```
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
                    // File dich
                    String desFile = folder + "\\" + f.getName();
                    // Ma Hoa
                    EnCrypt.encrypt(thuattoan, file, desFile, key);
                    // Ghi file 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(
                   // 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

	2
2. Chú ý trước khi sử dụng phân mêm	
2.1. Trong phần mã hóa đối xứng (Symmetric)	3
2.2. Trong phần mã hóa bất đối xứng (Asymmetric) và Session Key	3
3. Các bước thực hiện mã hóa và giải mã bằng phần mềm:	3
3.1. Thuật toán đối xứng (Symmetric):	3
3.1.1. Mã hóa:	3
3.1.2. Giải mã:	9
3.2. Tạo cặp khóa public và private cho mã hóa Asymmetric và Sessionkey	13
3.3. Thuật toán bất đối xứng (Asymmetric) và Session Key:	16
3.3.1. Mã hóa:	16
3.3.2. Giải mã:	18
3.4. Thuật toán Session:	20
3.4.1. Mã hóa:	20
3.4.2. Giải mã:	22

## 1. Giao diện chính của phần mềm

🛓 Algorithms	
File Help	
Symmetric Asyr	mmetric PBE Session Key Genkey Pair
Select	
Encrypt	] Decrypt
Property	Options
Algorithms	DES Mode NONE
Key size	56 V Padding NoPadding V
Browse File	
Key File	Browse
· · · ·	
Input File	Browse
Output File	Browse
	► Start

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.

🕌 Algorithms					
File Help					
Symmetric Asym	nmetric PBE Session K	ey 🛛 Genkey Pair	]		
Select(1)					
Encrypt	Decrypt				
Property		Options			
Algorithms	DES 💌	Mode	NONE	*	
Key size	56 💌	Padding	NoPadding	*	
Browse File					
Key File				E	Browse
Input File					Browse
Output File					Browse
		Start			

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.

🕌 Algorithms						
File Help						
Symmetric Asyr	nmetric PBE	Session Key	Genkey Pai	r		
Select						
🕑 Encrypt 🗧	Decrypt					
Property			Options			
Algorithms	Blowfish	<b>v</b> (2)	Mode	NONE	*	
Key size	56	✓ (3)	Padding	NoPadding	*	
Browse File						
Kev File						Browse
Input File						Browse
Output File						Browse
			▶ Start	]		

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.

🕌 Algorithms				
File Help				
Symmetric Asyr	mmetric PBE Session K	ey 🛛 Genkey Pair	]	
Select				
🗹 Encrypt 📘	Decrypt			
Property		Options		
Algorithms	Blowfish 🛛 💌	Mode	СВС	✓ (4)
Key size	56 💌	Padding	PKCS5Padding	✓ (5)
Browse File				
Key File				Browse
Input File				Browse
Output File				Browse
		▶ Start		

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.

🕌 Algorithms				
File Help				
Symmetric Asym	metric PBE Session K	ey Genkey Pair		
Select				
🕑 Encrypt 📃	Decrypt			
Property		Options		
Algorithms	Blowfish 💌	Mode	СВС 💌	
Key size	56 💌	Padding	PKCS5Padding 🛛 👻	
Browse File				
Key File				Browse (6)
Input File				Browse (7)
Output File				Browse (8)
				]
		▶ Start		

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.

🕌 Algorithms	15	
File Help		
Symmetric Asy	ymmetric PBE Session Key Genkey Pair	
Select		
🗹 Encrypt [	Decrypt	
Property	Options	
Algorithms	Blowfish V Mode CBC V	
Key size	56  Padding PKCS5Padding	
-Browse File -		
Key File	C:\Encrypt\Key k	Browse
Keyriic	C. Tenery percey. K	browse
Input File	C:\ABC\test.rar	Browse
Output File	C:\ABC\test-encrypt.rar	Browse
	▶ Start	

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.

