Trường Đại Học Công Nghệ Thông Tin

**Khoa Khoa Học Máy Tính**

**----------------------**



**ĐỒ ÁN MÔN HỌC**

**Phân Tích Và Thiết Kế Thuật Toán**

**THUẬT TOÁN TÌM KIẾM BRUTE FORCE**

**GVHD:** Thầy Nguyễn Thanh Sơn

SV thực hiện:

Võ Gia Bảo 18520502

Nguyễn Đức Hà 18520689

Trần Lê Duy 18520674

Lớp: KHCL2018.1

***TP. Hồ Chí Minh ngày 31 tháng 12 năm 2020***

**MỞ ĐẦU**

Hiện nay, có rất nhiều phương pháp được tin tặc sử dụng để truy cập vào máy tính, mạng máy tính, trang web hoặc dịch vụ trực tuyến. Thực hiện một cuộc tấn công Brute Force là một trong số các phương pháp đó. Nó là một trong những phương pháp đơn giản nhất, nhưng tốn thời gian để hack một máy chủ hoặc một máy tính bình thường. Cơ chế tấn công Brute force có những ưu điểm của nó. Nó cũng có thể được sử dụng để kiểm tra an ninh mạng và [khôi phục mật khẩu](https://quantrimang.com/khoi-phuc-lai-mat-khau-tai-khoan-windows-live-hotmail-da-mat-77997" \o "Khôi phục lại mật khẩu tài khoản Windows Live/Hotmail đã mất) đã quên. Bài viết này sẽ giúp bạn hiểu định nghĩa Brute Force Attack là gì và xem xét các phương pháp phòng ngừa cơ bản.

Và trong báo cáo lần này, chúng em xin phép mô tả ngắn gọn về thuật toán Brute Force.

**LỜI CẢM ƠN**

Để hoàn thành được đồ án môn học lần này 1 cách thành công tốt đẹp, em xin trân trọng cám ơn tập thể lớp và giảng viên thầy Nguyễn Thanh Sơn (phụ trách bộ môn Phân tích và thiết kế thuật toán, mã môn học: CS112.L12.KHCL) đã hỗ trợ nhóm em trong suốt thời gian học tập.

Do kiến thức còn nhiều hạn chế và khả năng tiếp thu thực tế còn nhiều bỡ ngỡ và chưa hoàn hảo nên báo cáo sẽ còn nhiều thiếu sót, kính mong sự góp ý và giúp đỡ từ thầy Nguyễn Thanh Sơn.

Nhóm em xin chân thành cám ơn!

**NHẬN XÉT CỦA GIẢNG VIÊN HƯỚNG DẪN**

….....................................................................................................................................................................................................................................................….....................................................................................................................................................................................................................................................….....................................................................................................................................................................................................................................................….....................................................................................................................................................................................................................................................…...............................................................................................................................................................................................................................................................................…...........................................................................................................................................................................................................................….....................................................................................................................................................................................................................................................….....................................................................................................................................................................................................................................................….....................................................................................................................................................................................................................................................….....................................................................................................................................................................................................................................................….....................................................................................................................................................................................................................................................….....................................................................................................................................................................................................................................................….....................................................................................................................................................................................................................................................….....................................................................................................................................................................................................................................................…......................................................................................................................................................................................................................................................................................................................................................................................

**MỤC LỤC**

[**Phần 1: Khái quát về thuật toán Brute Force:** - 1 -](#_Toc60519226)

[1.1.Giới thiệu tổng quan: - 1 -](#_Toc60519227)

[1.2.Các bước thực hiện: - 1 -](#_Toc60519228)

[1.3.Ưu, nhược điểm của thuật toán: - 5 -](#_Toc60519229)

[1.4.Ví dụ: - 5 -](#_Toc60519237)

[**Phần 2: Ứng dụng của thuật toán Brute Force:** - 7 -](#_Toc60519243)

[**Phần 3: Cải tiến thuật toán Brute Force:** - 9 -](#_Toc60519244)

[**KẾT LUẬN** - 11 -](#_Toc60519245)

**DANH MỤC TÀI LIỆU THAM KHẢO**

1. https://vi.wikipedia.org/wiki/Brute\_force
2. <https://en.wikipedia.org/wiki/Brute-force_attack>
3. <https://www.varonis.com/blog/brute-force-attack/>
4. https://www.forcepoint.com/cyber-edu/brute-force-attack

