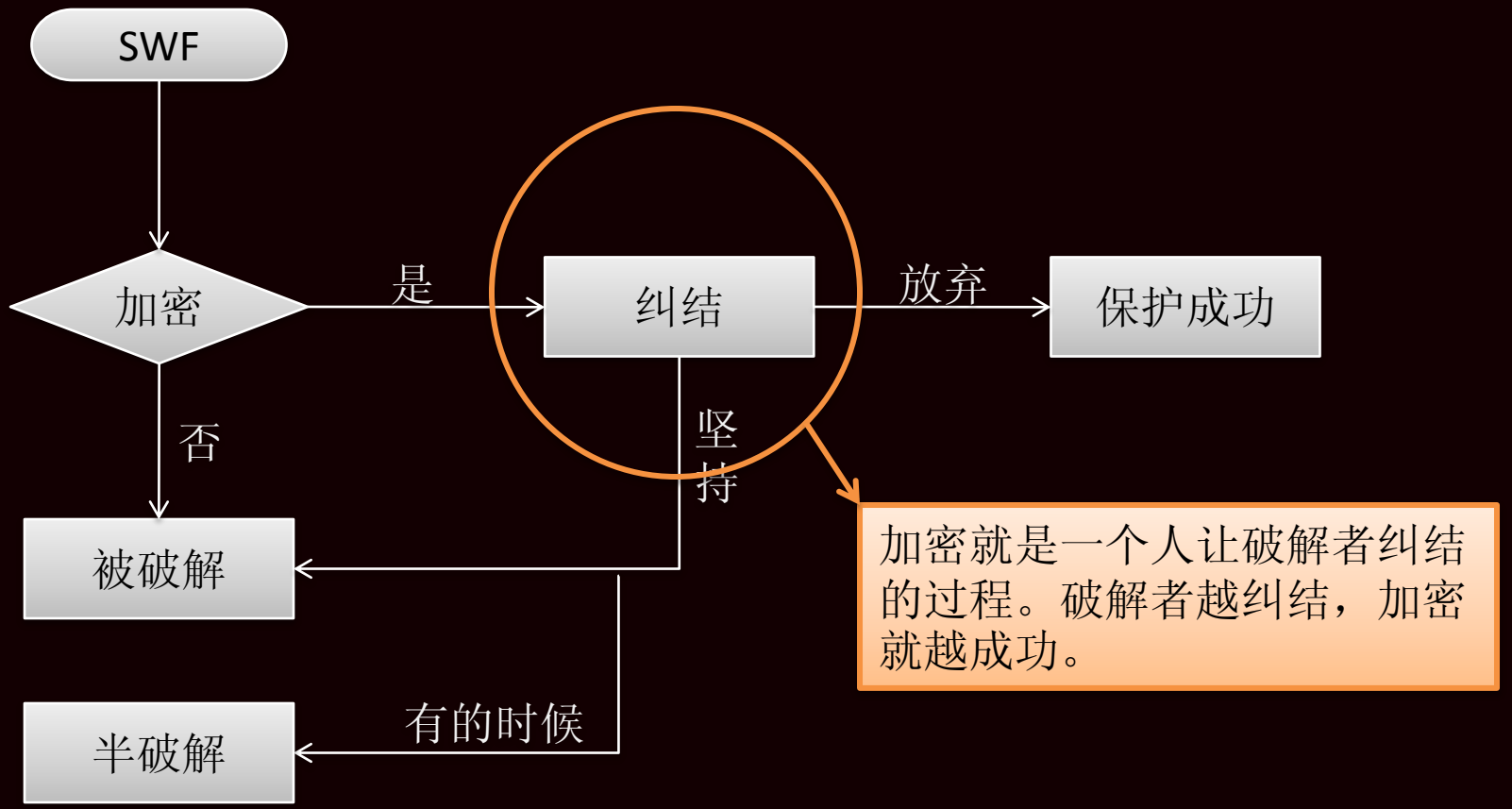
Flash加密和混淆

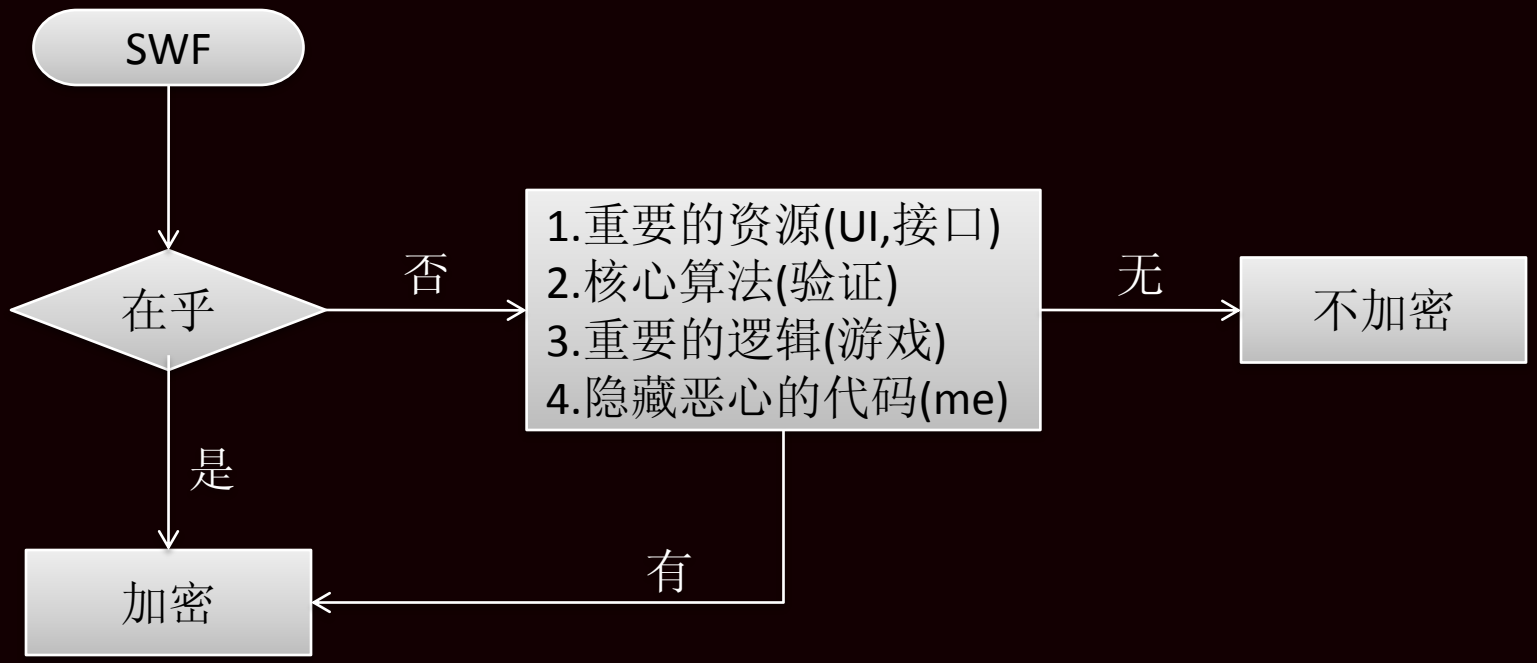
主讲人：laan


一些概念
加密
单文件加密
多文件加密
混淆
字符混淆
指令混淆
杂糅
解决方案
多文件
单文件
一些心得

加密的本质


SWF
加密
是
纠结
放弃
保护成功
否
坚持
被破解
有的时候
半破解
加密就是一个人让破解者纠结的过程。破解者越纠结，加密就越成功。

要不要加密



概念区分

