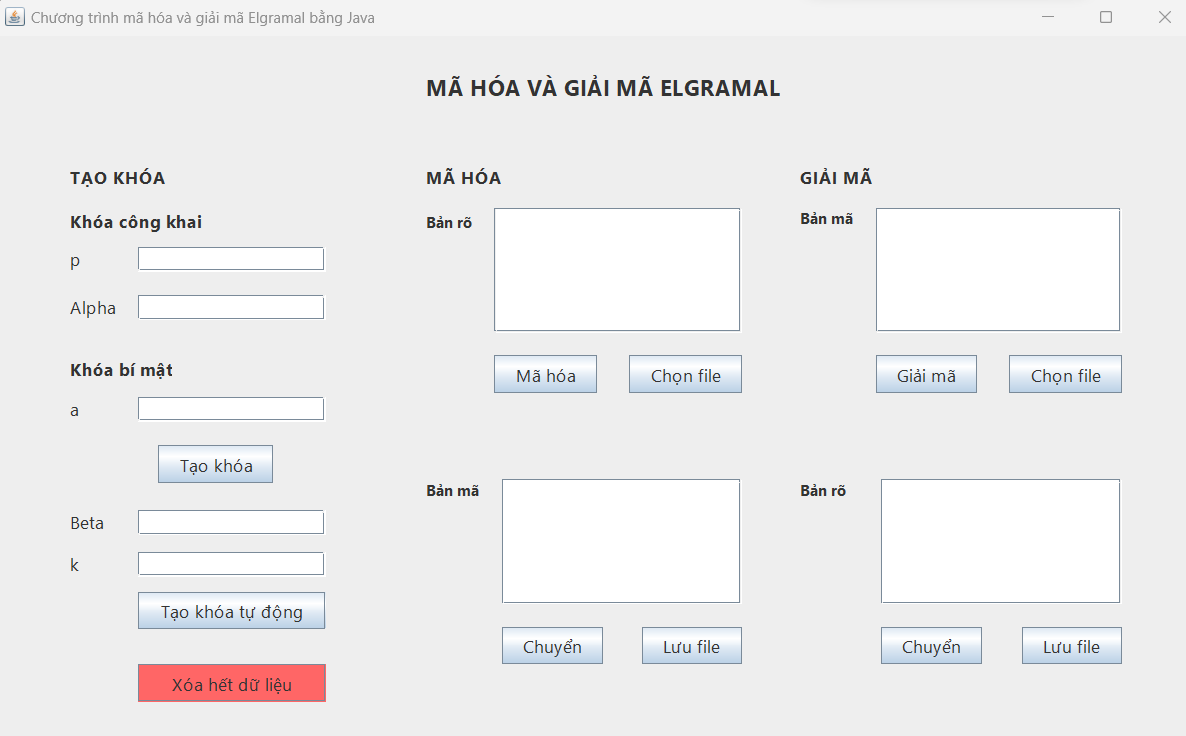
**2.1 Giới thiệu**

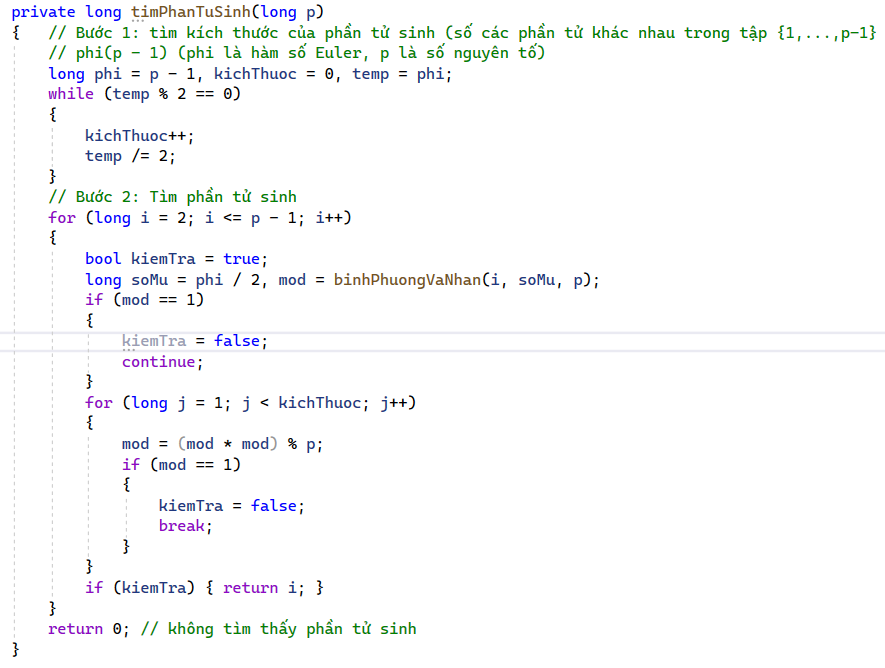


**2.2 Nội dung thuật toán**

1. Các thuật toán có liên quan khác

\* Thuật toán Baby-Step Giant-Step tìm phần tử sinh

* - Bước 1: Tạo một số nguyên tố ngẫu nhiên p và một số nguyên g thuộc Z\*p và g được chọn sao p-1 có nhiều thừa số nguyên tố khác nhau.
* Bước 2: Tìm kích thước của phần tử sinh bằng cách tính phi(p-1), trong đó phi là hàm số Euler.
* Bước 3: Tạo một danh sách các giá trị Baby-Step bằng cách tính g^i mod p với i từ 0 đến (kích thước của phần tử sinh – 1).
* Bước 4: Tạo một danh sách các giá trị Giant-Step bằng cách tính   
