DES???Data Encryption Standard, ???????????. ?????????????. ???????????, ????:

```
[ComVisibleAttribute(true)]
public sealed class DESCryptoServiceProvider : DES
```

???????????(sealed)?????, ????????. ??????DES??. ???DES?????:

```
[ComVisibleAttribute(true)]
public abstract class DES : SymmetricAlgorithm
```

??DES?????, ??????. ????, ????????????.

```
[ComVisibleAttribute(true)]
public abstract class SymmetricAlgorithm : IDisposable
```

?????SymmetricAlgorithm??DESCryptoProvider?????????, ??????????IDisposable??, ?????????????????????? ?????????(Dispose). ????DES??????64????.

??DESCryptoServiceProvider?????????????:

```
System.Object
  System.Security.Cryptography.SymmetricAlgorithm
    System.Security.Cryptography.DES
      System.Security.Cryptography.DESCryptoServiceProvider
```

????????mscorlib (? mscorlib.dll ?), ???????, ????????, ??????mscorlib.dll???.

????MSDN????????????DES????:

```
private static void EncryptData(String inName, String outName, byte[] desKey, byte[] desIV)
 {
    //Create the file streams to handle the input and output files.
    FileStream fin = new FileStream(inName, FileMode.Open, FileAccess.Read);
    FileStream fout = new FileStream(outName, FileMode.OpenOrCreate, FileAccess.Write);
    fout.SetLength(0);

    //Create variables to help with read and write.
    byte[] bin = new byte[100]; //This is intermediate storage for the encryption.
    long rdlen = 0;              //This is the total number of bytes written.
    long totlen = fin.Length;    //This is the total length of the input file.
    int len;                     //This is the number of bytes to be written at a time.

    DES des = new DESCryptoServiceProvider();
    CryptoStream encStream = new CryptoStream(fout, des.CreateEncryptor(desKey, desIV),
CryptoStreamMode.Write);

    Console.WriteLine("Encrypting...");

    //Read from the input file, then encrypt and write to the output file.
    while(rdlen < totlen)
    {
       len = fin.Read(bin, 0, 100);
       encStream.Write(bin, 0, len);
       rdlen = rdlen + len;
       Console.WriteLine("{0} bytes processed", rdlen);
    }

    encStream.Close();
    fout.Close();
    fin.Close();
 }
```

?????DES?????????(EncryptData), ???????????, ??????????, ?????????????:

1. inName: ?????????????????
2. outName: ????????????????
3. desKey: ???DES????????
4. desIV: ??CBC??????, DES?????, ???ECB

??????????????, ??????????DES??????. ??OOD?????, ?????????????, ???JAVA??.NET, I/O???????:

```
    DES des = new DESCryptoServiceProvider();
    CryptoStream encStream = new CryptoStream(fout, des.CreateEncryptor(desKey, desIV), 
CryptoStreamMode.Write);
```

????des????, ?????????????, ????????????. DESCryptoServiceProvider????????????DES???????. ? CryptoStream??, ?????????, new CryptoStream(...), ????????????, ?????????, ?????fout?FileStream??, CryptoStream???????????????????????, ???????????????.

```
[ComVisibleAttribute(true)]
public class FileStream : Stream

[ComVisibleAttribute(true)]
public class CryptoStream : Stream, IDisposable
```

???????????????????????Stream???, ??????????. ?Stream?????, FileStream??CryptoStream??????, ????, FileStream??CryptoStream???Stream???:

```
Stream sUsingFs=new FileStream(...);
Stream sUsingCs=new CryptoStream(...);
```

??FileStream??CryptoStream????Stream, ??????????, ???Stream?????, ?????????OOA???????????????:

1. OCP(Open-Close Principle)
2. DIP(Dependency Inversion Principle)
3. LSP(Lisksov Principle)

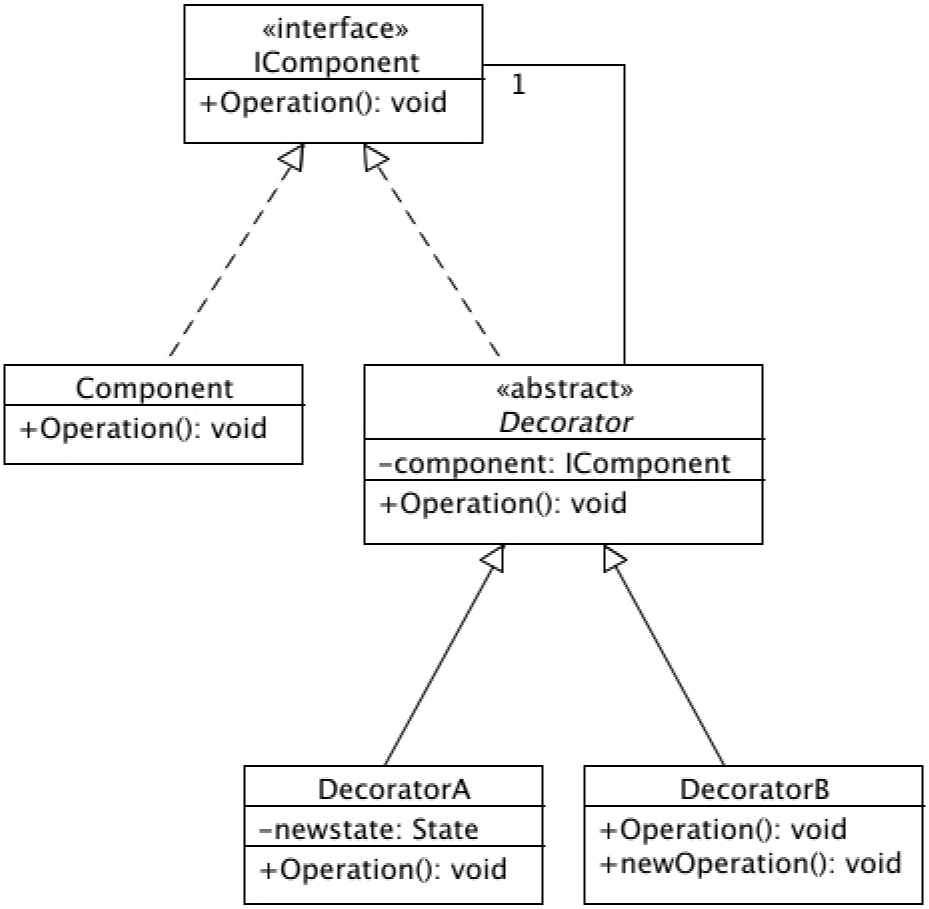
????????????????, ??????????????????. ???Stream??????, ??????????, CryptoStream???????????, ??fout? FileStream?????, ????????????????:

```
public CryptoStream (
   Stream stream,
   ICryptoTransform transform,
   CryptoStreamMode mode
)
```

?????, ?????????Stream??, ?????????, CryptoStream??????Stream?????, ???????FileStream?????, ???? CryptoStream?????????Stream????????, ????????????, ?????????. ?????, ????????????????CryptoStream? Stream???; ?FileStream??, ????Stream???IS-A???, ??Stream?CryptoStream??Stream?Filetream, ??????.NET Reflector??, ???????. Stream?Stream?????????????????, ???OOD?????, ???????Decorator Pattern??, ???????? ?, ????????:

**??????????????????, ?????????. ???????, ????(Decorator)??????????????.**

???UML???????- **?????????????????**:



??, ??????????. ???????T_A1??, ???????T_B1??, ?????????T_A1???????????, ????T_B1?????, ?????????, ??T_B1 ??????, ????????, ???????20??? ???????????????, ???????????????????, ????????20?????????????, ???????, ???? ?????????????. ??????, ????????(Refactor)???????????. ??Decorator????????.

T_A1?T_B1?????????, ????????????-Encode, ???????. ???????????:

```
interface T_DEV
```

?T_A1?T_B1?????????, ??T_A1?T_B1???????, ?????????????????:

```
public abstract class T_DEV_A: T_DEV
public abstract class T_DEV_B: T_DEV
```

??????????????, ????????????, ??T_A1?T_B1?????????????:

```
public sealed class T_A1: T_DEV_A
public sealed class T_B1: T_DEV_B
```

??sealed??????????????, ?????????????????. ???T_A1??T_B1??, ????T_DEV???, ???T_DEV??, ???????- Encode:

```
T_DEV Encode(...)
```

??????????????T_DEV, ????????, ???????UML??????:

1. T_DEV??IComponent
2. T_DEV_A?T_DEV_B??????Decorator
3. T_A1?T_B1?????T_DEV_A?T_DEV_B?instance class

IComponent???Encod(...)???????????????, ?????, ??????????:

```
byte[] GetBytes()
```

?????????????byte??, ?????????????????????????. ?????????:

```
interface T_DEV{
   T_DEV Encode(...);
   byte[] GetBytes();
}

public abstract class T_DEV_A: T_DEV {
   protected T_DEV _tDev;
   public T_DEV_A(T_DEV tDev){
      _tDev=tDev;
   }
}

public abstract class T_DEV_B: T_DEV {
   protected T_DEV _tDev;
   public T_DEV_B(T_DEV tDev){
      _tDev=tDev;
   }
}

public sealed class T_SRC<T>: T_DEV{
      //skip
     T _obj
      public T_SRC(T obj){
         _obj=obj;
      }
      public override T_DEV Encode(...){
         //skip
         return this;
      }

      public override GetBytes(){
         byte[] bContent;
         //skip
         return bContent;
      }
}

public sealed class T_A1: T_DEV_A{
      public T_A1(T_DEV tDev): base(tDev){
         //skip
      }

      public override T_DEV Encode(...){
         byte[] bContent=_tDev.GetBytes();
```

```
            //skip
            return this;
        }

        public override GetBytes(){
            byte[] bContent;
            //skip
            return bContent;
        }
}


public sealed class T_B1: T_DEV_B{
        public T_B1(T_DEV tDev): base(tDev){
            //skip
        }

        public override T_DEV Encode(...){
            byte[] bContent=_tDev.GetBytes();
            //skip
            return this;
        }

        public override GetBytes(){
            byte[] bContent;
            //skip
            return bContent;
        }
}
```

????????????, ????????????, ??T_B1??, ??????????????T_DEV???, ?????????????????, ????????????????, ??????. Encode(...)??????_tDev????, ??GetBytes()??????byte????. ????????T_DEV_SRC?????, ????????, ?????????, ??? T???????obj????, ???????????????????????????T_DEV??????????. ??, ?????????client, ??????:

```
string value="some content";
T_SRC<string> tSrc=new T_SRC<string>(value);
T_A1 tA1=new T_A1(tSrc);
T_B1 tB1=new T_B1(tA1);
byte[] bB1Content=tB1.GetBytes();
```

??????, ??????, ?????????????, ???????????, ??????????????????. Decorator Pattern?????????????????, ??????, ?????????, ??OCP???.

??, fin?FileStream????????????, ?????????????. fout????????????????????.

1. fin: ??????, ???=> ????, ???????????????????

2. fout: ????????=> ????, ??????????????????????

fout.SetLength(0)???????????0, ??????????????. ????????:

1. bin: ???100?bin??????????????????, ????100??
2. rdlen: ???????????, ?????
3. totlen: ??fin?????????????
4. len: ?????????