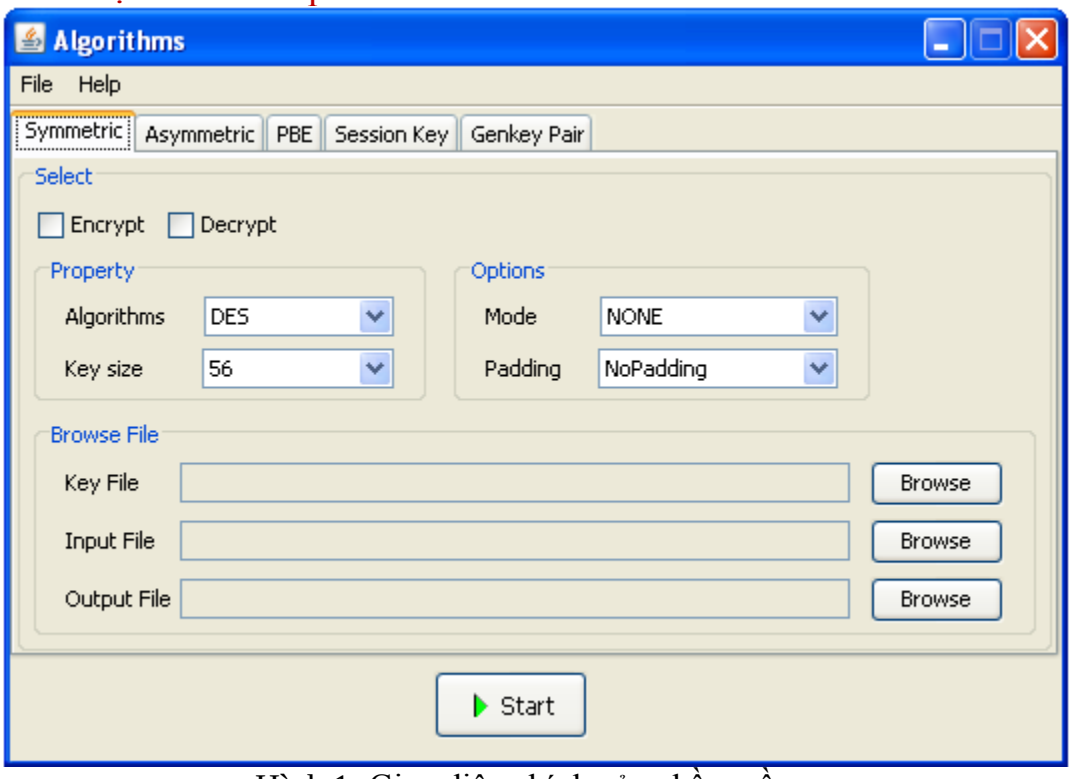
```
public class In_Out {
	public static void enCryptFile(String file, String folder,
			String thuattoan, int len) throws IOException {
		// Tao khi voi thuat toan, va do dai key
		Key key = CreateKey.getKey(thuattoan, len);
		File f = new File(file);
		// File dich
		String desFile = folder + "\\" + f.getName();
		// Ma Hoa
		EnCrypt.encrypt(thuattoan, file, desFile, key);

		// Ghi file key
		ObjectOutputStream oos = new ObjectOutputStream(new FileOutputStream(
				folder + "\\" + f.getName() + ".Key"));
		KeyObject ko = new KeyObject(thuattoan, key);
		oos.writeObject(ko);
		oos.close();
	}

	public static void deCryptFile(String file, String filekey, String folder) {
		try {
			// File key
			ObjectInputStream ois = new ObjectInputStream(new FileInputStream(
					filekey));
			// Lay Key da ghi trong file
			KeyObject ko = (KeyObject) ois.readObject();
			// Gia ma
			File f = new File(file);
			String filedes = folder + "\\" + f.getName();
			DeCrypt.decrypt(ko.thuattoan, file, filedes, ko.key);
		} catch (Exception e) {
		}
	}
}
```

HƯỚNG DẪN SỬ DỤNG PHẦN MỀM MÃ HÓA DỮ LIỆU

Mục lục

1. Giao diện chính của phần mềm



Hình 1: Giao diện chính của phần mềm

2. Chú ý trước khi sử dụng phần mềm

2.1. Trong phần mã hóa đối xứng (Symmetric)

- Để đảm bảo bạn không ghi đè file key (dữ liệu đã mã hóa có thể giải mã được), khi bạn mã hóa 1 file, key dùng trong mã hóa đó sẽ được load lên trên giao diện và bạn sẽ không thể chọn được thuật toán, độ dài key, mode hay padding khác. Khi đó, bạn có thể mã hóa liên tục nhiều file khác nữa, sử dụng chỉ bằng 1 file key này.

- Để có thể chọn được thuật toán, độ dài key, mode và padding khác. Việc làm đơn giản là bạn chỉ cần đổi tên file key(thay đổi đường dẫn khác).

- Để sử dụng lại key cũ để mã hóa cũng như giải mã, bạn chỉ cần browse đến file key đó để sử dụng.

2.2. Trong phần mã hóa bất đối xứng (Asymmetric) và Session Key

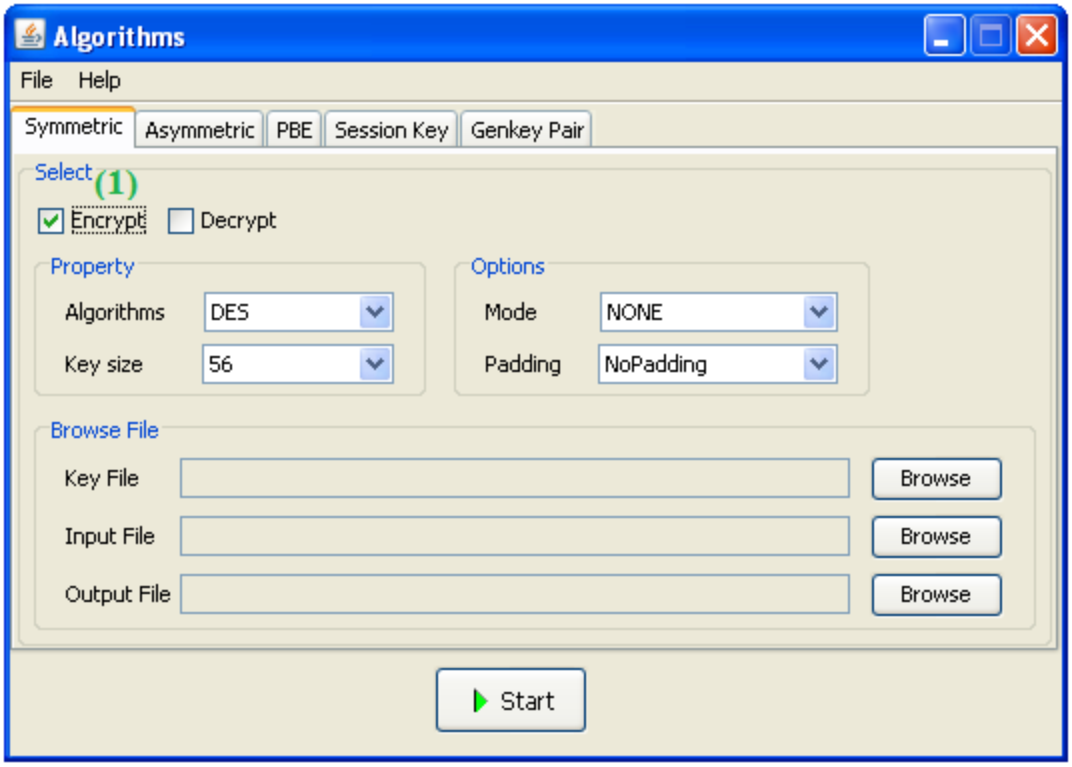
- Để có thể sử dụng được tab này, điều trước tiên bạn cần phải làm là tạo ra cặp public và private key trước (trong Genkey pair tab).
- Sau đó, khi mã hóa hoặc giải mã bạn chỉ cần browse tới 2 file key này.
- Mã hóa: sử dụng public key và để giải mã dùng private key.

3. Các bước thực hiện mã hóa và giải mã bằng phần mềm:

3.1. Thuật toán đối xứng (Symmetric):

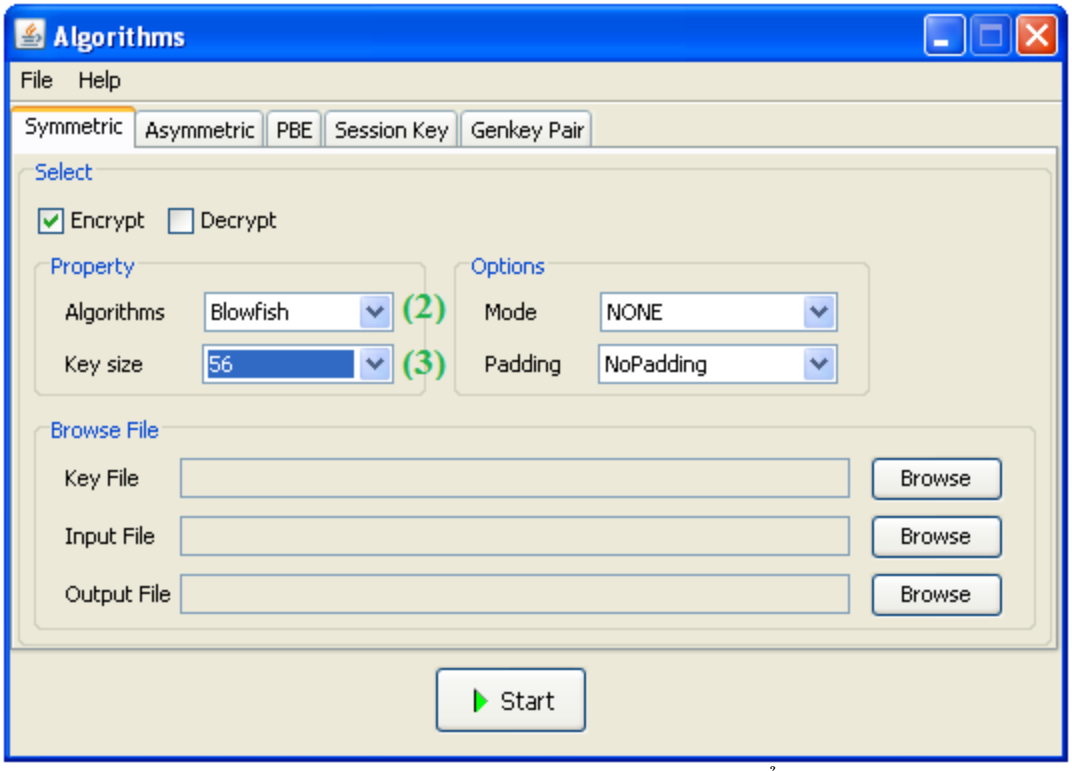
3.1.1. Mã hóa:

- **Bước 1**: Sau khi chạy phần mềm, trong tab Symmetric(thuật toán đối xứng) bạn click vào check box "**Encrypt**" để thực hiện việc mã hóa dữ liệu.