  g^(k \*j) mod p với j từ 0 đến (kích thước của phần tử sinh -1), trong đó k là một số nguyên được chọn sao cho k \* k <= p – 1.
* Bước 5: Duyệt qua danh sach Baby-Step và tìm giá trị đầu tiên xuất hiện trong danh sách Giant-Step, tức là một giá trị i sao cho   
  g^i mod p = g^(k\*j) mod p với một số j
* Bước 6: Trả về giá trị i là phần tử sinh của hệ mã Elgamal.



2. Quá trình sinh khóa

- Bước 1: Tạo ngẫu nhiên 1 số nguyên tố p lớn để bài toán Logarithm khó giải

- Bước 2: Chọn ngẫu nhiên phần tử nguyên thủy

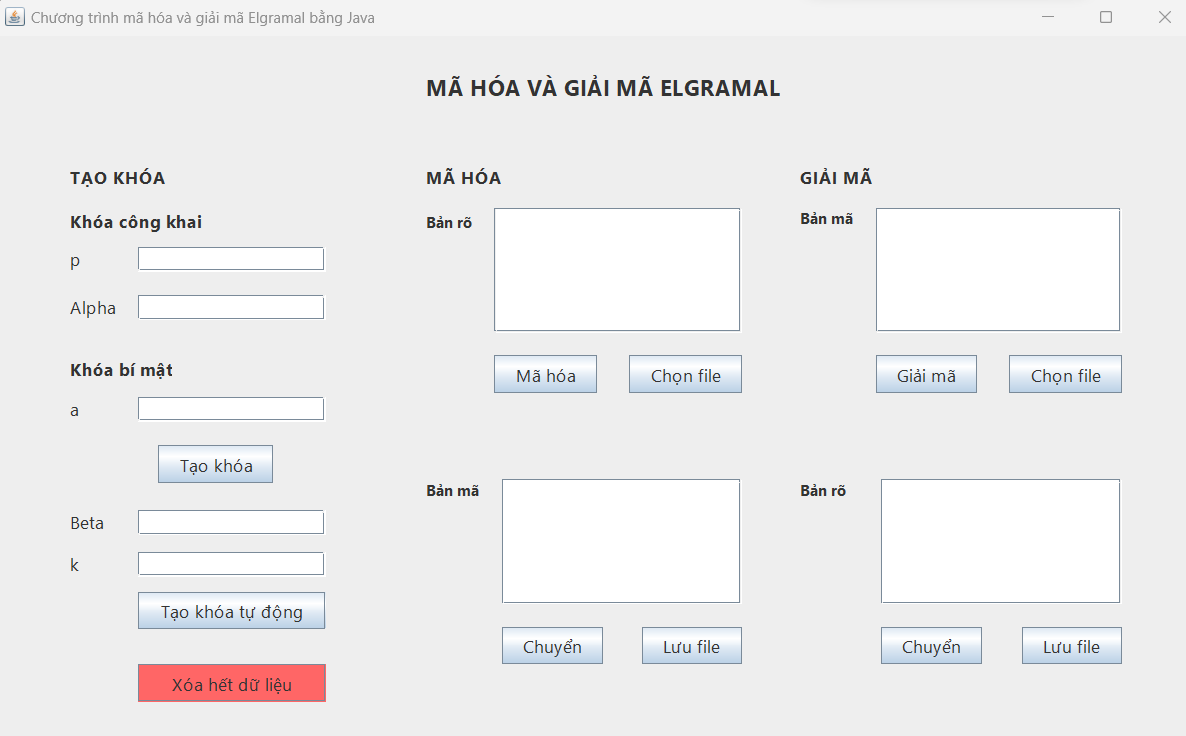
- Bước 3: Chọn số a bí mật thứ nhất sao cho