——我所认为的加密和混淆

加密

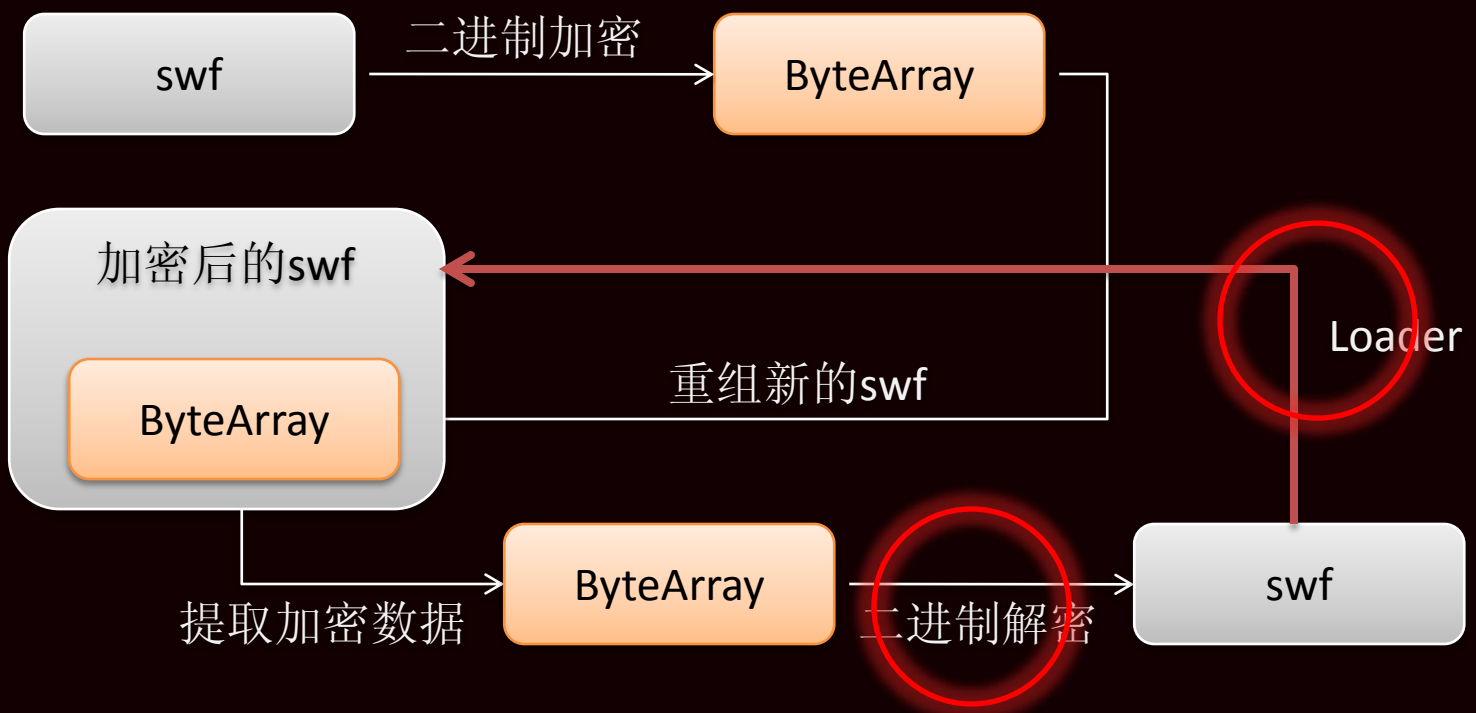
针对整个swf进行操作。处理后，包括代码、ui都被隐藏掉。

混淆

针对as代码(abc数据)进行混淆。包括包名、类名、方法名、属性名，还包括对指令的混淆

单文件加密

自加载加密[最简单明了]



单文件加密

怎么样隐藏解密算法

1.肯定没有固定的方法，不然很快就会被破解。

2.将解密过程分解为多个步骤。[指令移植]

```