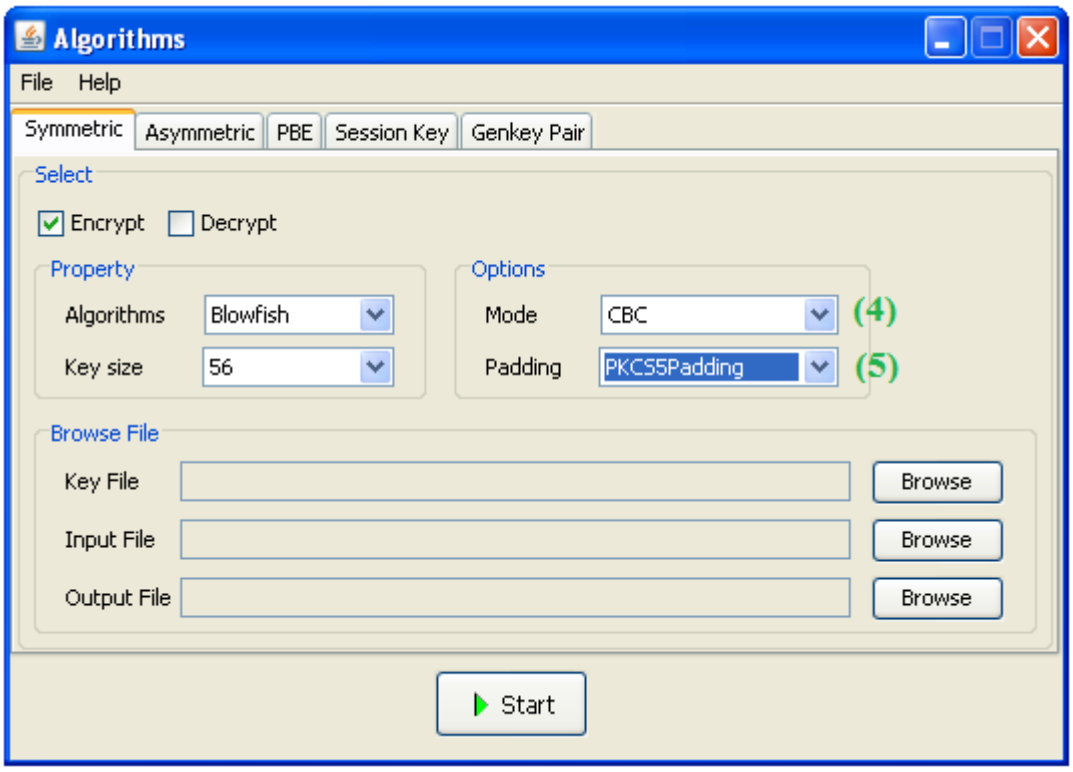
Hình 2: Giao diện click check box "Encrypt"

- **Bước 2**: Trong phần *Property*, bạn chọn thuật toán mà bạn muốn mã hóa dữ liệu, và chọn độ dài key mong muốn. Ở đây, tôi ví dụ chọn thuật toán Blowfish và độ dài key là 56 bit.



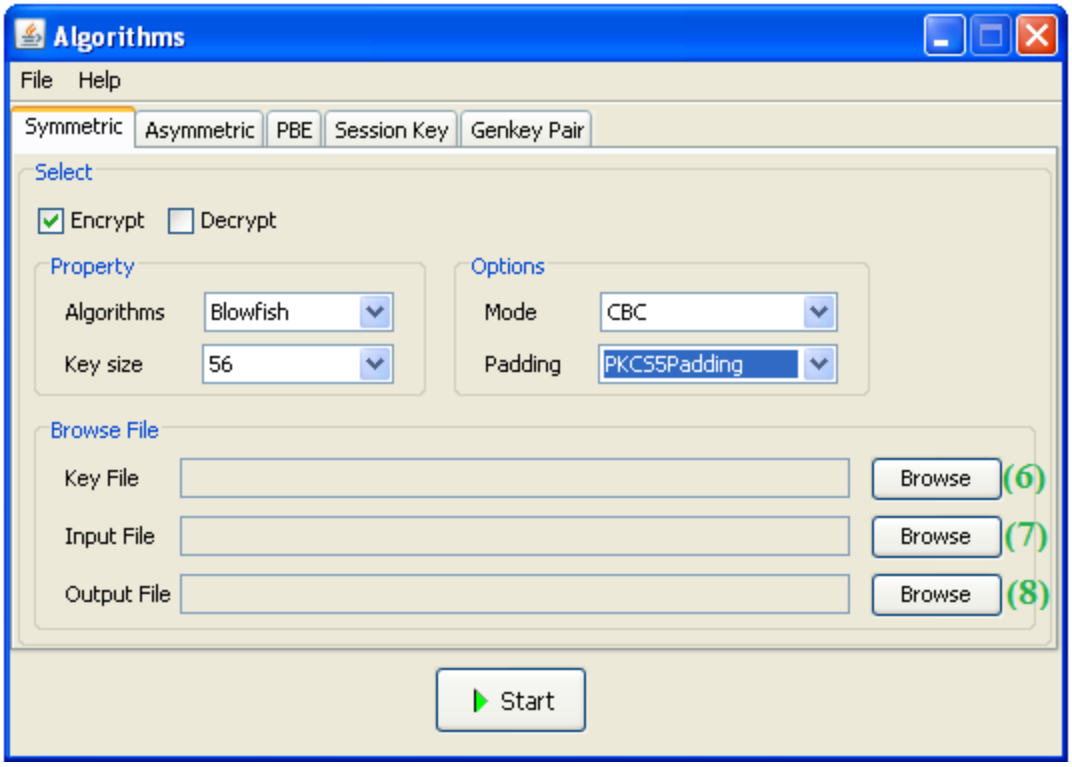
Hình 3: Giao diện chọn thuật toán và key để mã hóa

- **Bước 3**: Trong phần *Options*, bạn chọn mode và padding mà bạn muốn. Mặc định là mode là NONE và padding là NoPadding. Tôi ví dụ, chọn mode là CBC và padding là PKCS5Padding.



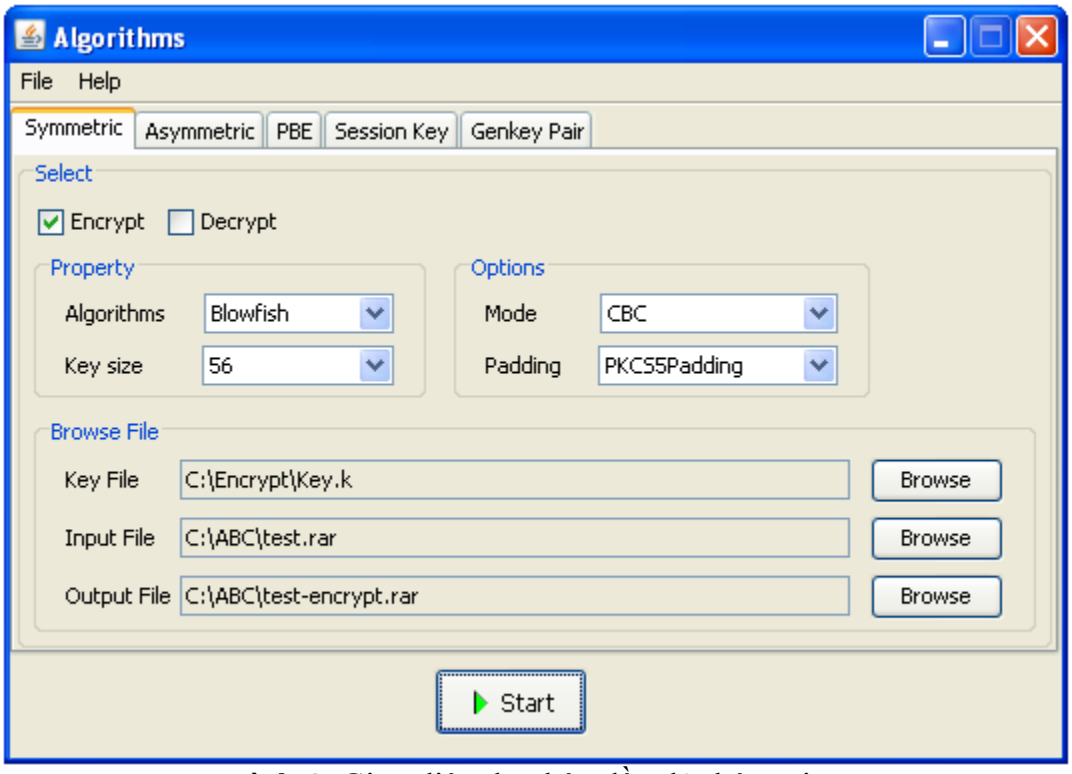
Hình 4: Giao diện chọn mode và padding

- **Bước 4**: Trong phần *Browse File*, ta lần lượt chọn Key File: đường dẫn lưu key sau khi mã hóa(encryp) hoặc sử dụng lại file key cũ để phục vụ cho việc giải mã, Input File: đường dẫn đến file cần mã hóa và Output File: đường dẫn tạo ra file mã hóa (bằng cách click nút "Browse") tương ứng.