- Bước 4: Tính Beta

- Bước 5: Tạo ngẫu nhiên 1 số k bất kỳ

**2.3 Thiết kế, cài đặt chương trình demo thuật toán Giao diện chương trinh demo**

**2.3.1 Giao diện chương trình demo Java**



1- Hình 1. Giao diện chương trinh demo bằng Java

**2.4 Cài đặt và triển khai**

**2.4.1 Giới thiệu công cụ**

\* **NetBeans IDE**

NetBeans IDE là một công cụ hỗ trợ lập trình viết mã code miễn phí, được sử dụng chủ yếu cho các lập trình viên phát triển Java.Công cụ này có thể hoạt động tốt với rất nhiều nền tảng hệ điều hành khác nhau như Linux, Windows, MacOS.

Là một mã nguồn mở cung cấp các tính năng cần thiết nhất nhằm tạo ra các ứng dụng web, thiết bị di động, desktop. Giao diện dễ sử dụng với người lập trình. Có đầy đủ các thư viện của ngôn ngữ Java giúp người lập trình sử dụng các API một cách dễ dàng. Ngoài ra NetBean còn hỗ trợ người lập trình dễ dàng thiết kế giao diện với thư viện Java application.

**Ưu điểm của công cụ NetBean:**

* Nền tảng đa: có thể chạy trên cả Windows và Linux điều hành.
* Không bị hạn chế về các nhà cung cấp công cụ, bao gồm tất cả các nhà cung cấp phần mềm độc lập (ISV).
* Hỗ trợ sử dụng nhiều công cụ lập tình.
* Tạo lợi ích cho tích hợp các mạch công cụ bên trong và xuyên qua nhiều loại nội dung và các nhà cung cấp công cụ khác nhau.
* Tải nhanh hơn sử dụng SWT/Jface.

**Nhược điểm của công cụ NetBean**

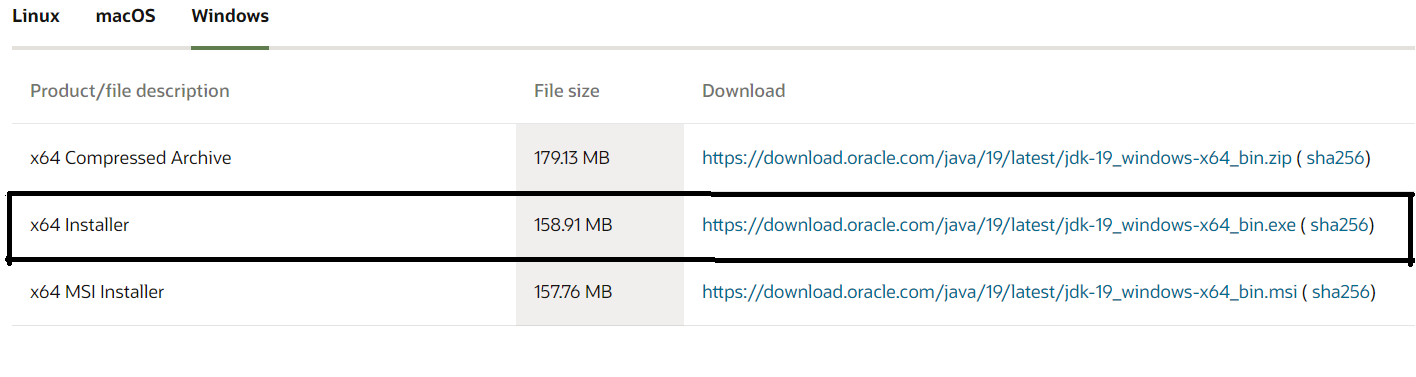
* Phần cứng và máy bộ nhớ cài đặt khá phức tạp.
* Phần mềm có dung lượng khá nặng.

