la), in thông báo và kết thúc |  |

A screenshot of a computer

Description generated with very high confidence

### Chương trình keygen

Dựa vào các thao tác trên, ta có thể viết được chương trình keygen:

A screenshot of a cell phone

Description generated with very high confidence