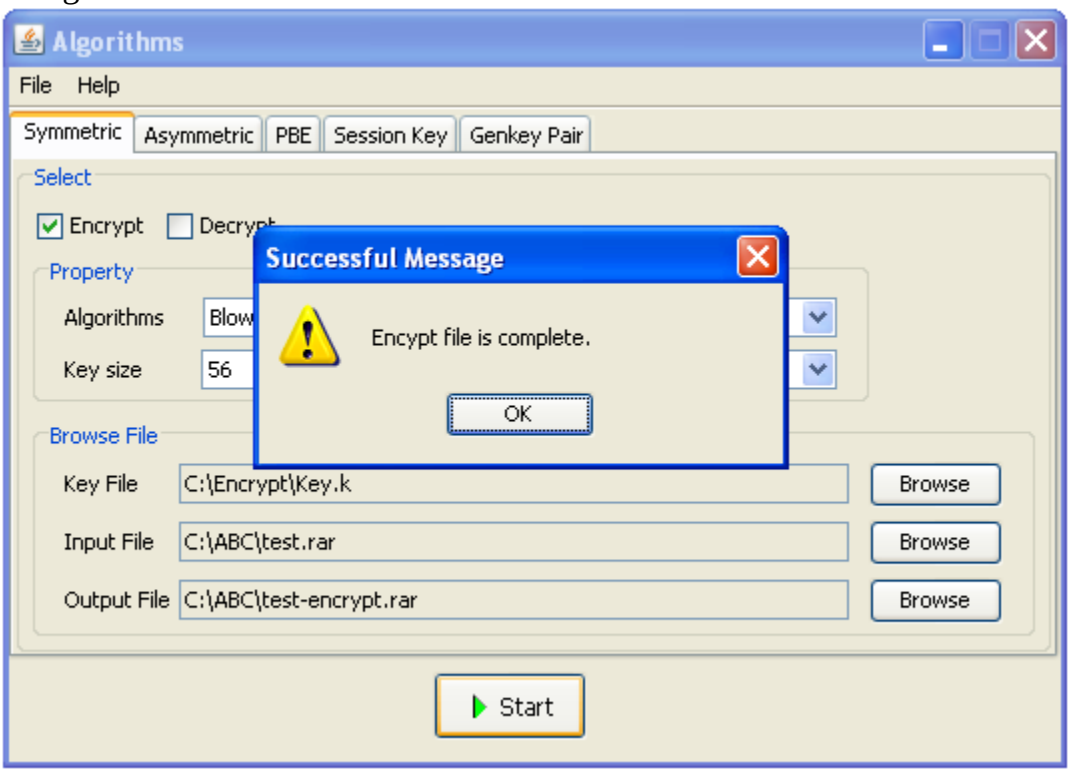
Hình 5: Giao diện chọn Key File, Input File và Output File

- **Bước 5**: Sau khi nhập đầy đủ thông tin, bạn click nút "Start" bên dưới để tiến hành mã hóa.

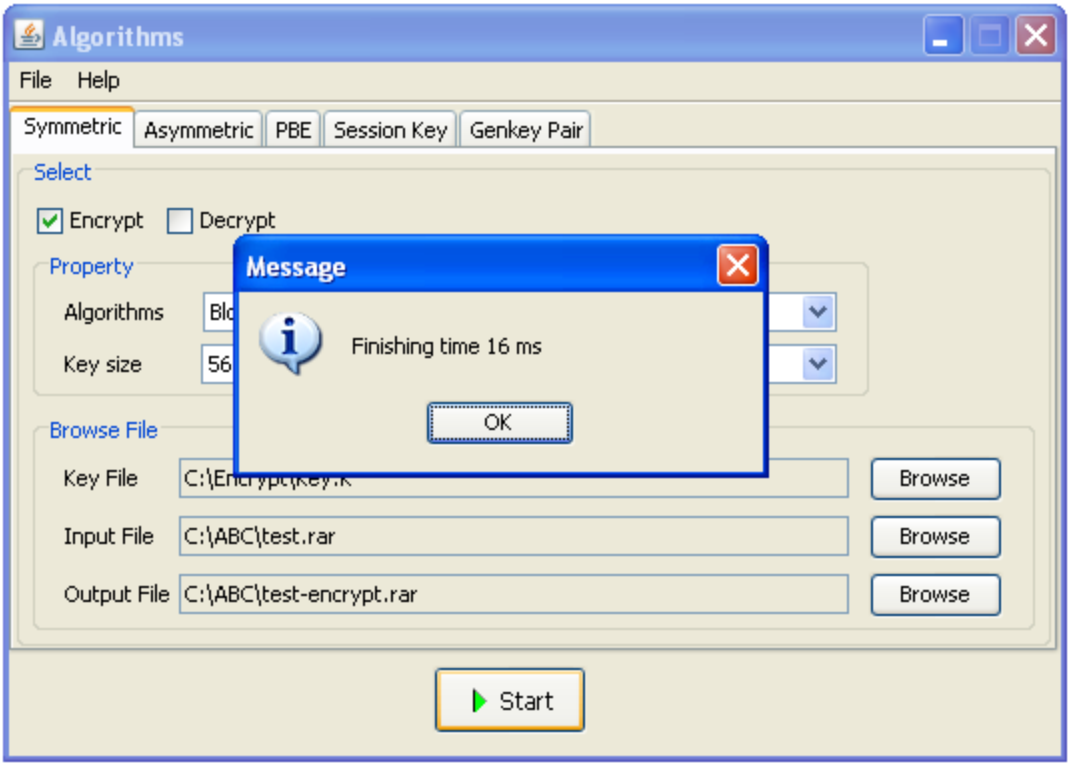


Hình 6: Giao diện đã nhập đầy đủ thông tin

- **Bước 6**: Sau khi mã hóa xong, màn hình sẽ xuất hiện thông báo thành công và thời gian thực hiện mã hóa file dữ liệu. Nếu có lỗi xảy ra, trên màn hình sẽ xuất hiện thông báo lỗi.



Hình 7: Giao diện thông báo mã hóa thành công

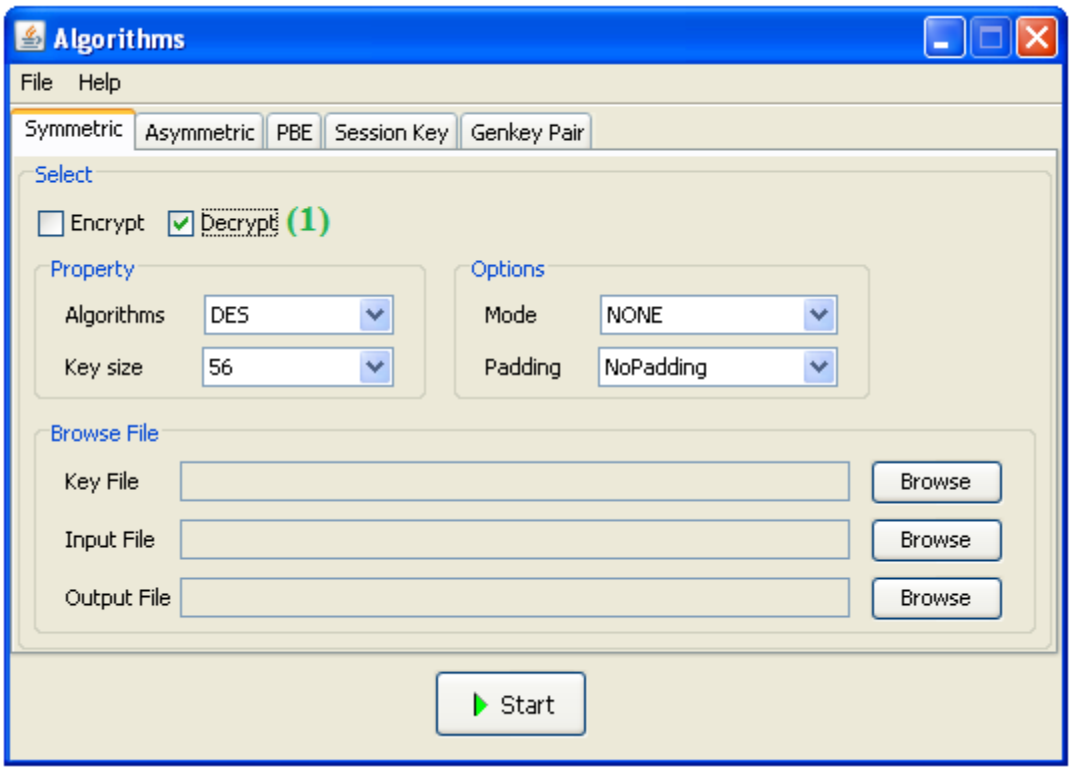


Hình 8: Giao diện thông báo thời gian mã hóa

- **Bước 7**: Kiểm tra kết quả. Sau khi mã hóa file được mã hóa không thể mở được và tạo ra file key trong thư mục chỉ định.

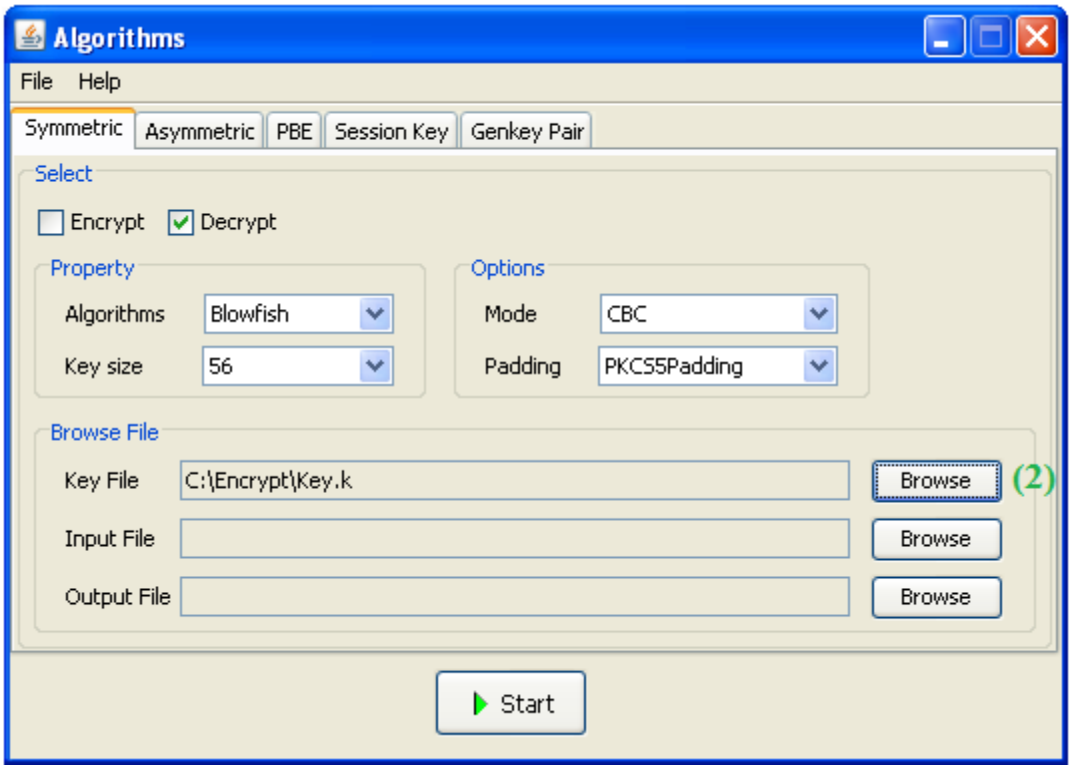
3.1.2. Giải mã:

- **Bước 1:** Để giải mã file đã được mã hóa ta click vào check box "**Decrypt**".