**2.4.2. Hướng dẫn cài đặt và chạy chương trình demo đã cài đặt**

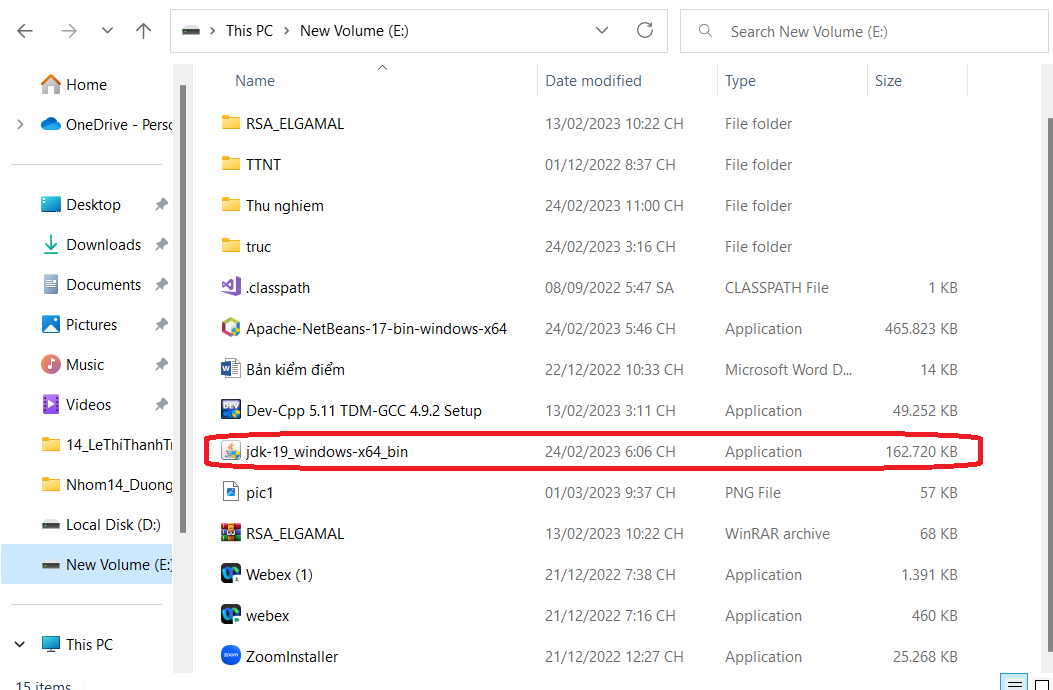
**\* Java**

- Trước khi cài NetBeans IDE, bạn phải cài đặt sẵn JDK trên máy.

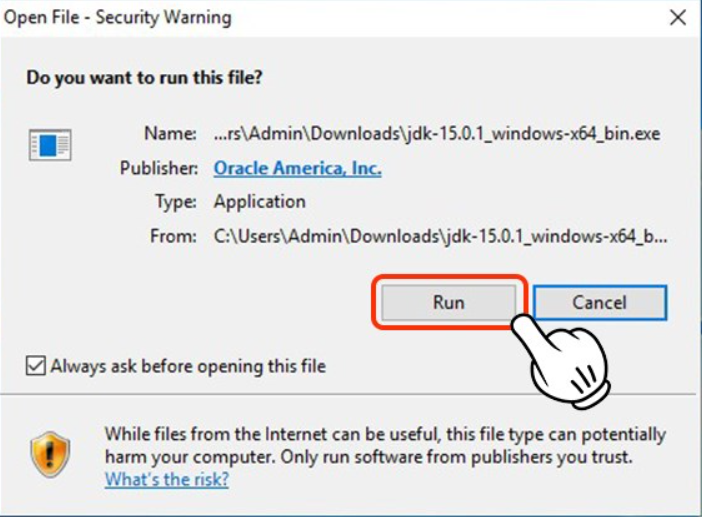
- Link :<https://www.oracle.com/java/technologies/downloads/>



* + Chọn phiên bản JDK (windows x64 installer) để phù hợp với hệ điều hành sử dụng windows. Và sau đó nhấn vào đường link dowload bên cạnh.
  + Sau khi đã tải tệp xuống. Vào Mục đã lưu nhấn đúp chuột vào **jdk-19\_windows-x64\_bin.**