private function decodeBytes(bytes:ByteArray):ByteArray {
        var key:String = “myKey”;
        //解密算法
}
```

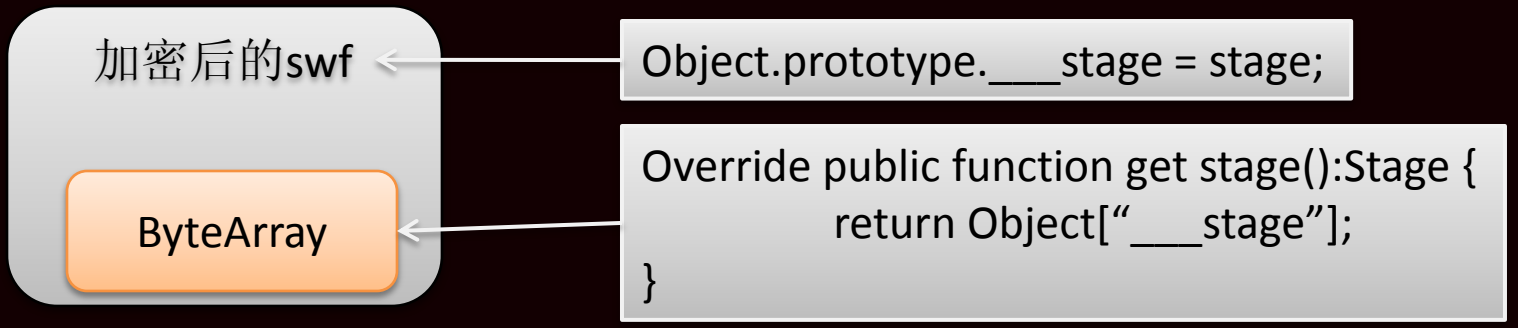
3.将解密key隐藏深一点

```
private function decodeBytes():void{
        var key:String = this[“key”];
        //解密算法
}
```