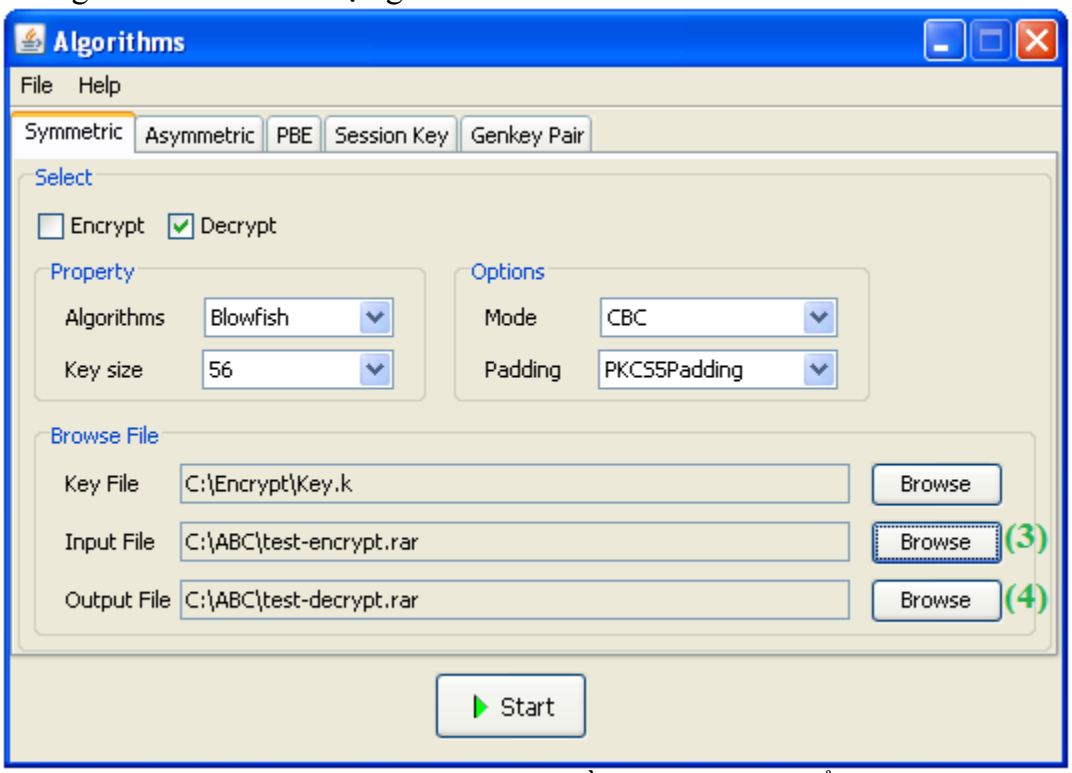
Hình 9: Giao diện click vào check box "Decrypt"

- **Bước 2:** Bạn không cần quan tâm thuật toán, key size, mode và padding là gì trong quá trình giải mã. Để tiện lợi cho người sử dụng, trong phần mềm này, bạn chỉ cần có file encrypt và file key là bạn có thể giải mã được. Khi bạn chọn file key, thuộc tính của file key này sẽ được load lên trên giao diện để bạn dễ nhận biết.



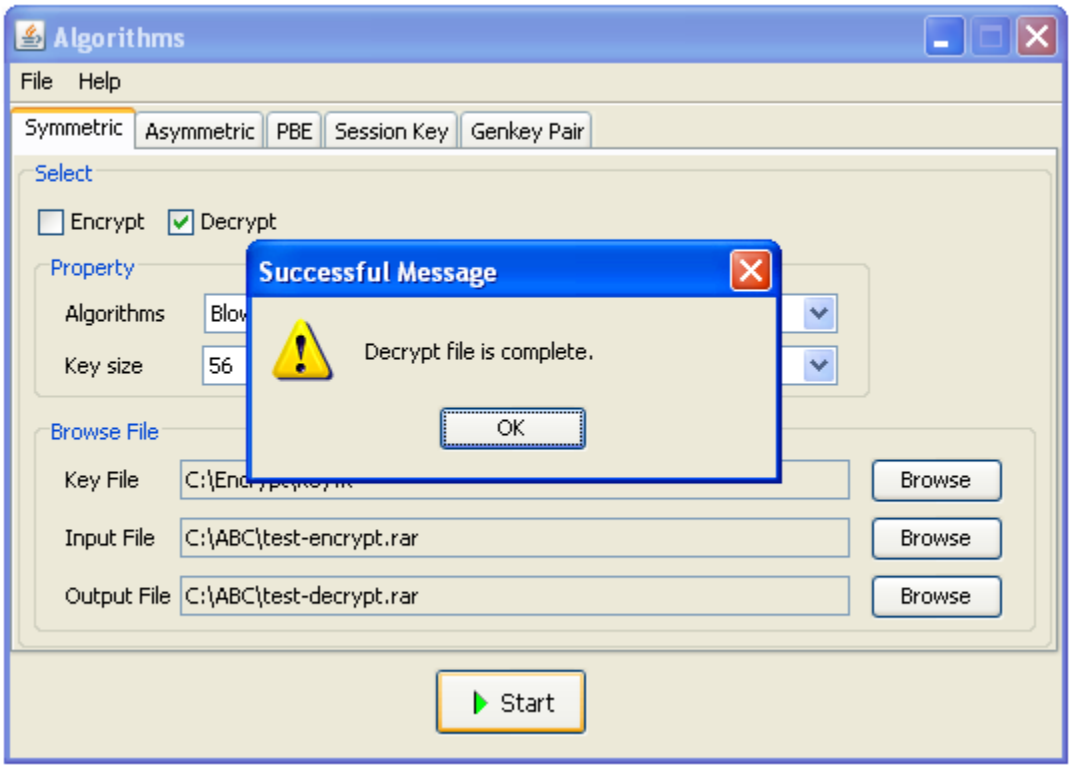
Hình 10: Giao diện sau khi chọn Key file

- **Bước 3:** Trong phần Input File: đường dẫn đến file cần được giải mã, Output File: đường dẫn đến file sẽ được giả mã ra.

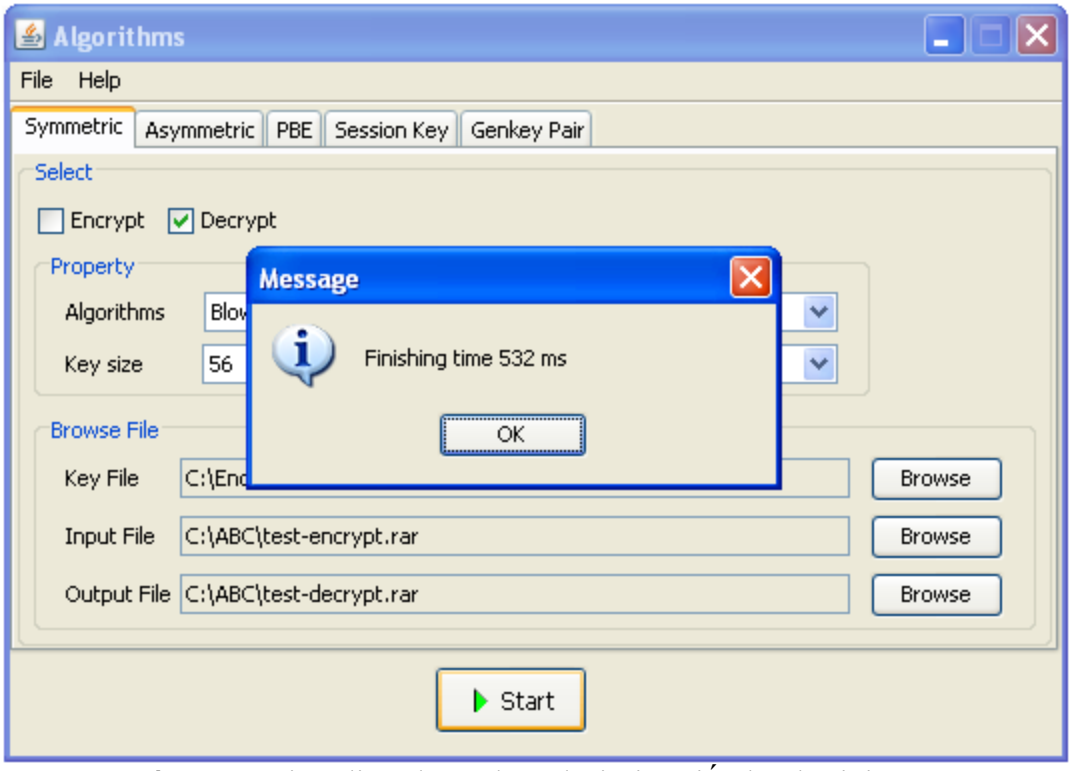


Hình 11: Giao diện sau khi nhập đầy đủ thông tin để giải mã

- **Bước 5:** Sau khi nhập đầy đủ thông tin, bạn click và nút "Start" bên dưới để tiến hành giải mã file.
- **Bước 6:** Sau khi giải mã xong, màn hình sẽ xuất hiện thông báo thành công và thời gian thực hiện giải mã file. Nếu có lỗi xảy ra, trên màn hình sẽ xuất ra thông báo lỗi.