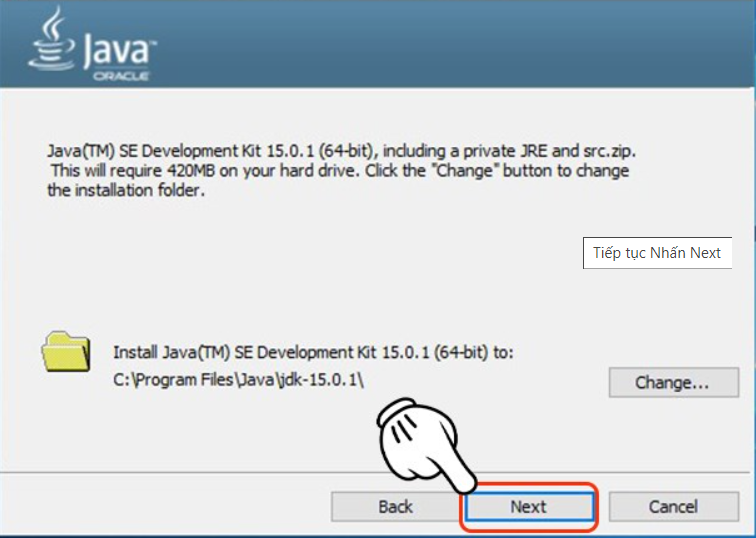
* + Sau khi hiện lên nhấn chọn **Run**



* + Nhấn chọn **Next** để bắt đầu cài đặt



* + Nhấn **Next** tiếp để tiếp tục

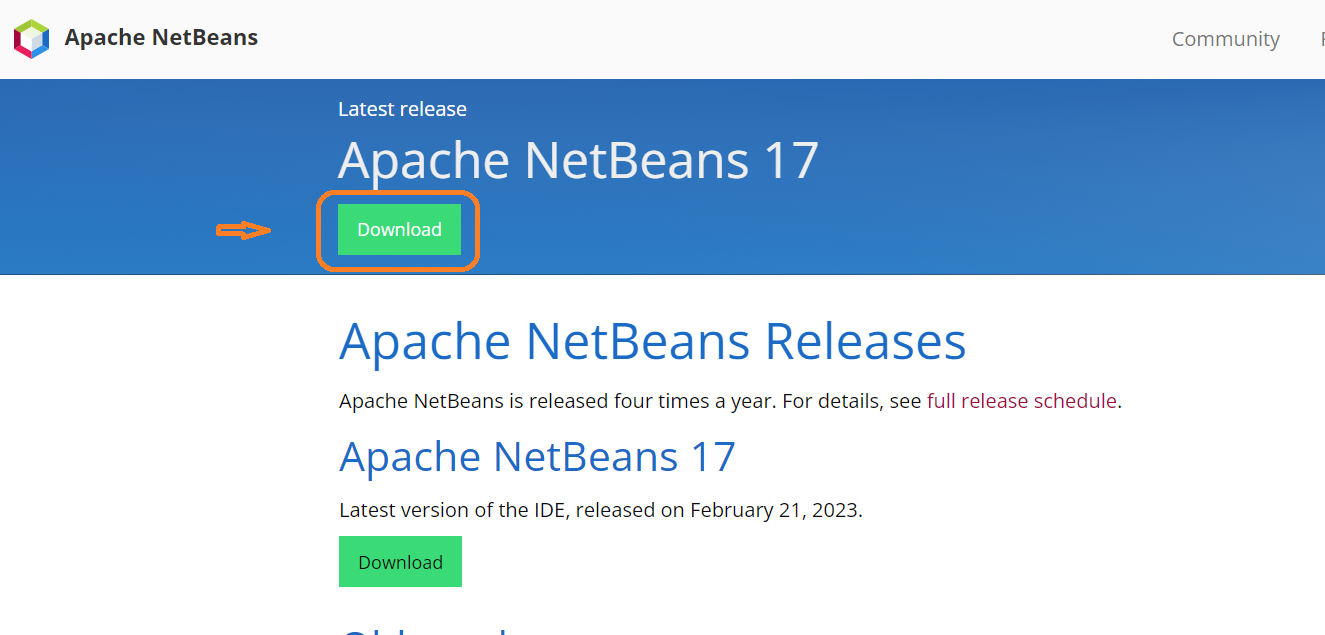


* + Nhấn vào **Close** để hoàn thành việc cài đặt JDK.

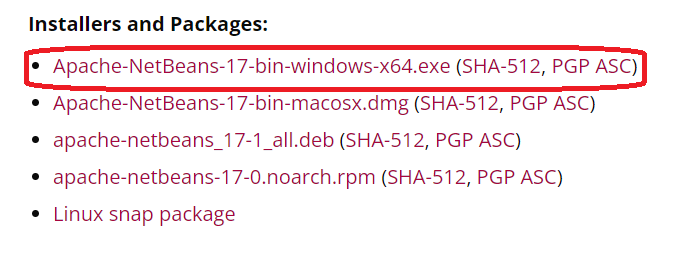


**\*Cài đặt NetBean**

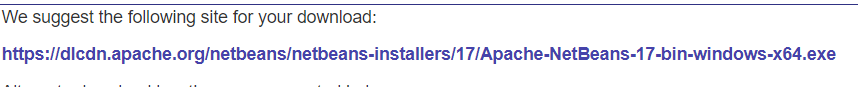
* **B1:**Nhấn vào đường link[**https://netbeans.apache.org/download/index.html**](https://netbeans.apache.org/download/index.html) **,** sau đó chọn dowloads ở phiên bản mới nhất.