# **Phần 1: Khái quát về thuật toán Brute Force:**

### Giới thiệu tổng quan:

**Brute Force là một thuật toán vét cạn, thuật toán này sẽ chạy tất cả các trường hợp có thể có để giải quyết một vấn đề nào đó (Bao gồm cả trường hợp đúng và các trường hợp sai hay còn gọi là trường hợp dư thừa).**

### Các bước thực hiện của bài toán tìm kiếm Brute Force:

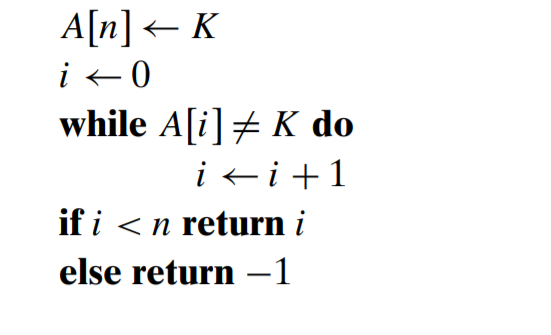
Bằng cách dịch chuyển biến đếm j qua phải lần lượt từng kí tự của file văn bản. Sau đó lấy m kí tự liên tiếp trong P (bắt đầu từ vị trí j) tạo thành 1 chuỗi phụ r. So sánh r với s, nếu giống nhau thì xuất kết quả.

1. Tìm kiếm tuần tự (Sequence search):

**Thuật toán:**

* **Input**: Một mảng A gồm n phần tử và khóa tìm kiếm K.
* **Output**: Chỉ số của phần tử đầu tiên trong A [0..n - 1] có giá trị bằng K hoặc −1 nếu không tìm thấy phần tử như vậy.

**Tổng quát:**



**Ví dụ:**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Key** |  | **List** | | | | |
| 7 |  | **6** | 4 | 1 | 9 | 7 |
|  |  | 6 | 4 | 1 | 9 | 7 |
|  |  | 6 | 4 | 1 | 9 | 7 |
|  |  | 6 | 4 | 1 | 9 | 7 |
|  |  | 6 | 4 | 1 | 9 | 7 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Key** |  | **List** | | | | |
| 7 |  | **6** | 4 | 1 | 9 | 7 |
| 7 |  | 6 | **4** | 1 | 9 | 7 |
|  |  | 6 | 4 | 1 | 9 | 7 |
|  |  | 6 | 4 | 1 | 9 | 7 |
|  |  | 6 | 4 | 1 | 9 | 7 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Key** |  | **List** | | | | |
| 7 |  | **6** | 4 | 1 | 9 | 7 |
| 7 |  | 6 | **4** | 1 | 9 | 7 |
| 7 |  | 6 | 4 | **1** | 9 | 7 |
|  |  | 6 | 4 | 1 | 9 | 7 |
|  |  | 6 | 4 | 1 | 9 | 7 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Key** |  | **List** | | | | |
| 7 |  | **6** | 4 | 1 | 9 | 7 |
| 7 |  | 6 | **4** | 1 | 9 | 7 |
| 7 |  | 6 | 4 | **1** | 9 | 7 |
| 7 |  | 6 | 4 | 1 | **9** | 7 |
|  |  | 6 | 4 | 1 | 9 | 7 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Key** |  | **List** | | | | |
| 7 |  | **6** | 4 | 1 | 9 | 7 |
| 7 |  | 6 | **4** | 1 | 9 | 7 |
| 7 |  | 6 | 4 | **1** | 9 | 7 |
| 7 |  | 6 | 4 | 1 | **9** | 7 |
| 7 |  | 6 | 4 | 1 | 9 | 7 |

**Kết luận:** Khóa tìm kiếm K=7 vét hết n = 5 phần tử và tìm ra được ở vị trí thứ 5.

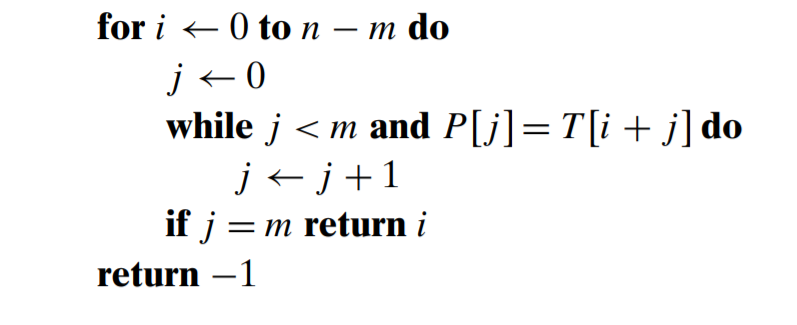
**Độ phức tạp:** O(n).

1. Tìm kiếm chuỗi trùng khớp:

**Thuật toán:**

* **Input:** Một mảng T [0..n - 1] gồm n kí tự đại diện cho một văn bản và một mảng P [0..m - 1] gồm m kí tự đại diện cho một mẫu.
* **Output:** Chỉ số của ký tự đầu tiên trong văn bản bắt đầu một khớp với chuỗi con hoặc −1 nếu tìm kiếm không thành công.

**Tổng quát:**



**Ví dụ:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| BA | BA | BAN | BANH | BEO |
| BANH | | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| BA | BA | BAN | BANH | BEO |
| BANH | | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| BA | BA | BAN | BANH | BEO |
| BANH | | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| BA | BA | BAN | BANH | BEO |
| BANH | | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| BA | BA | BAN | BANH | BEO |
| BANH | | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| BA | BA | BAN | BANH | BEO |
| BANH | | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| BA | BA | BAN | BANH | BEO |
| BANH | | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| BA | BA | BAN | BANH | BEO |
| BANH | | | | |

**Kết luận:** Mảng T và mảng P được trùng khớp.

**Độ chính xác:** O(m\*n).

### Ưu, nhược điểm của thuật toán:

### Ưu điểm:

### Đơn giản, dễ sử dụng, không quá phức tạp.

### Dễ hiểu, không đòi hỏi kĩ năng cao.

### Kết quả luôn chính xác.

### Nhược điểm:

### Nếu dùng thuật toán trâu bò như vậy thì với lượng dữ liệu đầu vào rất lớn thì tốc độ chạy thuật toán là rất chậm.

### Đối với các bài toán có dữ liệu đầu vào nhỏ, số lượng trường hợp ít thì thuật toán Brute Force chạy cũng không mất quá nhiều thời gian.

### Ví dụ:

### Ví dụ 1: Cho 2 chuỗi T và chuỗi P (20 < t, P < 100000). Tìm tất cả các vị trí mà chuỗi T xuất hiện trong chuỗi P. Ví dụ minh họa: + Chuỗi T = “abc” + Chuỗi P = “abcdefghijkabbcabchgjak” => Chuỗi T sẽ xuất hiện trong P tại 2 vị trí là 1 và 16.

### Nếu dùng thuật toán Brute Force thì bạn sẽ chạy từ kí tự đầu tiên đến kí tự cuối cùng của chuỗi P, nếu vị trí thứ i có kí tự trùng với kí tự đầu tiên trong chuỗi T thì bạn thực hiện chạy 1 vòng lặp nữa để so sánh xem chuỗi T có xuất hiện trong P ở vị trí thứ i hay không.

### Cách chạy như vậy được gọi là Brute Force hay thuật toán trâu bò.

### 

### Ví dụ 2:  Cho 2 mảng số nguyên a, b có tối đa 1000000 phần tử. Tìm tất cả các cặp phần tử (i, j) sao cho ai = bj = 1. Nếu không có cặp nào thì xuất (-1, -1). => Nếu bài này các bạn giải theo Brute Force thì sẽ chạy 1 vòng lặp tất cả phần tử của a, với mỗi phần tử của a có giá trị là 1 thì cần chạy duyệt tất cả phần tử của b xem b có phần tử nào có giá trị là 1 thì xuất ra cặp (i, j)

# **Phần 2: Ứng dụng của thuật toán Brute Force:**

1. Tấn công Brute Force là gì?

* Tấn công Brute Force là một loại tấn công mạng, trong đó bạn có một phần mềm, xoay vòng các ký tự khác nhau, kết hợp để tạo ra một mật khẩu đúng.
* Phần mềm Brute Force Attack password cracker đơn giản sẽ sử dụng tất cả các kết hợp có thể để tìm ra mật khẩu cho máy tính hoặc máy chủ mạng. Nó rất đơn giản và không sử dụng bất kỳ kỹ thuật thông minh nào.
* Vì phương pháp này chủ yếu dựa trên toán học, phải mất ít thời gian hơn để crack mật khẩu, bằng cách sử dụng các ứng dụng brute force thay vì tìm ra chúng theo cách thủ công.
* Nói phương pháp này dựa trên toán học vì máy tính làm rất tốt các phép toán và thực hiện chúng trong vài giây, nhanh hơn rất nhiều lần so với bộ não con người (mất nhiều thời gian hơn để tạo ra các sự kết hợp).

1. Tốc độ của máy tính và vấn đề mật khẩu trong cuộc tấn công Brute Force:

* Nếu mật khẩu đang sử dụng tất cả các chữ cái thường và không có ký tự đặc biệt hoặc chữ số, chỉ mất 2-10 phút là một cuộc tấn công brute force có thể crack mật khẩu này. Ngược lại, một mật khẩu có sự kết hợp của cả chữ hoa và chữ thường cùng với một vài chữ số (giả sử có 8 chữ số) sẽ mất hơn 14-15 năm để bị crack.
* Nó cũng phụ thuộc vào tốc độ của bộ vi xử lý máy tính, như bao lâu để [crack mật khẩu](https://quantrimang.com/cac-phuong-thuc-crack-passwords-44472) của mạng hoặc đăng nhập bình thường vào một máy tính Windows độc lập.
* Vì vậy, một [mật khẩu mạnh](https://quantrimang.com/6-cach-tao-mat-khau-an-toan-nhat-109825" \o "Tổng hợp cách tạo mật khẩu mạnh và quản lý mật khẩu an toàn nhất) mang lại rất nhiều ý nghĩa. Để tạo một mật khẩu thực sự mạnh, bạn có thể sử dụng các ký tự ASCII để tạo mật khẩu mạnh hơn. Ký tự [ASCII](https://quantrimang.com/bang-ma-ascii-va-bang-ky-tu-latin-chuan-iso-1252-144939) tham chiếu đến tất cả các ký tự có sẵn trên bàn phím và hơn thế nữa (bạn có thể xem chúng bằng cách nhấn ALT + số (từ 0 đến 255) trên [Numpad](https://quantrimang.com/cach-de-them-numpad-vao-ban-phim-tren-windows-10-149773)). Có khoảng 255 ký tự ASCII và mỗi ký tự có một code được đọc bằng máy và chuyển thành nhị phân (0 hoặc 1), sao cho nó có thể được sử dụng bằng máy tính. Ví dụ, code ASCII cho dấu cách là 32. Khi bạn nhập một dấu cách, máy tính đọc nó là 32 và chuyển đổi nó thành nhị phân - sẽ là 10000. Các ký tự 1, 0, 0, 0, 0, 0 được lưu trữ dưới dạng ON, OFF, OFF, OFF, OFF, OFF trong bộ nhớ của máy tính. Điều này không liên quan gì đến brute force, trừ trường hợp bạn sử dụng tất cả các ký tự ASCII. Nếu bạn sử dụng các ký tự đặc biệt trong mật khẩu, tổng thời gian cần để crack mật khẩu có thể lên đến 100 năm.