Hình 12: Giao diện thông báo giải mã thành công

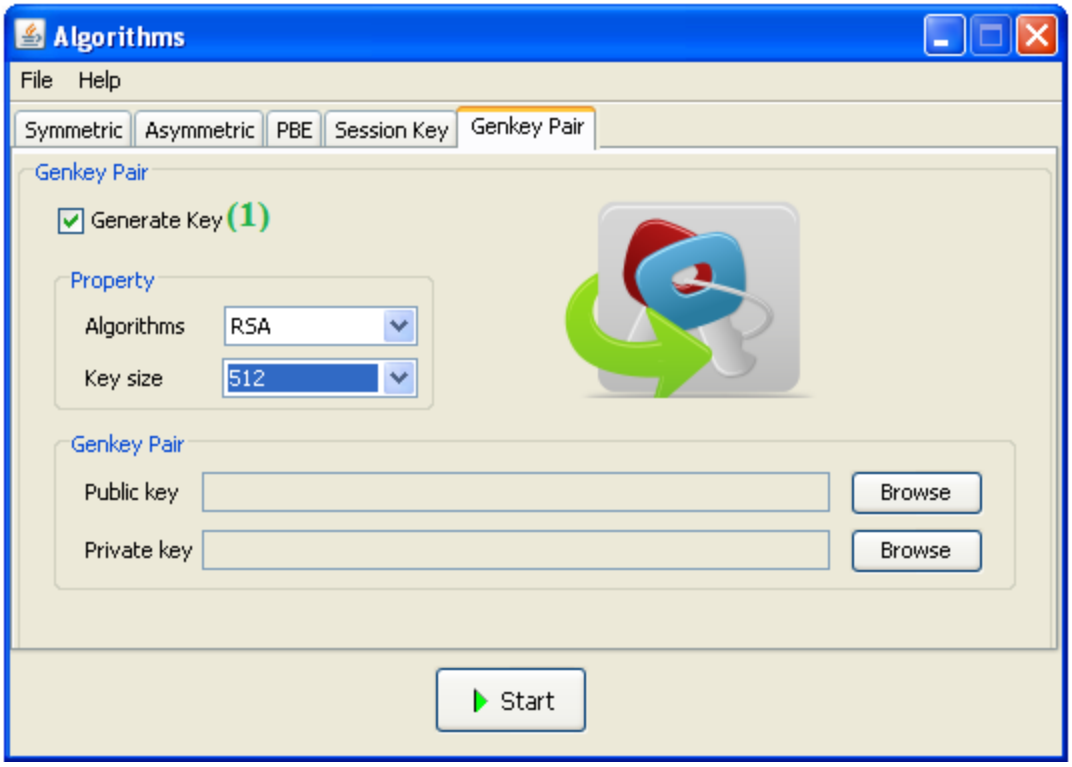


Hình 13: Giao diện thông báo thời gian tiến hành giải mã

- **Bước 7:** Kiểm tra kết quả, vào đường dẫn file đã được mã hóa (Output File) mở file lên, ta thấy được mở file thành công.

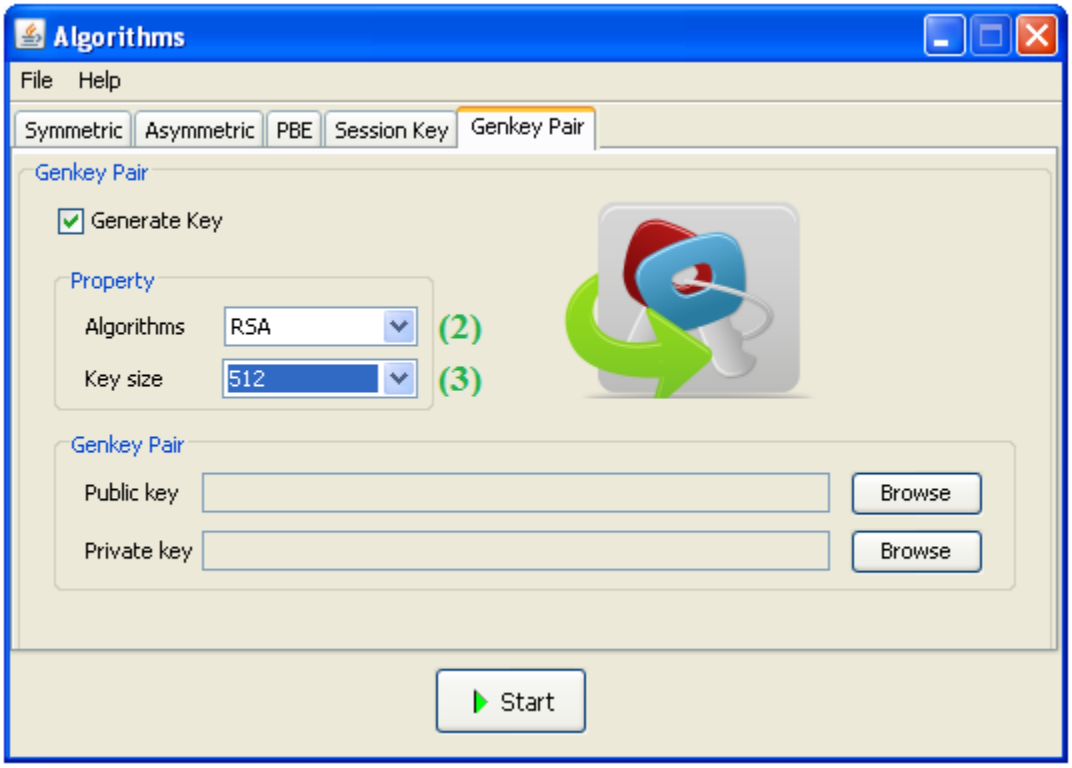
3.2. Tạo cặp khóa public và private cho mã hóa Asymmetric và Sessionkey

- **Bước 1:** Click vào check box "**Generate Key**" để tiến hành tạo cặp khóa.



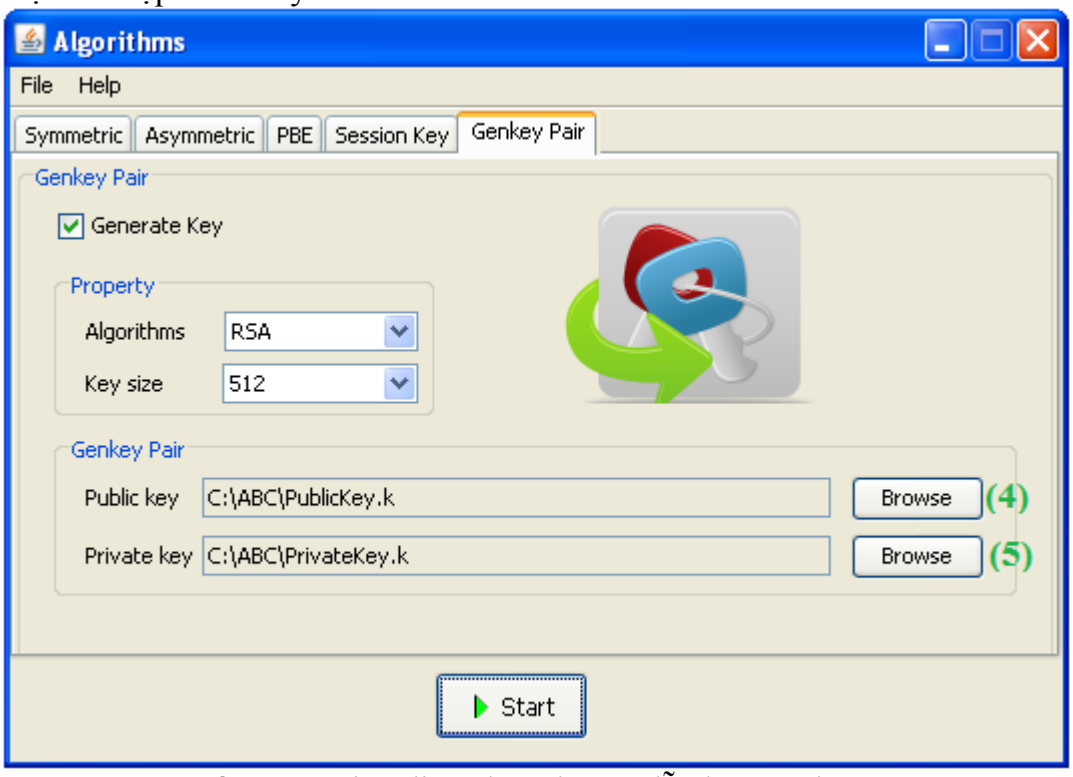
Hình 14: Giao diện click vào check box "Generate Key"

- **Bước 2:** Trong phần Property, chọn thuật toán và độ dài key mà bạn muốn tạo.



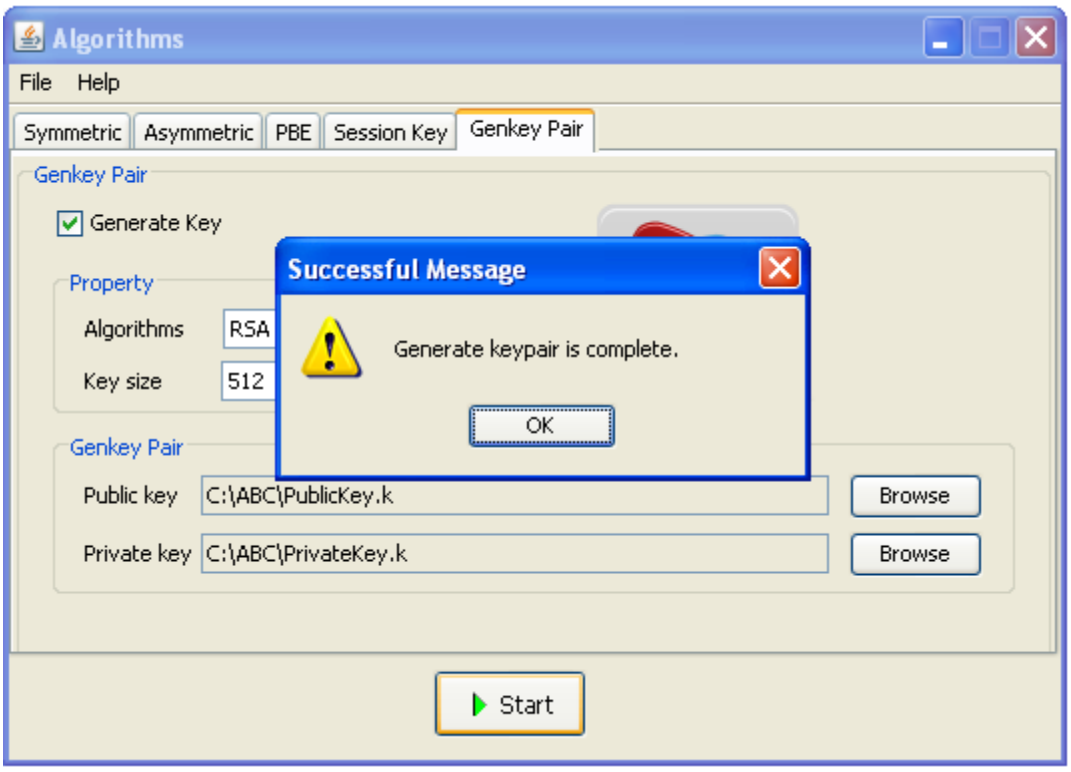
Hình 15: Giao diện chọn thuật toán và key size

- **Bước 3:** Trong phần Genkey Pair, click vào nút "Browse" tương ứng để chọn thư mục lưu cặp khóa này.