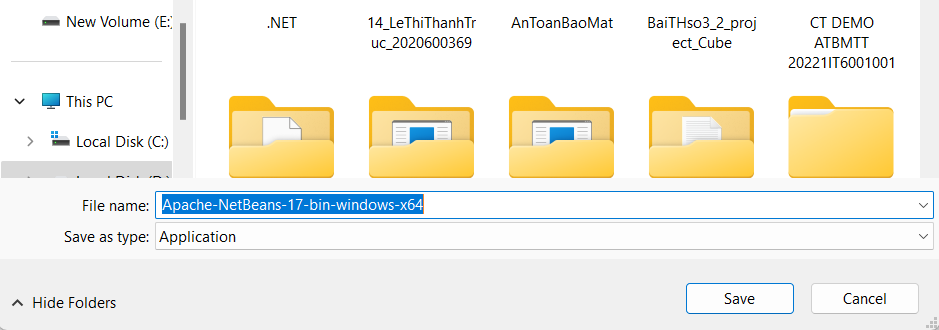
* **B2:** Ở mục Installers, chọn vào nền tảng windows để tải.



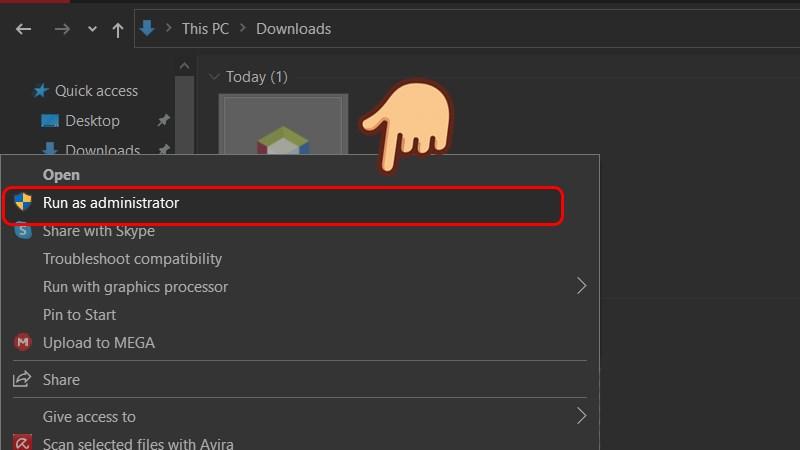
* **B3:** chọn vào đường link dưới dòng We suggest the following site for your download.



* **B4**: Chọn nơi lưu file và **Save**



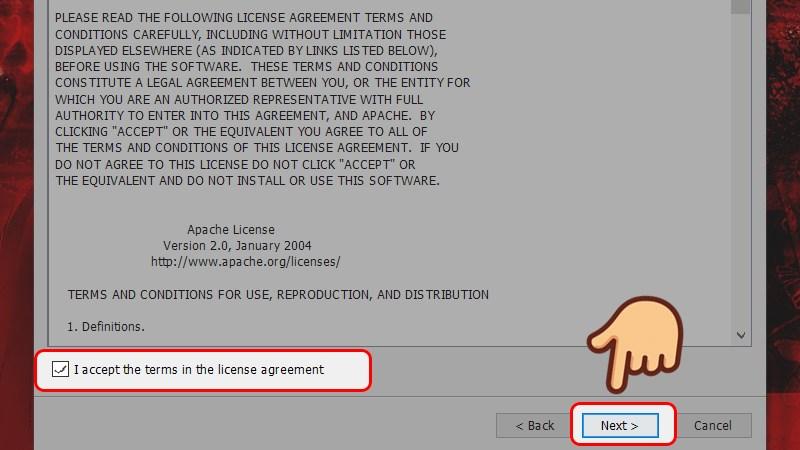
* **B5**: Sau khi tải xong, nhấp chuột phải vào biểu tượng NetBeans IDE và chọn **Run as administrator**.



* **B6**: Chọn **Next** để tiếp tục quá trình cài đặt.



* **B7**: Tích vào ô **I accept the terms in the license agreement** và chọn **Next**.