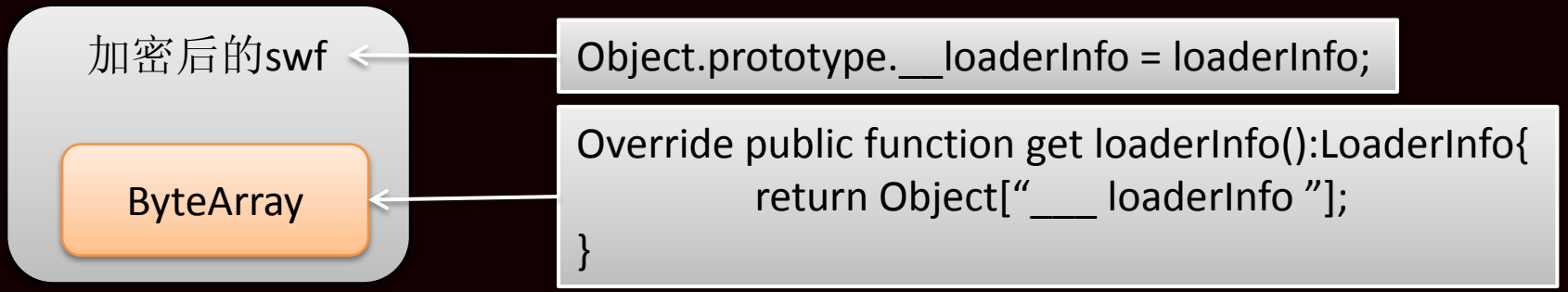
Main.prototype.key = “myKey”

