什么是国密算法？

国密算法是指由中国国家密码管理局发布的密码算法标准，旨在保障国家信息安全。目前，国家密码管理局已发布了一系列国产商用密码标准算法，包括 SM1（SCB2）、SM2、SM3、SM4、SM7、SM9 以及祖冲之密码算法（ZUC）等。通过在金融、电子政务及安防等领域广泛应用国密算法，在对敏感数据进行机密性、完整性和可用性保护的同时，减少对外部密码产品的依赖，提升国家信息安全水平。

*查看更多词条，请访问：*https://wiki.h3c.com

为什么需要国密算法？

国密算法的产生背景

在网络信息传输和存储过程中，数据的保密性和安全性是一项重要的需求。传统的国际标准加密算法虽然安全可靠，但由于无法保证源代码的安全性，因此存在着源代码被外部恶意攻击者渗透或篡改的风险。为了构建安全的行业网络环境并增强国家行业信息系统的“安全可控”能力，中国积极开展了针对信息安全需求的研究和探索。自 2007 年开始，中国制定了国密算法标准，并于 2010 年正式发布。

经过多年的发展、改进和完善，国密算法已成为中国自主研发的密码算法标准，并在各行业得到广泛应用。它的诞生不仅显著提升了中国在密码技术领域的核心竞争力，还为国家信息安全建设作出了重要贡献。

国密算法的特点

国密算法具备如下特点：

- 安全性高：国密算法采用了严密的密码学原理和复杂的运算方式，具有较高的安全性。它在加密、数字签名和哈希等功能上都能提供可靠的保护，抵抗了各种传统和现代密码攻击手段。
- 高效性与灵活性：国密算法在保证安全性的同时，注重算法的效率。它的加密速度和运行效率相对较高，同时也能适应不同的密码长度和密钥长度，以满足不同场景的需求。
- 标准化广泛：国密算法已被国家标准化机构认可和采用。它符合国际密码学标准的基本要求，具备与国际算法相媲美的能力。同时，国密算法也在国内推广和应用广泛，成为中国信息安全领域的基础核心算法之一。
- 自主创新：国密算法是中国自主研发的密码算法，所以对于算法的实现和推广都具有独立的掌控能力。这意味着中国可以更好地保护自己的国家信息安全，减少对外依赖，提高自主抵抗能力。

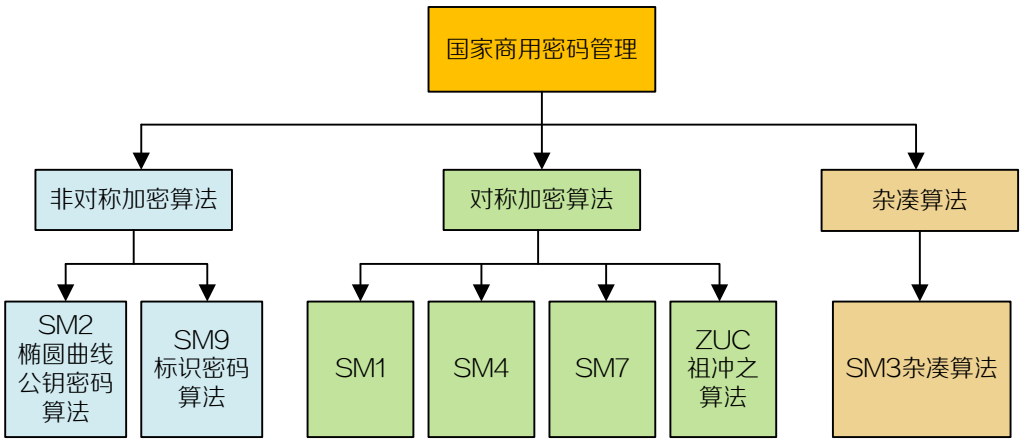
- 面向多领域应用：国密算法不仅局限于某个特定领域的应用，它适用于金融业、电子商务、通信、物联网、区块链等不同领域的信息安全保护。它的广泛应用范围使得国密算法可以满足不同行业的安全需求。

国密算法如何工作？

国密算法包括 SM1（SCB2）、SM2、SM3、SM4、SM7、SM9 以及祖冲之密码算法（ZUC）等。其中，SM1、SM4、SM7、祖冲之密码（ZUC）属于对称算法；SM2、SM9 属于非对称算法；SM3 属于杂凑算法。

下文将主要介绍国密算法中的常用算法 SM1、SM2、SM3 和 SM4 的实现和应用。

图1 国密算法分类

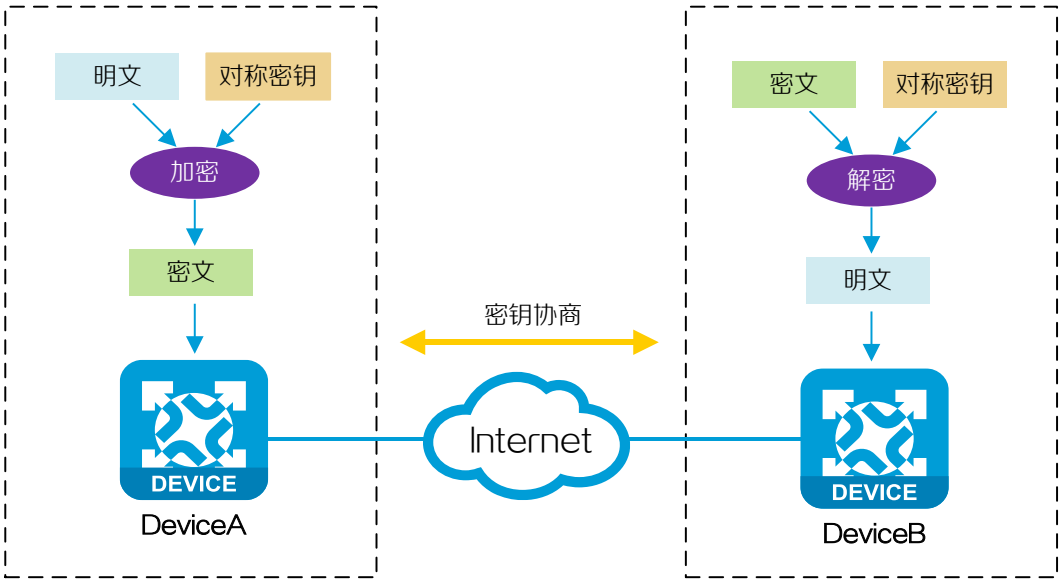


SM1 算法的实现和应用

SM1 算法是国密算法中的一种对称加密算法，其特点是加解密使用相同密钥。利用 SM1 对称加密算法加解密数据的过程如图 2 所示。

SM1 算法未公开，仅以 IP 核（Intellectual Property Core，一种预先做好的集成电路功能模块）的形式存在于芯片中。SM1 算法主要用于小数据量的加密保护，因此被广泛用于研制智能 IC 卡、智能密码钥匙、门禁卡、加密卡等安全产品。

图2 对称加密算法加解密原理示意图



SM2 算法的实现和应用

SM2 算法是基于 ECC（Elliptic Curve Cryptography）椭圆曲线的非对称加密算法，包括了 SM2-1 椭圆曲线数字签名算法、SM2-2 椭圆曲线密钥交换协议和 SM2-3 椭圆曲线公钥加密算法，分别用于实现数字签名、密钥协商和数据加密等功能。

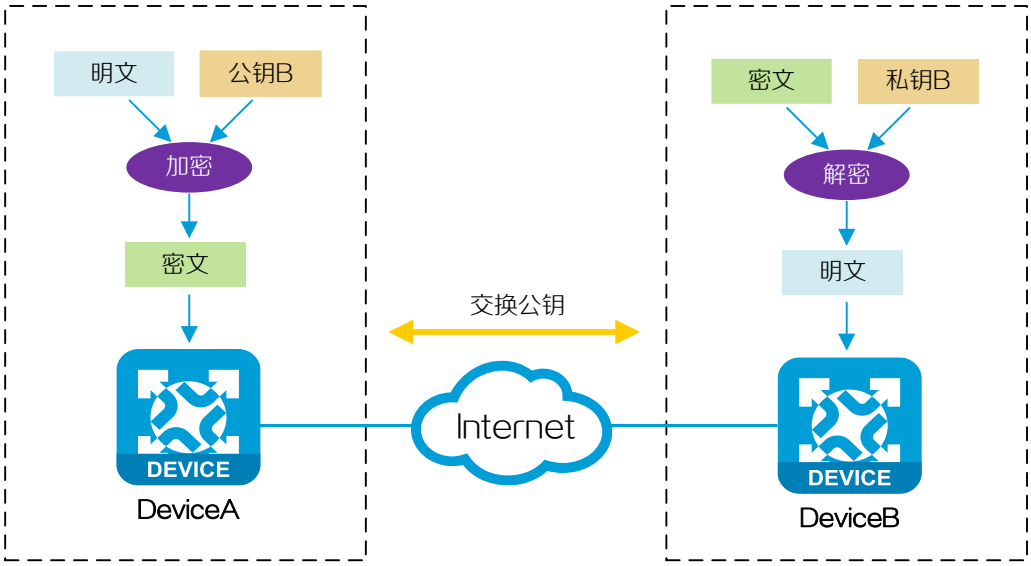
SM2 算法在许多领域都有广泛的应用。在电子商务领域，SM2 算法被用于保护用户个人信息的安全传输，确保用户在网上交易过程中的隐私和财产的安全。在互联网金融领域，SM2 算法被用于数字支付、电子银行等场景，实现用户身份认证和交易的安全性。此外，SM2 算法还适用于物联网领域，保护物联网设备之间的通信安全，确保数据的可靠传输。