* **B8**:  Tích vào ô kiểm **Check for Update** để kiểm tra NetBeans có phiên bản cập nhật tức thời. Chọn **Install** để tiến hành quá trình cài đặt.

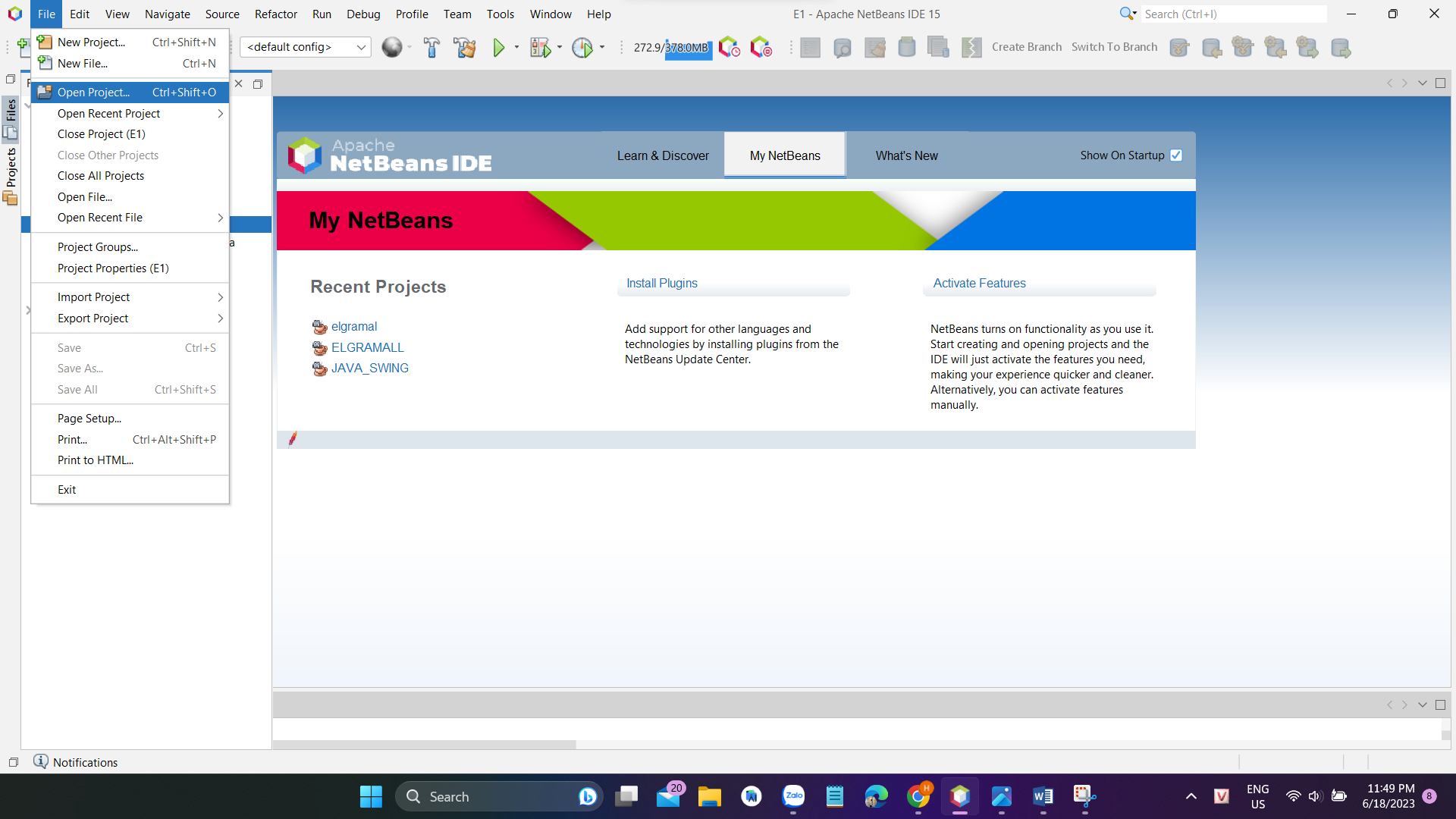


* **B9**: Chọn **Finish** để kết thúc quá trình cài đặt NetBeans IDE.