自加载的局限性

1.被加密文件的Document class的构造函数中使用了stage



2.loaderInfo.paramters, loaderInfo.url

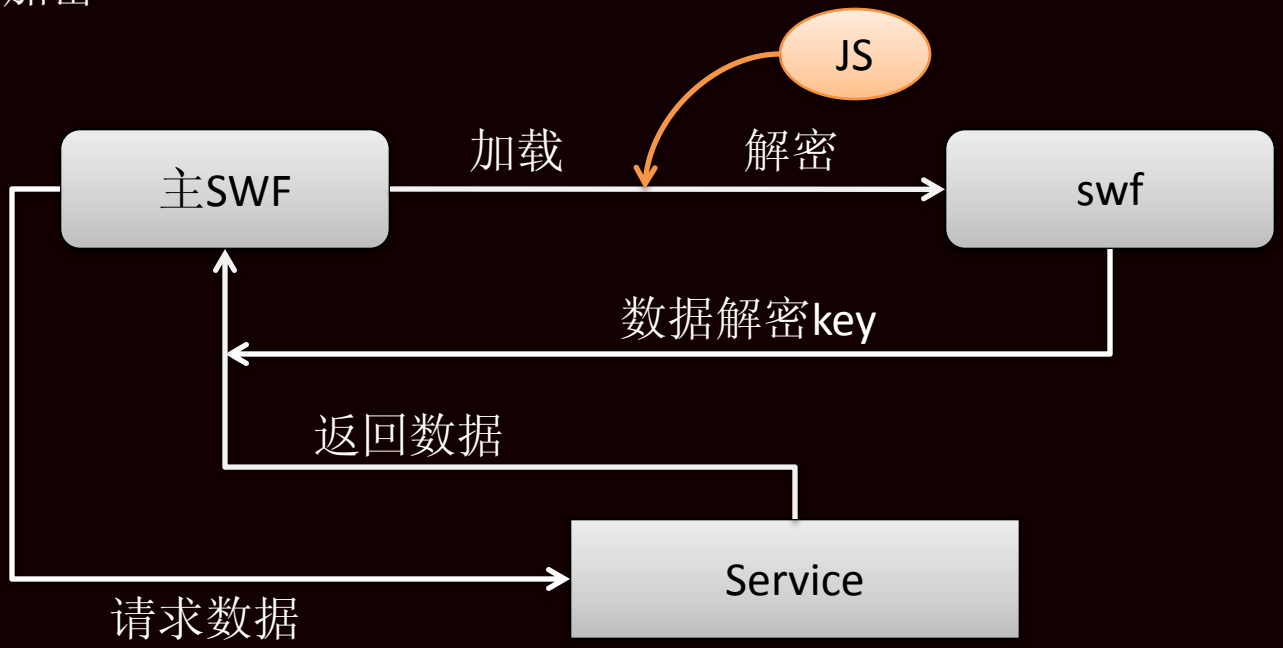


针对项目加密 多文件加密

1.使用完全相同与单个swf加密过程

[相对而言，比较容易破解]

2.依赖加密



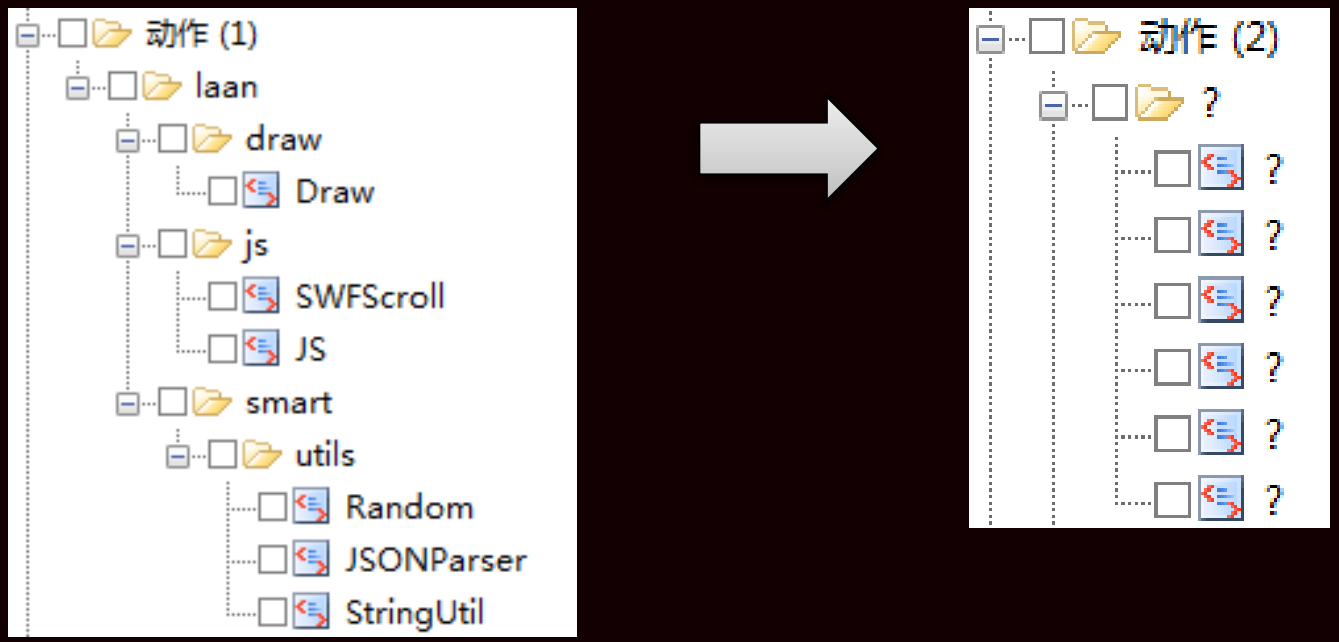
理论很简单，实现很复杂。

混淆

1. 字符混淆

将包名、类名、方法名、属性名、参数名等用很难读懂的字符替换，以达到保护代码的目的。

[不可能还原]



理论很简单，实现很复杂。

混淆

```
private function foo():String {
            return _foo;
}
```

```
ExternalInterface.call("foo");

var obj:Object = {};
obj.foo = "foo" + 1 ;
```

```
override public function get alpha():Number{
            return 0;
}
```

```
var  xml:XML = new XML(value);
var a:String = String(xml.foo);
```

理论很简单，实现很复杂。

混淆

2. 指令混淆

将在程序指令中加入冗余指令，以让破解软件无法识别或识别错误。

[效果比较好，速度、体积]

```
0    getlocal0
1    pushscope
2    getlocal0
3    constructsuper        (0)
```

```
0    getlocal0
1    pushscope
2    jump          5
3    istypelate
4    hasnext
5    label
6    getlocal0
7    constructsuper        (0)
```

```
2    jump          5
3    newObject
4    1000000
5    label
```

理论很简单，实现很复杂。

混淆

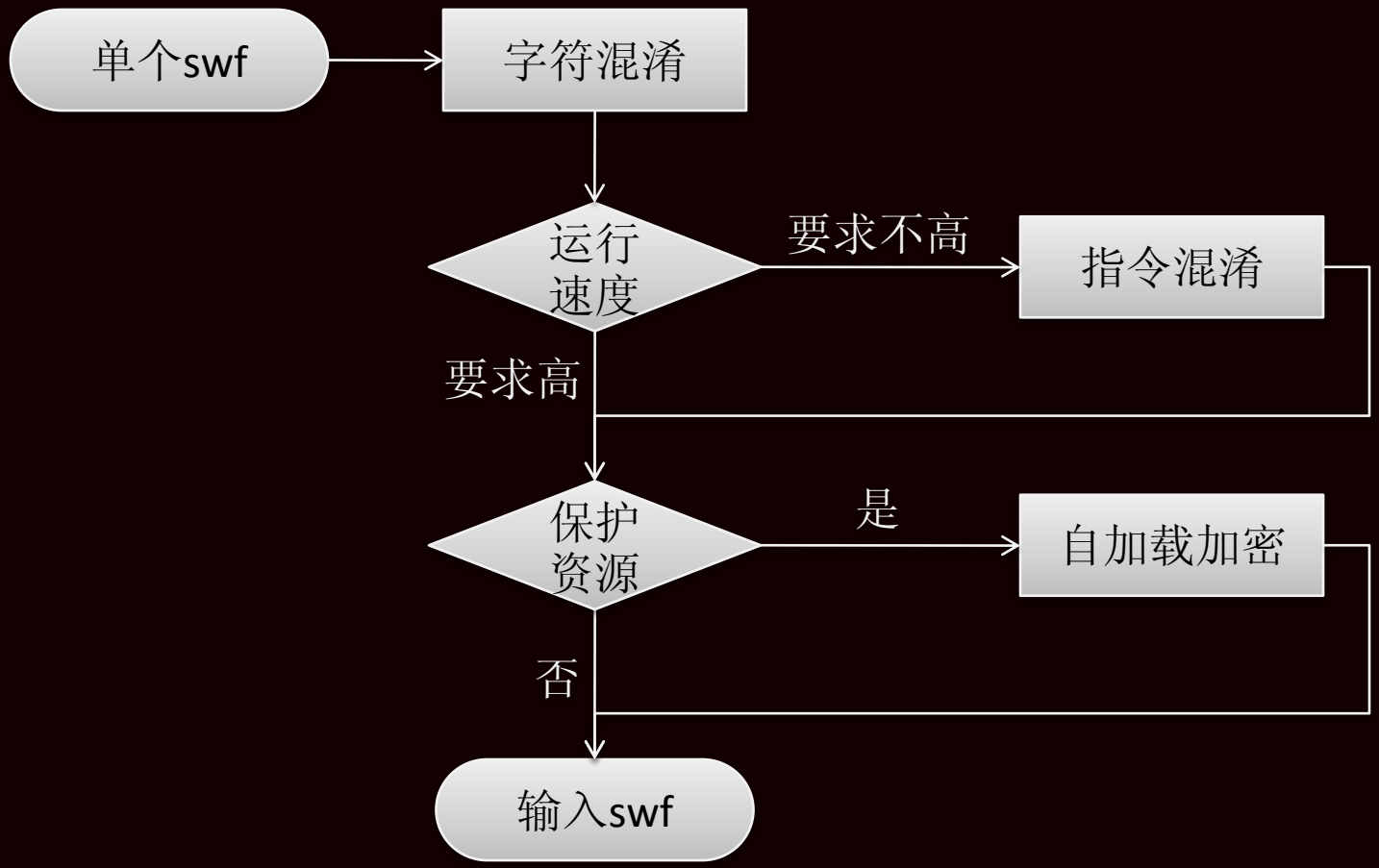
3. 杂糅

将多个类、方法合并或置换；将所有代码完全杂糅——但是又不影响程序运行。

[理想,目标]