🛓 Algorithms		
File Help		
Symmetric Asymmetric PBE	Session Key Genkey Pair	
Select		
Encrypt 🔄 Decrypt		
Property	cessful Message 🛛 🔀	
Algorithms Blow	Encypt file is complete	
Key size 56 🥌		
Browse File	OK	
Key File C:\Encrypt\Ke	ey.k	Browse
Input File C:\ABC\test.r.	ar	Browse
	encrypt rar	Browse
	and About on	Diomse
	▶ Start	

Hình 7: Giao diện thông báo mã hóa thành công

🛓 Algorithms		
File Help		
Symmetric Asyn	nmetric PBE Session Key Genkey Pair	
Select		
🗹 Encrypt 📃	Decrypt	
Property	Message	
Algorithms	Bl	
Key size	56 Finishing time 16 ms	
Browse File	OK	
Key File	C:\Encrypc;key;k	Browse
Input File	C:\ABC\test.rar	Browse
Output File	C:\ABC\test-encrypt.rar	Browse
	Start	

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".

🕌 Algorithms					
File Help					
Symmetric Asyn	nmetric PBE Session K	(ey 🛛 Genkey Pair			
Select					
🔄 Encrypt 🕑	Decrypt (1)				
Property		Options			
Algorithms	DES 💌	Mode	NONE	*	
Key size	56 💌	Padding	NoPadding	*	
Browse File					
Key File					Browse
Toput File					Province
					browse
Output File					Browse
► Start					

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.

🕌 Algorithms	;				
File Help					
Symmetric Asy	mmetric PBE Session Key	Genkey Pair			
Select					
Encrypt	Z Decrypt				
Property		Options			
Algorithms	Blowfish 💌	Mode	СВС	~	
Key size	56 💌	Padding	PKCS5Padding	*	
Browse File					
Key File	C:\Encrypt\Key.k				Browse (2)
Input File					Browse
Output File					Browse
	[	▶ Start			

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. -

🛓 Algorithm	S	
File Help		
Symmetric Asy	vmmetric PBE Session Key Genkey Pair	
Select		
Encrypt	Decrypt	
Property	Options	n
Algorithms	Blowfish V Mode CBC V	
Key size	56 V Padding PKCS5Padding V	
Browse File		
Key File	C:\Encrypt\Key.k	Browse
Toput File		Browse (3)
Inpactilo		
Output File	C:\ABC\test-decrypt.rar	Browse (4)
	▶ Start	

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.

🛓 Algorithm	s		
File Help			
Symmetric Asy	mmetria	PBE Session Key Genkey Pair	
Select			
Encrypt	🗸 Decry	/pt	
Property		Successful Message	
Algorithms	Blov		
Key size	56	Decrypt file is complete.	
Browse File		ок	
Key File	C:\Enc		Browse
1.07 1 110		() perfection	
Input File	C:\ABC	Clest-encrypt.rar	Browse
Output File	C:\ABC	C\test-decrypt.rar	Browse
			]
		▶ Start	

Hình 12: Giao diện thông báo giải mã thành công

🖆 Algorithms	
File Help	
Symmetric Asymmetric PBE Session Key Genkey Pair	
Select	
Encrypt 🔽 Decrypt	
Property Message	
Algorithms Blov	
Key size 56 🐺 Finishing time 532 ms	]
Browse File	
Key File C:\End	Browse
Toput File C//APC/test engrupt you	Browner
Input Hie C: (ABC (test-entrypt.ran	browse
Output File C:\ABC\test-decrypt.rar	Browse
▶ Start	

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.

🖆 Algorithms	
File Help	
Symmetric Asymmetric PBE Session Key Genkey Pair	
Genkey Pair	
Generate Key (1)	
Property /	
Algorithms RSA 💌	
Key size 512	
Genkey Pair	
Public key	Browse
Private key	Browse
▶ Start	

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.

-

🖆 Algorithms	×
File Help	
Symmetric Asymmetric PBE Session Key Genkey Pair	
Genkey Pair	
Generate Key	
Property	
Algorithms RSA 🔽 (2)	
Key size 512 (3)	
Genkey Pair	
Public key Browse	
Private key Browse	
► Start	

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.