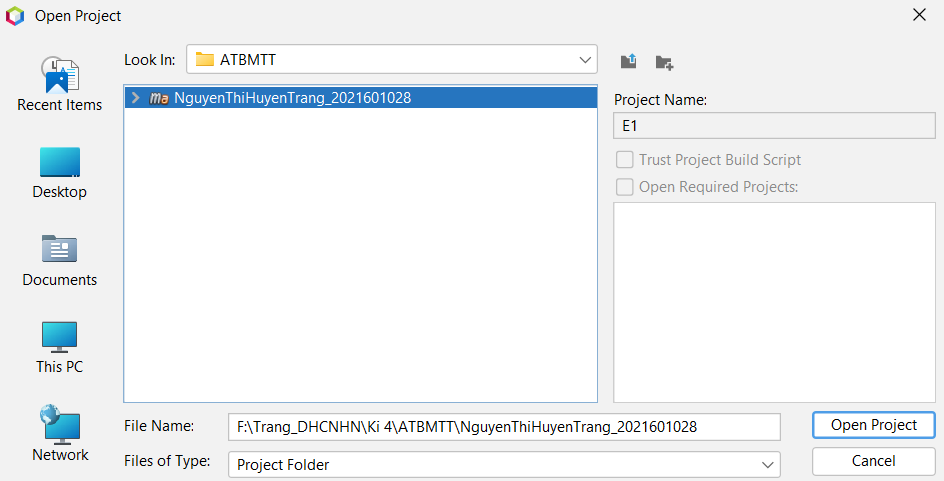


**\*Chạy chương trình demo**

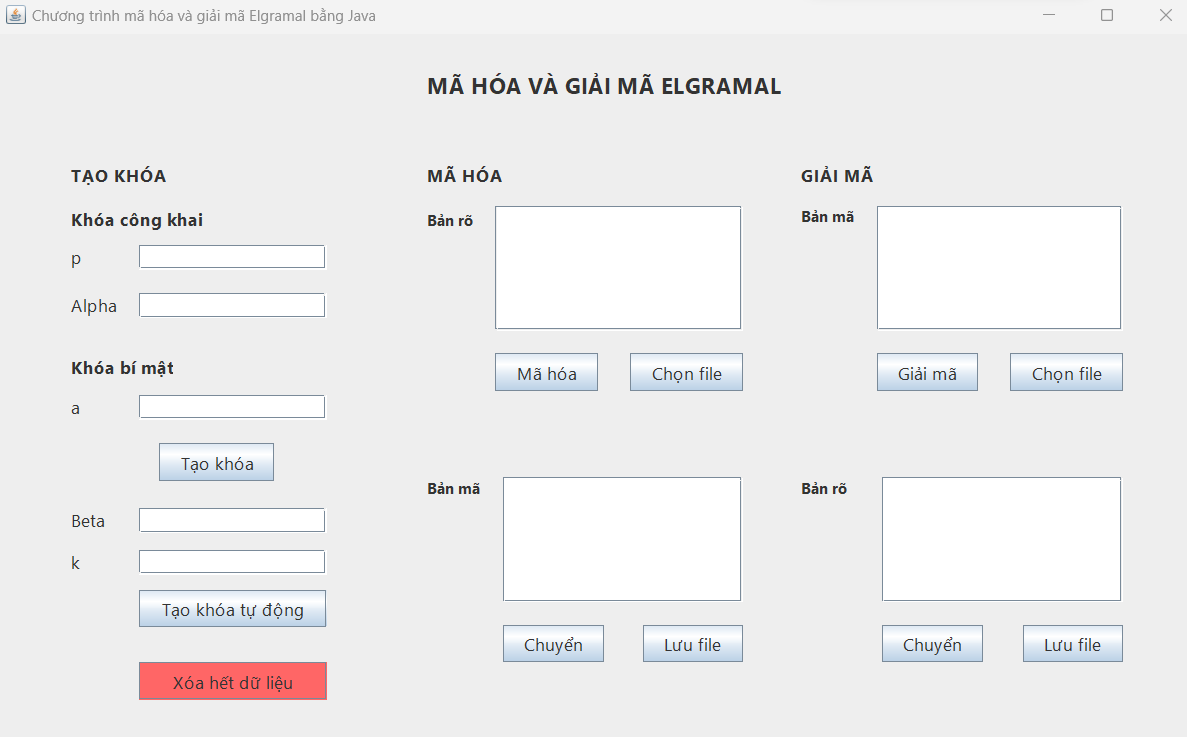
**B1**: Mở phần mềm NetBeans IDE, chọn **File** -> **Open Project**



**B2**: Chọn nơi lưu Project và ấn vào **Open Project**



**B3**: Nhấn **Run Project** hoặc **F6** để chạy chương trình



**B4**: Thêm vào văn bản hoặc tệp văn bản, thực hiện chạy chương trình và kiểm tra kết quả:

