# **相关概念**

ECC：

ECC（EllipticCurves Cryptography，椭圆曲线密码编码学）是由Koblitz和Miller两人于1985年提出，其数学基础是基于椭圆曲线上离散对数计算难题（ECDLP）。ECC算法的数学理论非常深奥和复杂，在工程应用中比较难以实现，但它的单位安全强度相对较高。用国际上公认的针对ECC算法最有效的攻击方法——Pollard rho方法去破译和攻击ECC算法，它的破译或求解难度基本上是指数级的。

因此，ECC算法的单位安全强度远高于RSA算法，可以用较少的计算能力提供比RSA算法更高的安全强度，而所需的密钥长度却远比RSA算法低。目前，****基于ECC的SM2证书普遍采用256位密钥长度，加密强度等同于3072位RSA证书，远高于业界普遍采用的2048位RSA证书。****

此外，为了提高安全强度必须不断增加密钥长度，ECC算法密钥长度增长速度较慢（例如：224-256-384），而RSA算法密钥长度则需呈倍数增长（例如：1024-2048-4096）。



# **SM2椭圆曲线公钥密码算法**

**简介：**

SM2算法就是ECC椭圆曲线密码机制，但在签名、密钥交换方面不同于ECDSA、ECDH等国际标准，而是采取了更为安全的机制。另外，SM2推荐了一条256位的曲线作为标准曲线。  
SM2标准包括总则，数字签名算法，密钥交换协议，公钥加密算法四个部分，并在每个部分的附录详细说明了实现的相关细节及示例。  
SM2算法主要考虑素域Fp和F2m上的椭圆曲线，分别介绍了这两类域的表示，运算，以及域上的椭圆曲线的点的表示，运算和多倍点计算算法。然后介绍了编程语言中的数据转换，包括整数和字节串，字节串和比特串，域元素和比特串，域元素和整数，点和字节串之间的数据转换规则。详细说明了有限域上椭圆曲线的参数生成以及验证，椭圆曲线的参数包括有限域的选取、椭圆曲线方程参数、椭圆曲线群基点的选取等，并给出了选取的标准以便于验证。最后给椭圆曲线上密钥对的生成以及公钥的验证，用户的密钥对为（s，sP），其中s为用户的私钥，sP为用户的公钥，由于离散对数问题从sP难以得到s，并针对素域和二元扩域给出了密钥对生成细节和验证方式。  
数字签名算法、密钥交换协议以及公钥加密算法都使用了国家密管理局批准的SM3密码杂凑算法和随机数发生器。数字签名算法、密钥交换协议以及公钥加密算法根据总则来选取有限域和椭圆曲线，并生成密钥对。

SM2算法在很多方面都优于RSA算法。

**优点：**

SM2算法具有抗攻击性强、CPU 占用少、内容使用少、网络消耗低、加密速度快等特点。

**参考资料：**

<https://www.cnblogs.com/alsodzy/p/9854521.html>

# **SM3杂凑算法**

**简介：**

SM3密码杂凑（哈希、散列）算法给出了杂凑函数算法的计算方法和计算步骤，并给出了运算示例。此算法适用于商用密码应用中的数字签名和验证，消息认证码的生成与验证以及随机数的生成，可满足多种密码应用的安全需求。在SM2，SM9标准中使用。  
此算法对输入长度小于2的64次方的比特消息，经过填充和迭代压缩，生成长度为256比特的杂凑值，其中使用了异或，模，模加，移位，与，或，非运算，由填充，迭代过程，消息扩展和压缩函数所构成。具体算法及运算示例见SM3标准。

**参考资料：**

<https://www.cnblogs.com/Marydon20170307/p/9303233.html>

# **SM4对称算法**

**简介：**

此算法是一个分组算法，用于无线局域网产品。该算法的分组长度为128比特，密钥长度为128比特。加密算法与密钥扩展算法都采用32轮非线性迭代结构。解密算法与加密算法的结构相同，只是轮密钥的使用顺序相反，解密轮密钥是加密轮密钥的逆序。  
此算法采用非线性迭代结构，每次迭代由一个轮函数给出，其中轮函数由一个非线性变换和线性变换复合而成，非线性变换由S盒所给出。其中rki为轮密钥，合成置换T组成轮函数。轮密钥的产生与上图流程类似，由加密密钥作为输入生成，轮函数中的线性变换不同，还有些参数的区别。SM4算法的具体描述和示例见SM4标准。

参考资料：

<https://www.cnblogs.com/Marydon20170307/p/9266946.html>

填充模式：

PKCS5

PKCS7

参考资料：<https://blog.csdn.net/wjb123sw99/article/details/105015933>

加密模式：

### ECB

****优点:****

1.简单；

2.有利于并行计算；

3.误差不会被传送；

****缺点:****

1.不能隐藏明文的模式；

2.可能对明文进行主动攻击；

### CBC

****优点：****

1.不容易主动攻击,安全性好于ECB,适合传输长度长的报文,是SSL、IPSec的标准。

****缺点：****

1.不利于并行计算；

2.误差传递；

3.需要初始化向量IV

### CFB

****优点：****

1.隐藏了明文模式;

2.分组密码转化为流模式;

3.可以及时加密传送小于分组的数据;

****缺点:****

1.不利于并行计算;

2.误差传送：一个明文单元损坏影响多个单元;

3.唯一的IV;

### OFB

****优点:****

1.隐藏了明文模式;

2.分组密码转化为流模式;

3.可以及时加密传送小于分组的数据;

****缺点:****

1.不利于并行计算;

2.对明文的主动攻击是可能的;

3.误差传送：一个明文单元损坏影响多个单元;

参考：<https://www.iteye.com/blog/ctwen-1591712>

# **SM9标识密码算法**

**简介：**

为了降低公开密钥系统中密钥和证书管理的复杂性，以色列科学家、RSA算法发明人之一Adi Shamir在1984年提出了标识密码（Identity-Based Cryptography）的理念。标识密码将用户的标识（如邮件地址、手机号码、QQ号码等）作为公钥，省略了交换数字证书和公钥过程，使得安全系统变得易于部署和管理，非常适合端对端离线安全通讯、云端数据加密、基于属性加密、基于策略加密的各种场合。2008年标识密码算法正式获得国家密码管理局颁发的商密算法型号：SM9(商密九号算法)，为我国标识密码技术的应用奠定了坚实的基础。  
SM9算法不需要申请数字证书，适用于互联网应用的各种新兴应用的安全保障。如基于云技术的密码服务、电子邮件安全、智能终端保护、物联网安全、云存储安全等等。这些安全应用可采用手机号码或邮件地址作为公钥，实现数据加密、身份认证、通话加密、通道加密等安全应用，并具有使用方便，易于部署的特点，从而开启了普及密码算法的大门。

# **Smxstudy项目**

**SM2Test有3个测试用例，分别是非对称加密测试、数字签名测试、2个用户间协商会话密钥测试。会话密钥测试协商的会话密码可用于作为sm4的对称加密的key,来加密会话信息。**

**活跃的q群**

**629078626**

**工具使用**

**输入的数据都是二进制解密后的数据**