Hình 16: Giao diện chọn đường dẫn lưu cặp key

- **Bước 4:** Sau khi nhập đầy đủ thông tin, ta click nút "Start" để bắt đầu việc tạo cặp khóa. Khi tạo thành công sẽ xuất hiện thông báo:

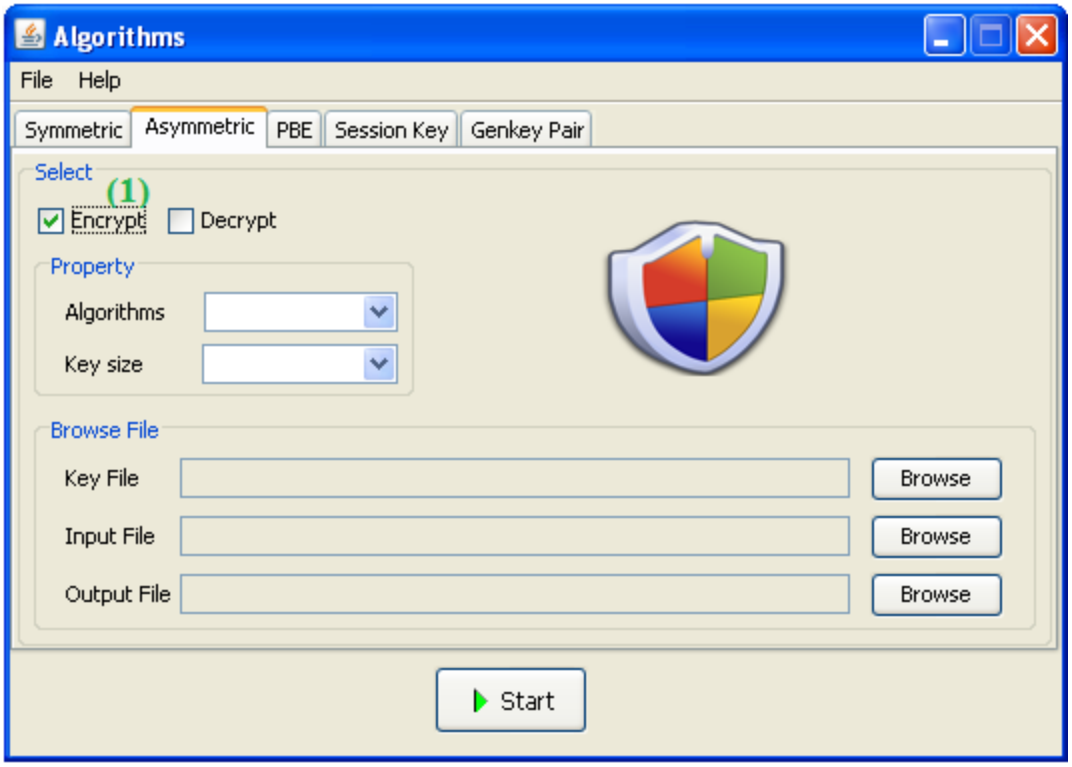


Hình 17: Giao diện thông báo tạo cặp khóa thành công

3.3. Thuật toán bất đối xứng (Asymmetric) và Session Key:

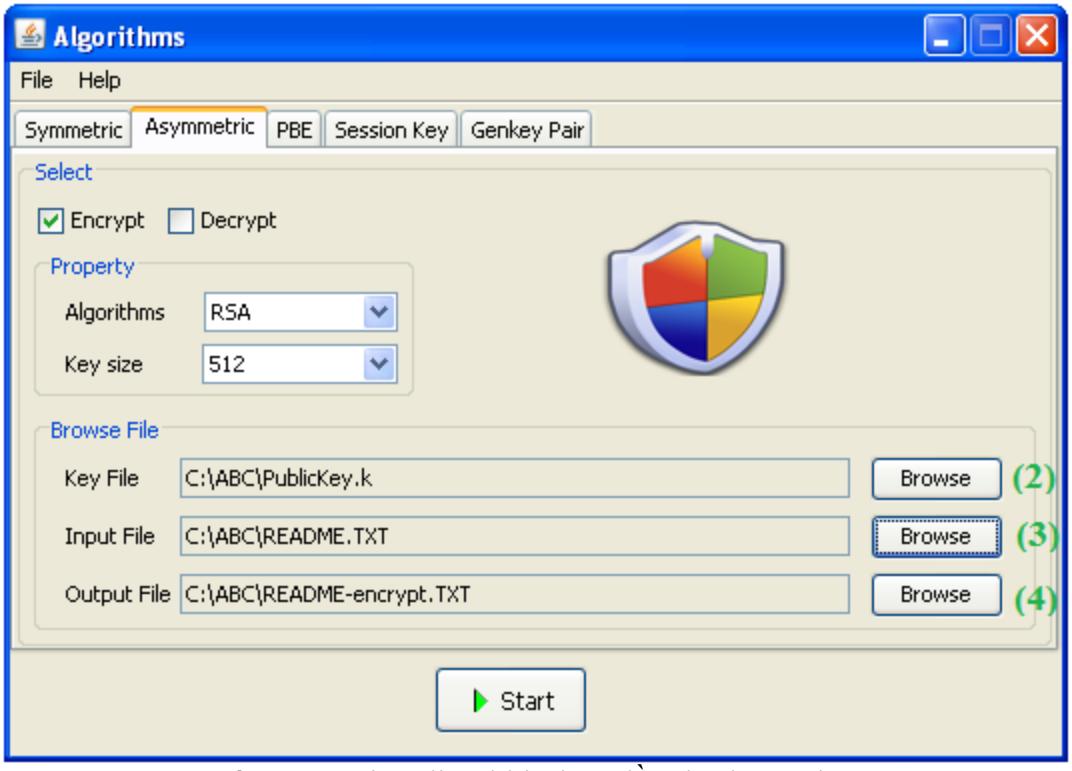
3.3.1. Mã hóa:

- **Bước 1**: Qua tab Genkey Pair để tạo cặp key (public key và private key) trước.
- **Bước 2**: Click chọn check box "**Encrypt**" để tiến hành mã hóa.



Hình 18: Giao diện click vào check box "Encrypt"

- **Bước 3:** Trong phần Browse File, Key File: đường dẫn đến file public key mà bạn dùng key này để mã hóa. Input File: đường dẫn đến file cần được mã hóa. Output File: đường dẫn file mã hóa được tạo ra (Click nút "Browse" tương ứng để chọn) . Khi bạo browse lên file public key, giao diện sẽ hiển thị thông tin của file public key đó(thuật toán, độ dài key).

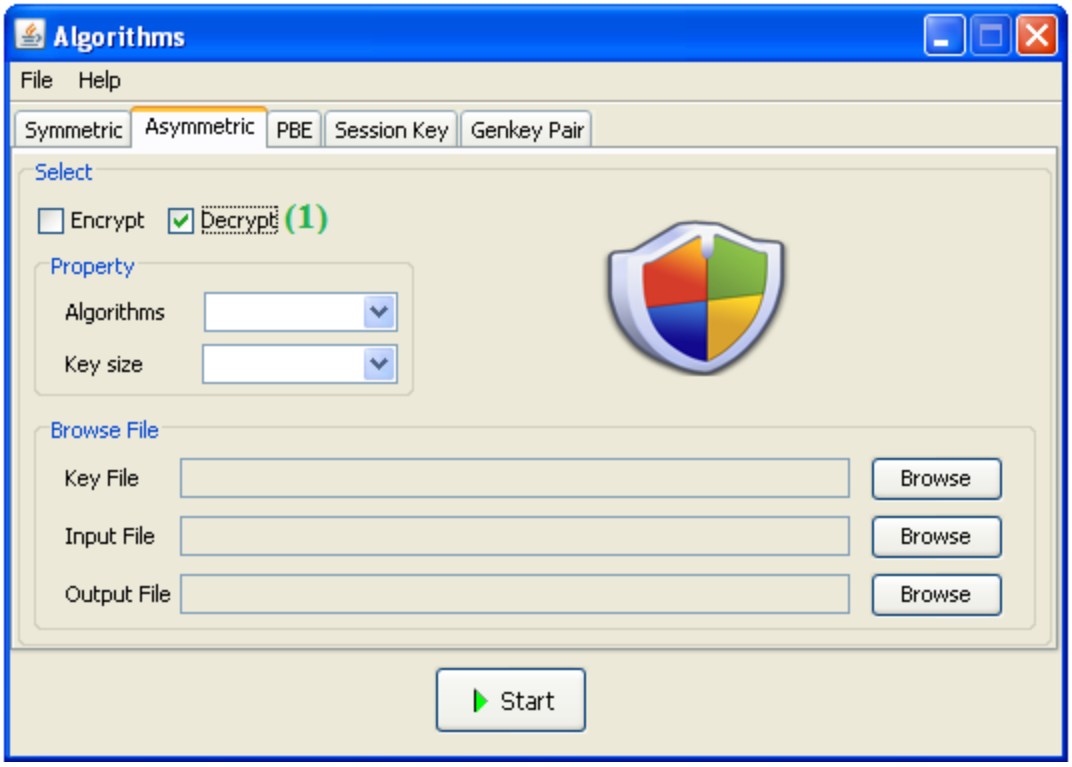


Hình 19: Giao diện khi nhập đầy đủ thông tin

- **Bước 4:** Sau khi nhập đầy đủ thông tin, click nút "Start" để tiến hành mã hóa. Khi phần mềm mã hóa thành công sẽ có thông báo cho bạn biết.

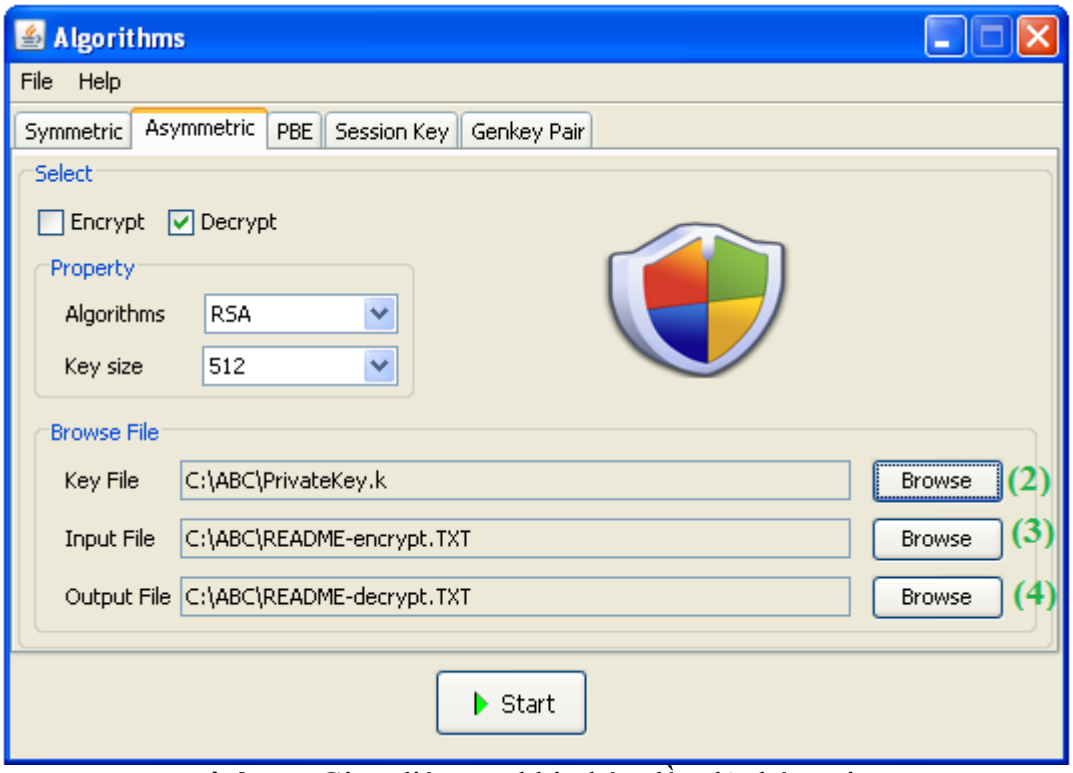
3.3.2. Giải mã:

- **Bước 1**: Click vào check box "**Decrypt**" để tiến hành giải mã.



Hình 20: Giao diện click vào check box "Decrypt"

- **Bước 2**: Trong phần Browse File, Key File: đường dẫn đến private key dùng để giải mã. Input File: đường dẫn đến file cần được giải mã(encrypt file). Output File: đường dẫn chỉ định file giải mã sau khi thực hiện sẽ lưu tại đó.
  Trong phần Property, bạn không cần quan tâm. Vì khi load file key lên, thuộc tính của file key đó sẽ được hiển thị trên giao diện(thuật toán, độ dài key).



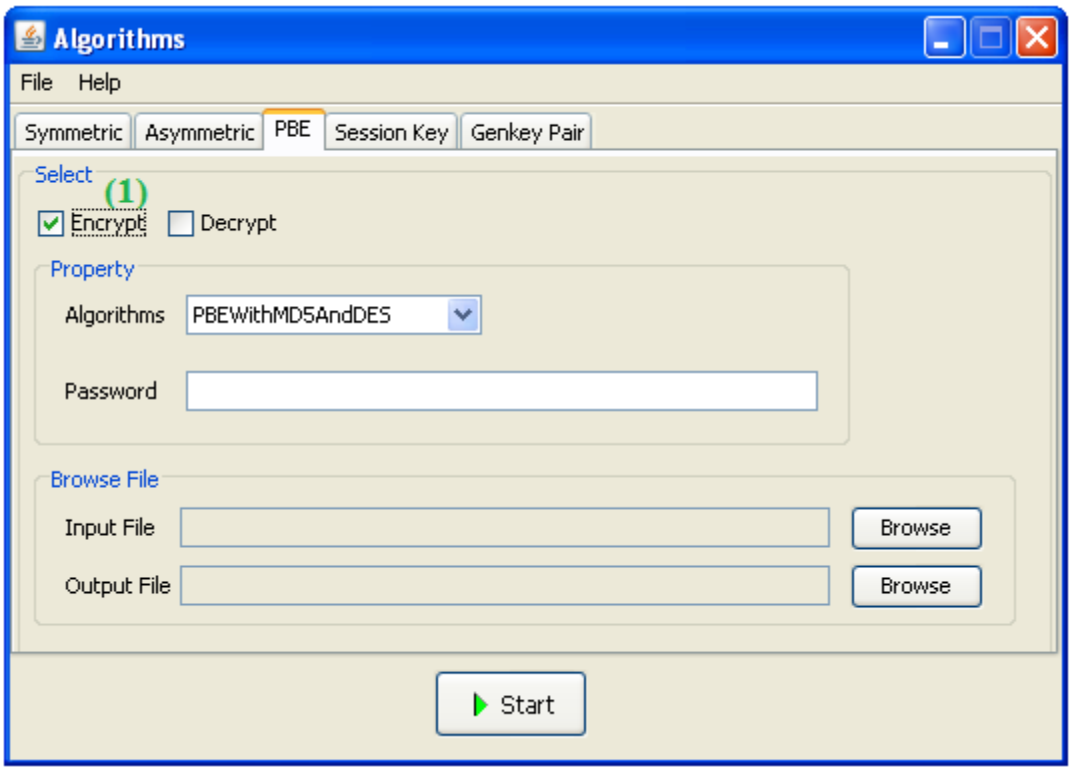
Hình 21: Giao diện sau khi nhập đầy đủ thông tin

- **Bước 3**: Sau khi nhập đầy đủ thông tin, ta tiến hành mã hóa bằng cách click vào nút Start.

3.4. Thuật toán Session:

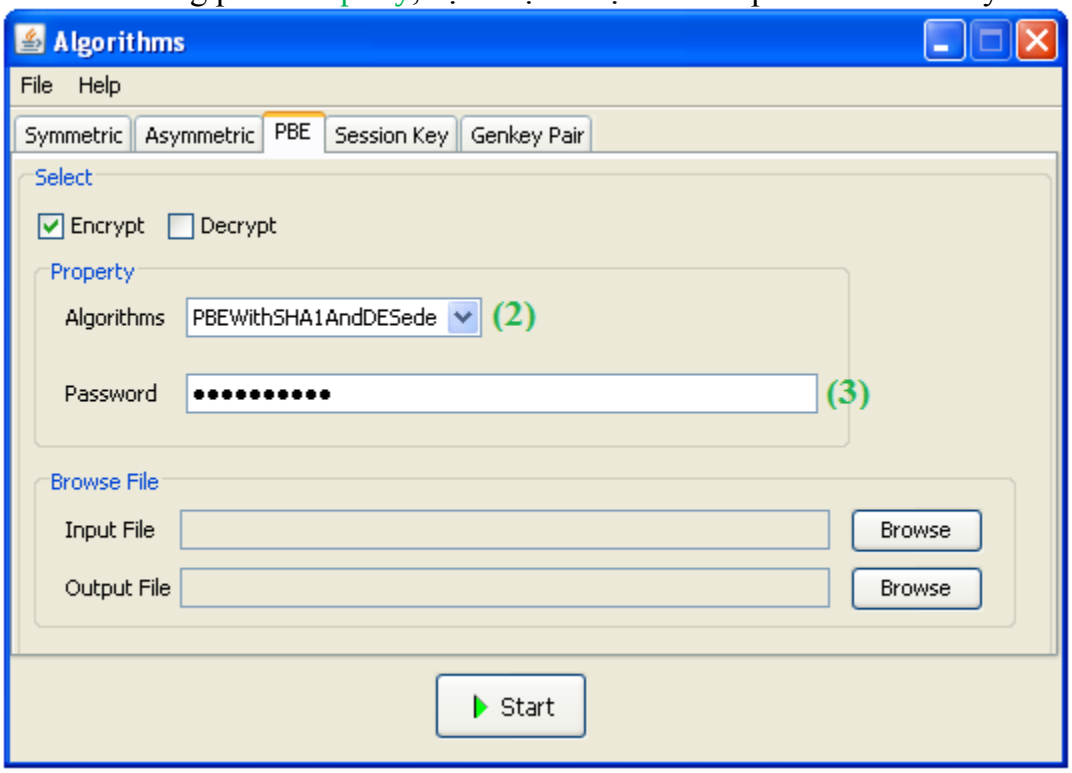
3.4.1. Mã hóa:

- **Bước 1**: Click vào check box "**Encrypt**" để tiến hành mã hóa dữ liệu.



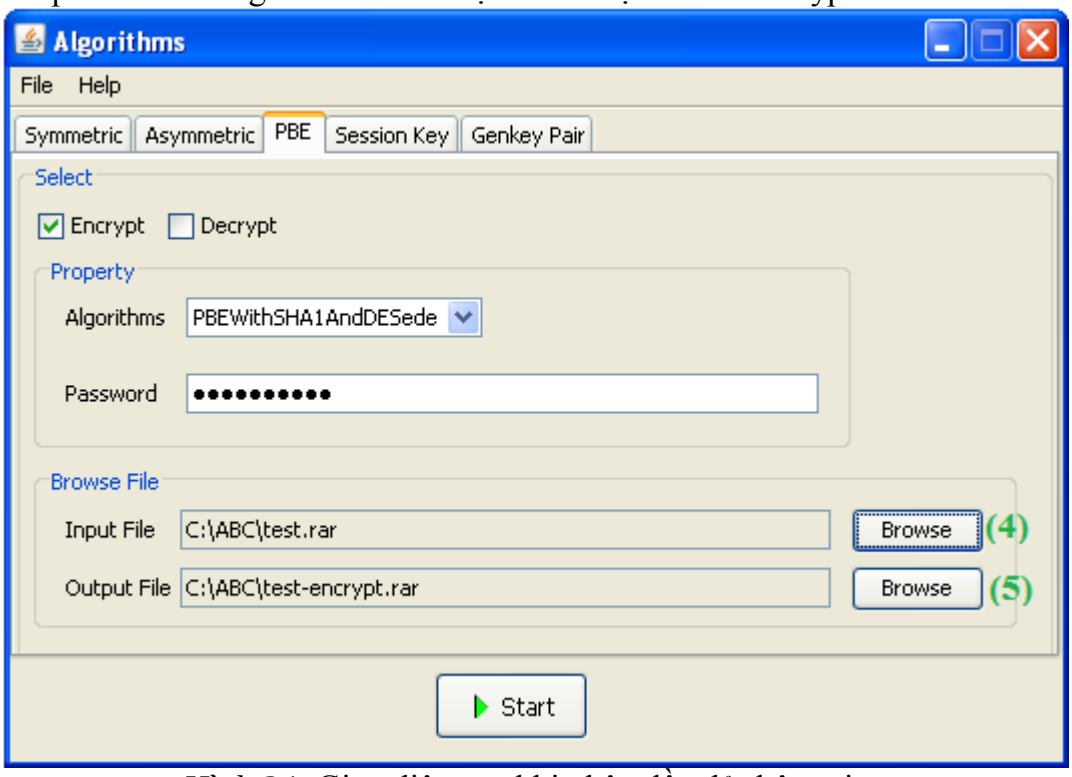
Hình 22: Giao diện click vào check box "Encrypt"

- **Bước 2**: Trong phần Property, bạn chọn thuật toán và password vào đây.



