20180909

阅读前可先阅读Java中安全API内容

# 出口限制

<https://www.oracle.com/technetwork/java/javase/downloads/jce-6-download-429243.html>

将下载完后文件覆盖至JDK或JRE 下lib\securtiy目录

比如AES算法若无该文件则不能使用 256位的加密

KeyGenerator kg = KeyGenerator.getInstance( "AES" );

kg.init( 256 );

SecretKey secretKey = kg.generateKey();

System.out.println( new String( secretKey.getEncoded() ) );

否则将抛出 InvalidKeyException

# 配置加密组件Bouncy Castle

包括许多JCE不提供的算法，如MD4、IDEA、国际数据加密算法。

<!-- https://mvnrepository.com/artifact/org.bouncycastle/bcprov-jdk15on -->

<dependency>

<groupId>org.bouncycastle</groupId>

<artifactId>bcprov-jdk15on</artifactId>

<version>1.59</version>

</dependency>

<!-- https://mvnrepository.com/artifact/org.bouncycastle/bcprov-ext-jdk15on -->

<dependency>

<groupId>org.bouncycastle</groupId>

<artifactId>bcprov-ext-jdk15on</artifactId>

<version>1.59</version>

</dependency>

以MD4算法为例：

byte[] data = "Helloworld".getBytes();

MessageDigest md = MessageDigest.getInstance("MD4");

md.update(data);

byte[] digest = md.digest();

System.out.println( new String(digest));

若无配置则抛出MD4 MessageDigest not available异常

## 配置

添加至 lib\security\java.security中

security.provider.11=org.bouncycastle.jce.provider.BouncyCastleProvider

并将 bcprov-ext-jdk15-149.jar放在lib的ext中

## 调用方式

有时候需要显式引入Provider,首先将bcprov-jdk15-159.jar引入工程

则需要在初始化密钥工厂、密钥引擎之前调用如下代码：

Servurity.addProvider( new BouncyCastleProvider() )

或者，在初始化密钥工厂、密钥生成器等引擎类，采用如下方式：

MessageDigest md = MessageDigest.getInstance( “MD4”, “BC” );

## Bouncy Castle简介

JCE工具及其扩展包：仅包括 org.bouncycastle.jce。这是对JCE的支持。

JCE支持者及其测试包：包括org.bouncycastle.jce.provider包及其子包。

轻量级加密包：包括org.bouncycastle.crypto包及其子包。

OCSP和OpenSSL PEM支持包。

ASN.1编码支持包

工具包

其他包