🛃 Algorithms 📃 🗖 🗙
File Help
Symmetric Asymmetric PBE Session Key Genkey Pair
Genkey Pair
🗹 Generate Key
Property
Algorithms RSA
Key size 512
Genkey Pair
Public key C:\ABC\PublicKey.k Browse (4)
Private key C:\ABC\PrivateKey.k Browse (5)
▶ Start

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 xuật hiện thông báo:

🖆 Algorithms	
File Help	
Symmetric Asymmetric PBE Session Key Genkey Pair	
Genkey Pair	
🗹 Generate Key	
Property Successful Message	
Algorithms RSA Generate keypair is complete	
Key size 512	
Genkey Pair	
Public key C:\ABC\PublicKey.k	Browse
Private key C:\ABC\PrivateKey.k	Browse
▶ Start	

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. -
- -

🛎 Algorithms	
File Help	
Symmetric Asymmetric PBE Session Key Genkey Pair	
Select (1) Encrypt Decrypt	
Property	
Algorithms	
Key size	
Browse File	
Key File	Browse
Input File	Browse
Output File	Browse
▶ Start	

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).

🖆 Algorithms	
File Help	
Symmetric Asymmetric PBE Session Key Genkey Pair	
Select	
Encrypt Decrypt	
Property	
Algorithms RSA 💌	
Key size 512 💌	
Browse File	
Key File C:\ABC\PublicKey.k	Browse (2)
Input File C:\ABC\README.TXT	Browse (3)
Output File C:\ABC\README-encrypt.TXT	Browse (4)
	]
► Start	

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.

🛎 Algorithms	
File Help	
Symmetric Asymmetric PBE Session Key Genkey Pair	
Select	
Encrypt Decrypt (1)	
Property	
Algorithms 💽	
Key size	
Browse File	
Key File	Browse
Input File	Browse
Output File	Browse
► Start	

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).

🔊 Algorithms	
File Help	
Symmetric Asymmetric PBE Session Key Genkey Pair	
Select	
Encrypt 🔽 Decrypt	
Property	
Algorithms RSA 💌	
Key size 512 💌	
Key File C:\ABC\PrivateKey.k	Browse (2)
Input File C:\ABC\README-encrypt.TXT	Browse (3)
Output File C:\ABC\README-decrypt.TXT	Browse (4)
▶ Start	

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.

🛎 Algorithms	
File Help	
Symmetric Asymmetric PBE Session Key Genkey Pair	
Select (1) Encrypt Decrypt	
Property	
Algorithms PBEWithMD5AndDE5	
Password	
Browse File	
Input File	Browse
Output File	Browse
▶ Start	

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

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

📓 Algorithms 📃 🗖 🗙
File Help
Symmetric Asymmetric PBE Session Key Genkey Pair
Select
Encrypt Decrypt
Property
Algorithms PBEWithSHA1AndDESede 🔽 (2)
Browse File
Input File Browse
Output File Browse
► Start

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.

📓 Algorithms 📃 🗖 🔀
File Help
Symmetric Asymmetric PBE Session Key Genkey Pair
Select
Encrypt Decrypt
Property
Algorithms PBEWithSHA1AndDESede 💌
Password •••••••
Input File C:\ABC\test.rar Browse (4)
Output File C:\ABC\test-encrypt.rar Browse (5)
► Start

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.

🛓 Algorithms	
File Help	
Symmetric Asyr	nmetric PBE Session Key Genkey Pair
Select	
🔄 Encrypt 💽	Decrypt (1)
Property	
Algorithms	PBEWithMD5AndDES
Password	
Browse File	
Input File	Browse
Output File	Browse
ļ,	
-	▶ Start

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.

🕌 Algorithms		
File Help		
Symmetric Asymmetric PBE Session Key Genkey Pair		
Select		
Encrypt 🔽 Decrypt		
Property		
Algorithms PBEWithMD5AndDES V (2)		
Password (3)		
Input File Brow	se	
Output File Brow	se	
▶ Start		

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.

🛃 Algorithms 📃 🗖 🔀
File Help
Symmetric Asymmetric PBE Session Key Genkey Pair
Select
Encrypt 🔽 Decrypt
Property
Algorithms PBEWithSHA1AndDESede 💌
Password •••••••
C Regime File
Input File C:\ABC\test-encrypt.rar Browse (4)
Output File C:\ABC\test-decrypt.rar Browse (5)
▶ Start

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.