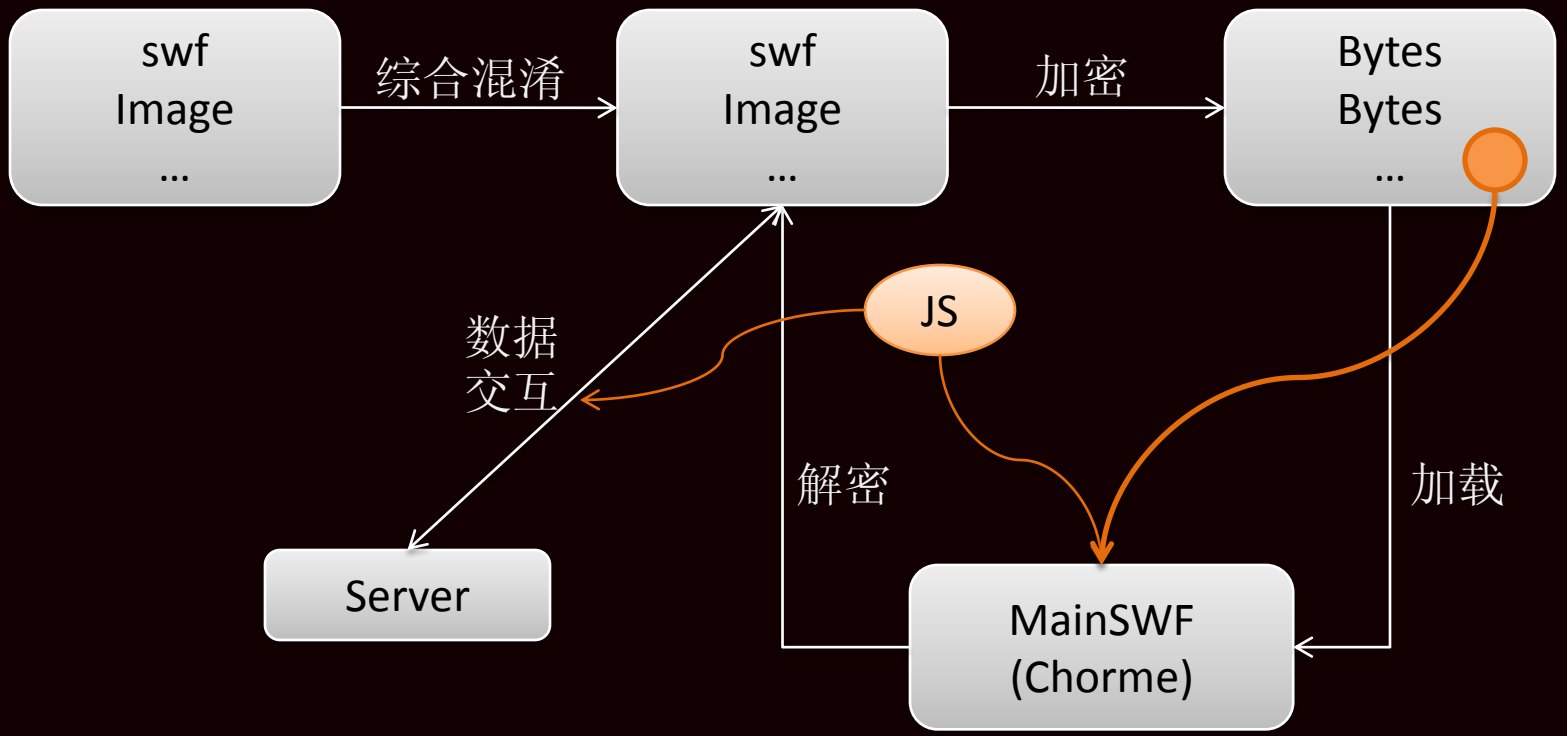
```
package laan.smart.utils {

    public class JSONParser {

        public static function encode

        // Error while decompiling!

        public static function decode

        // Error while decompiling!


    }
}//package laan.smart.utils
```

解决方案[单个swf]



解决方案[一个项目多个swf]

比较灵活，仅抛砖引玉



一些心得

- 没有绝对的加密，只有绝对恶心的加密
- 能让主流破解软件不能破解就差不多了；会手动破解的人很少。
- 做游戏外挂的人，一般是高手。建议你绕N圈，把关键代码隐藏很深。看谁更有耐心了。
- 加密是一个讲究技巧的过程。[深于他人想法]
- 开源是一个很好的选择。但是并不是什么都能开源。

谢谢 & QA