## 国密算法测试

日期：2020-11-13 作者：刘腾飞，马璐瑶

## ·项目介绍

项目中包括SM2算法的加密/解密/签名/验签 , SM3算法的摘要计算 , SM4算法的对称加密/解密 , 以及相应算法的公私钥对的生成方法。

## ·项目测试脚本使用

在项目中的test包下SecurityTestAll.java类中的main方法下有SM2/SM3/SM4的按照加解密流程实现的一整套测试脚本，直接执行可以输出如下测试结果:

--产生SM2秘钥--:

公钥:04ec7e40b8dfa4b14383f703ec5403b71db0ab505b9fc41f0df45a9910a307dfbd5b3c5afdd4b90d79fa0ab70d53fd88422df77e09b254a53e72b4857f74ab1da4

私钥:58967e2beb6fffd3c96545eebd3000b39c10087d48faa0d41f9c7bf3720e0ea4

--测试加密开始--

原文UTF-8转hex:49204c6f766520596f75

加密:

密文:1b40e51d8462d97ac1cc9929039313152b8067eecfcff7ba0348a721d3f4d257e83f924364b84147879906d62a72472403a3c3d36d4cf243055ff77a4c794909673cc0e39954fbc8b01c50a4b708216d4d19c400719734b98bc0a6d7da92a078b6ef8dd9713cee910276

解密:I Love You

--测试加密结束--

--测试SM2签名--

原文hex:49204c6f766520596f75

签名测试开始:

软加密签名结果:3046022100d2665f92221efd00aa96d2729475aa05690bd10766641fd169c6e13c1a441b87022100c8ff9f00c7bb0a8308e183629cebef53e4fd65542c7ee6068275a606e3010088

加密机签名结果:d2665f92221efd00aa96d2729475aa05690bd10766641fd169c6e13c1a441b87c8ff9f00c7bb0a8308e183629cebef53e4fd65542c7ee6068275a606e3010088

验签1,软件加密方式:

软件加密方式验签结果:true

验签2,硬件加密方式:

签名R:d2665f92221efd00aa96d2729475aa05690bd10766641fd169c6e13c1a441b87

签名S:c8ff9f00c7bb0a8308e183629cebef53e4fd65542c7ee6068275a606e3010088

硬件加密方式验签结果:true

--签名测试结束--

--SM3摘要测试--

hash:700B1D31B7BF81A3CE2B5AC97057AE783C9C51F56FA4EA14E13CF3EC6E58159A

--SM3摘要结束--

--生成SM4秘钥--

sm4Key:c8e8e733ac8c4043a1d6464ae82d70e6

--生成SM4结束--

--SM4的CBC加密--

密文:046be2948f89c9f78e9248fc562a9d0c

CBC解密

解密结果:I Love You

--ECB加密--

ECB密文:851b68592ac1a029976204ef66f62a5d

ECB解密

ECB解密结果:I Love You

## ·SM2

SM2秘钥格式说明

在本项目中 , SM2算法中秘钥都是在DER编码下输出的 , SM2秘钥的组成部分有 私钥D 、公钥X 、公钥Y , 他们都可以用长度为64的16进制的HEX串表示 。在加解密调用的时候都会将hexString转换成byte[]后再作为参数传入。其中SM2公钥并不是直接由X+Y表示 , 而是额外添加了一个头。

SM2签名说明

SM2签名结果可以分解为签名R和签名S , 在本项目中签名返回的签名结果软件加密和硬件加密也存在头不一致的情况 , 硬件加密机返回的签名结果是标准的R+S , 而软件加密返回的签名结果有所不同。

## ·SM3

在商用密码体系中，SM3主要用于数字签名及验证、消息认证码生成及验证、随机数生成等，其算法公开。据国家密码管理局表示，其安全性及效率与SHA-256相当。

## ·SM4

2012年3月，国家密码管理局正式公布了包含SM4分组密码算法在内的《祖冲之序列密码算法》等6项密码行业标准。与DES和AES算法类似，SM4算法是一种分组密码算法。其分组长度为128bit，密钥长度也为128bit。加密算法与密钥扩展算法均采用32轮非线性迭代结构，以字（32位）为单位进行加密运算，每一次迭代运算均为一轮变换函数F。SM4算法加/解密算法的结构相同，只是使用轮密钥相反，其中解密轮密钥是加密轮密钥的逆序。

SM4秘钥说明

由于SM4秘钥长度为32位的hex串 , 所以本项目中直接使用UUID随机生成的秘钥串。

SM4的ECB模式和CBC模式

SM4加解密涉及到ECB模式和CBC模式 , ECB模式简单有利于计算,但是存在被攻击的可能 , CBC模式更加安全 , 在加解密的过程中需要传入一个IV值 , 在本项目中IV值均设置为16进制下的字符串:"31313131313131313131313131313131" , 其实就是UTF-8下的16个"1" 通过getBytes[].toHexString()得来的，这个值可以根据需要修改。

在SM4加密算法中 , 要求原始数据长度必须是长度为32的整数倍hex串 , 但是在实际情况中数据长度并不能保证这么长 , 这里就涉及到了原始数据填充的问题 , 在类SM4.java文件中padding()方法使用基于PBOC2.0的加解密数据填充规范 , 在数据后填充一个0x80和多个0x00来解决数据长度填充的问题。