1. Cách phòng chống và bảo vệ để tránh khỏi các cuộc tấn công Brute Force:

* Vì không có logic đặc biệt nào được áp dụng trong các cuộc tấn công Brute Force, ngoại trừ việc thử các kết hợp khác nhau của các ký tự được sử dụng để tạo mật khẩu, nên biện pháp phòng ngừa ở mức rất cơ bản và tương đối dễ dàng.
* Ngoài việc sử dụng [phần mềm bảo mật](https://quantrimang.com/top-10-phan-mem-bao-mat-internet-66706" \o "Top 10 phần mềm bảo mật Internet) và [hệ điều hành Windows](https://quantrimang.com/lich-su-ve-he-dieu-hanh-windows-cua-microsoft-59098" \o "Lịch sử hệ điều hành Windows của Microsoft xuyên suốt qua các thời kỳ) được cập nhật đầy đủ, nên sử dụng một mật khẩu mạnh có một số đặc điểm sau:
* Có ít nhất một chữ hoa.
* Có ít nhất một chữ số.
* Có ít nhất một ký tự đặc biệt.
* Mật khẩu phải có tối thiểu 8-10 ký tự.
* Bao gồm ký tự ASCII.
* Mật khẩu càng dài thì càng mất nhiều thời gian để crack nó. Nếu mật khẩu giống như **'PA$$w0rd',** sẽ mất hơn 100 năm để crack nó bằng các ứng dụng tấn công Brute Force hiện có. Xin vui lòng không sử dụng mật khẩu được đề xuất trong ví dụ, vì nó rất dễ dàng bị phá vỡ, bằng cách sử dụng một số phần mềm thông minh, có thể tổng hợp các mật khẩu đề xuất trong các bài viết liên quan đến các cuộc tấn công Brute Force.
* Phần mềm miễn phí **PassBox** là một công cụ nhỏ tiện dụng sẽ ghi nhớ tất cả mật khẩu và thậm chí còn tạo mật khẩu mạnh cho tài khoản nữa. Nếu không, có thể sử dụng một số trình tạo mật khẩu trực tuyến miễn phí để tạo mật khẩu mạnh ẩn danh. Sau khi thực hiện điều đó, hãy kiểm tra mật khẩu mới của bạn bằng **Microsoft Password Checker** - Trình kiểm tra mật khẩu của Microsoft. Trình kiểm tra mật khẩu này giúp [đánh giá sức mạnh mật khẩu](https://quantrimang.com/mat-khau-cua-ban-manh-den-dau-77875" \o "Cách kiểm tra độ mạnh mật khẩu) bạn đã nhập.
* Nếu đang sử dụng phần mềm website [WordPress](https://quantrimang.com/wordpress), thì cũng có nhiều plugin bảo mật WordPress tự động chặn các cuộc tấn công brute force. Sử dụng [tường lửa](https://quantrimang.com/tong-quan-ve-firewall-84474" \o "Tường lửa (Firewall) là gì? Những kiến thức tổng quan về Firewall) web như Sucuri hoặc Cloudflare là một tùy chọn khác mà bạn có thể xem xét. Một cách nữa để chặn các cuộc tấn công brute-force là [khóa các tài khoản sau một số lần nhập mật khẩu không chính xác](https://quantrimang.com/khoa-may-tinh-khi-nguoi-khac-co-gang-doan-mat-khau-truy-cap-71198" \o "Cách tạm khóa máy tính khi nhập sai mật khẩu nhiều lần). **Plugin Limit Logins WordPress** rất tốt cho việc ngăn chặn các cuộc tấn công brute force trên blog của bạn. Các biện pháp khác bao gồm cho phép đăng nhập từ chỉ các [địa chỉ IP](https://quantrimang.com/dia-chi-ip-la-gi-143625" \o "Địa chỉ IP là gì?) được chọn, thay đổi URL đăng nhập mặc định thành một thứ khác và sử dụng Captcha để tăng cường bảo mật blog WordPress.

**Phần 3: Cải tiến thuật toán Brute Force:**

* Nếu dùng thuật toán trâu bò như vậy thì với lượng dữ liệu đầu vào rất lớn thì tốc độ chạy thuật toán là rất chậm, đối với các bài toán có dữ liệu đầu vào nhỏ, số lượng trường hợp ít thì thuật toán Brute Force chạy cũng không mất quá nhiều thời gian.
* Vì vậy trong các trường hợp cần chạy nhanh, chính xác thì nên cải tiến Brute Force (nếu có thể) hoặc sử dụng các thuật toán khác để đảm bảo tốc độ chạy chương trình như: Two Pointer, Hash, KMP/MP…

# **KẾT LUẬN**

Trong bài báo cáo kì này, chúng em xin phép giới thiệu một phương pháp rất phổ biến trong Phương pháp thiết kế thuật toán đó là thuật toán Brute Force.

Nhờ đó, có lẽ đã giúp chúng em nắm thêm những kiến thức về các phương pháp trong lập trình

Vì đây là lần đầu chúng em làm 1 bài báo cáo đầy đủ nên có điều gì sai sót và chưa hoàn chỉnh mong thầy góp ý để chúng em rút kinh nghiệm cho những bài báo cáo sau.