Hình 23: Giao diện chọn thuật toán và nhập password

- **Bước 3**: Trong phần Browse File, Input File: đường dẫn đến file cần mã hóa. Output File: đường dẫn đến thư mục mà nó tạo ra file encrypt sau khi mã hóa.

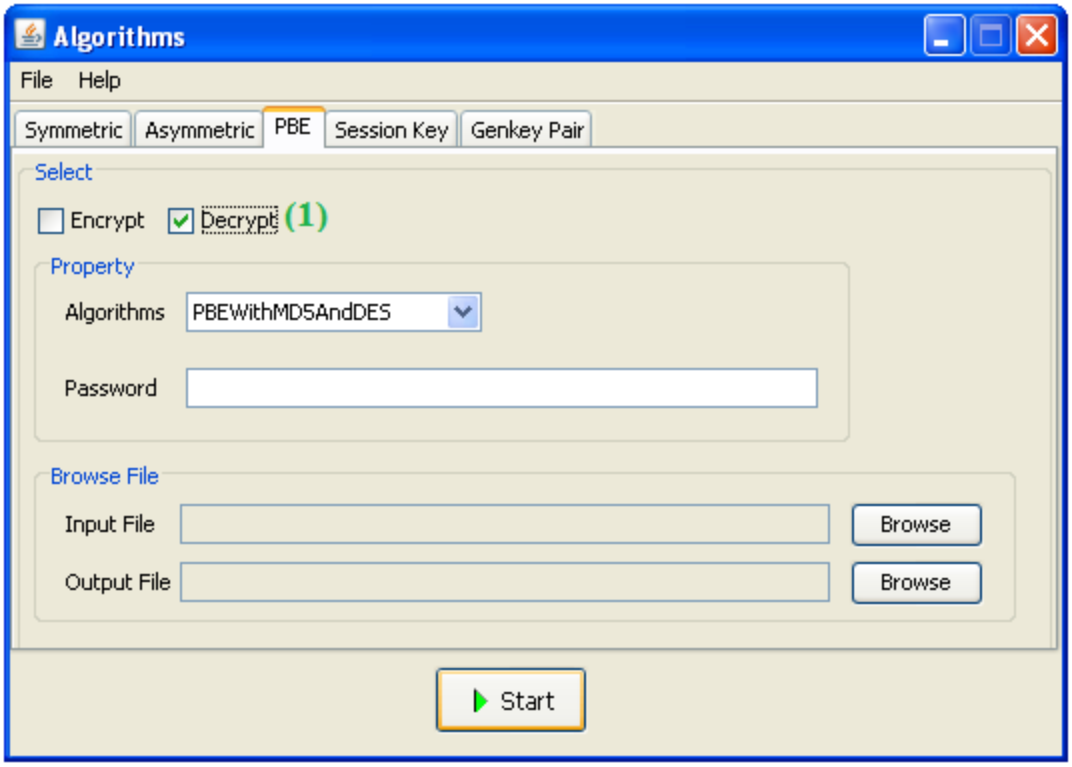


Hình 24: Giao diện sau khi nhập đầy đủ thông tin

- **Bước 4**: Sau khi nhập đầy đủ thông tin, click nút "Start" để tiến hành mã hóa.

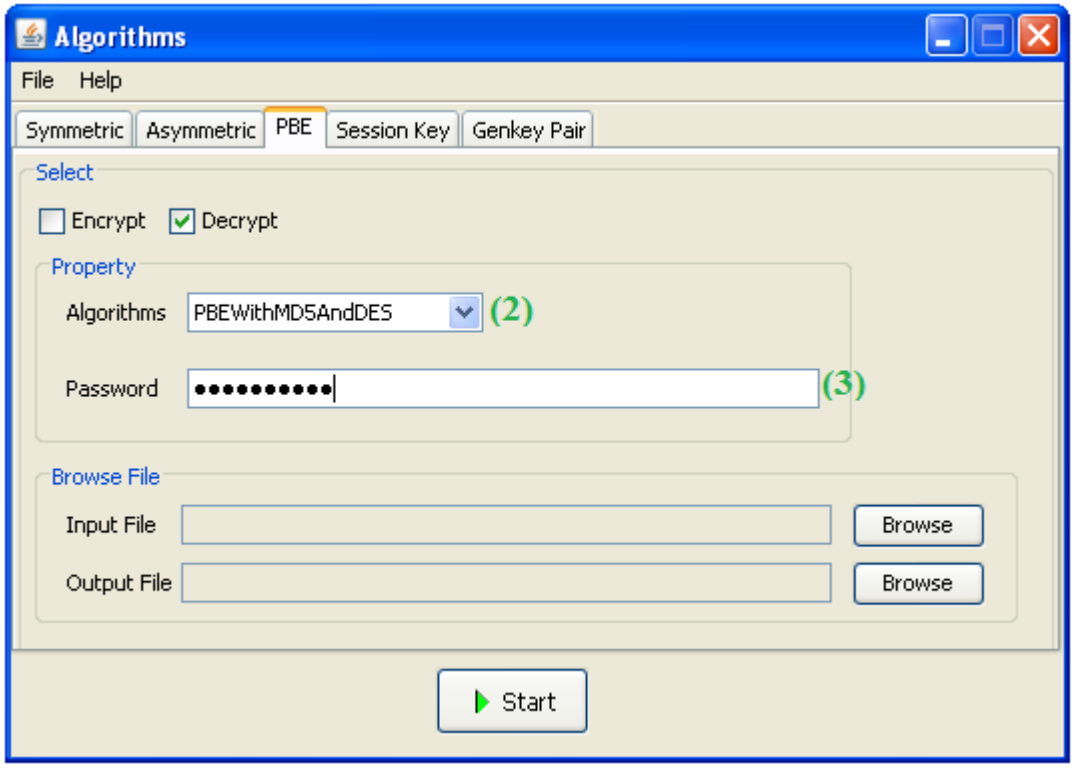
3.4.2. Giải mã:

- **Bước 1**: Click vào check box "**Decrypt**" để tiến hành giải mã.



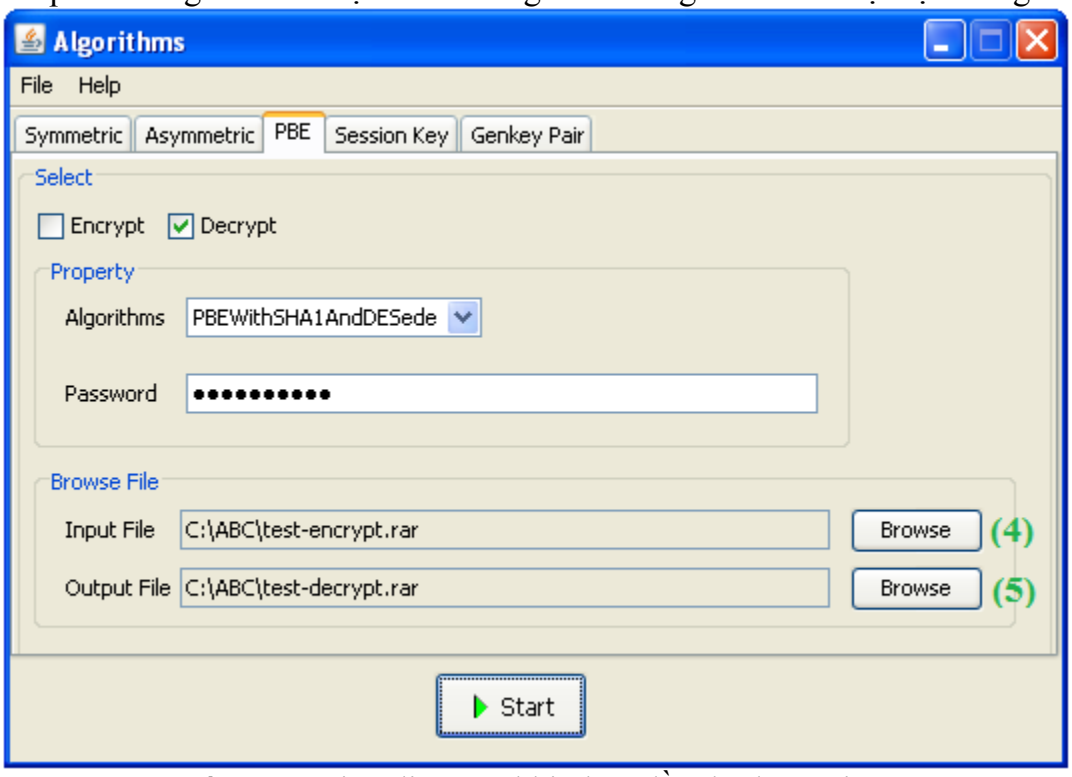
Hình 25: Giao diện click vào checkbox "Decrypt"

- **Bước 2**: Trong phần Property, chọn thuật toán và nhập password đúng như lúc mã hóa để tiến hành giải mã.



Hình 26: Giao diện chọn thuật toán và nhập password

- **Bước 3**:Trong phần Browse File, Input File: đường dẫn đến file cần được giải mã. Output: đường dẫn khi thực thi chương trình file giải mã sẽ được tạo trong đó.



Hình 27: Giao diện sau khi nhập đầy đủ thông tin

- **Bước 4**: Sau khi nhập xong thông tin, click nút "Start" để tiến hành giải mã. Nếu trong quá trình thực hiện, password hay thuật toán không trùng sẽ xuất hiện thông báo.