数据加密

在非对称加密算法中，可对外公布的密钥称为“公钥”，只有持有者所知的密钥称为“私钥”。发送者使用接收者的公钥来加密消息，接收者用自己的私钥解密和读取该消息。

利用 SM2 非对称加密算法加解密数据的过程如图 3 所示。

图3 非对称加密算法加解密原理示意图



密钥协商

由于椭圆曲线的计算复杂性高，破解难度大，因此 SM2 算法在密钥协商技术领域也起着关键作用。利用 SM2 算法进行密钥协商的过程如图 4 所示。

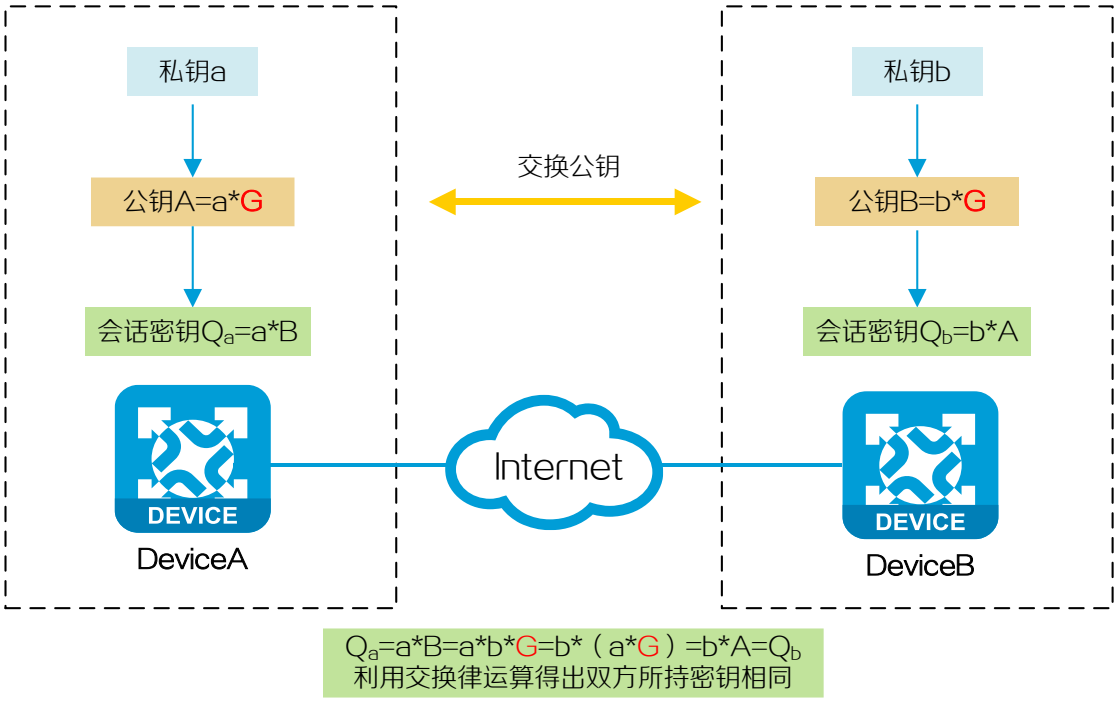
(1) 会话双方生成自己的私钥（随机数）。

(2) 会话双方由私钥、ECC 椭圆曲线参数 G 各自计算出公钥。

(3) 会话双方将自己的公钥传递给对方，传递过程公开。由于椭圆曲线的计算复杂性高，破解难度大，因此攻击者难以通过公钥和椭圆曲线参数 G 反推出私钥。

(4) 双方将自己的私钥与对方的公钥进行运算，最终得到相同的会话密钥，该会话密钥可作为共享密钥用于对称加密（例如 SM4 算法）通信。

图4 SM2 算法密钥协商原理示意图



数字签名

数字签名是一种用于验证信息完整性、真实性和来源的技术手段。它通常用于确保数据在传输或存储过程中没有被篡改，并且可以追溯到特定的发送方。发送方使用自己的私钥对消息进行加密，生成数字签

名。接收方使用发送方的公钥对签名进行解密和验证，以验证消息的完整性和真实性。

在数字签名应用中，SM2 算法通常与 SM3 摘要算法一起使用，具体的实现过程请参见 SM3 算法的实现和应用中的图 5。

SM3 算法的实现和应用

SM3 杂凑（Hashing）算法是国密算法中的一种摘要算法。SM3 算法通过哈希函数将任意长度的消息压缩成固定长度的摘要。摘要具有唯一性，即不同信息生成的摘要不同，且无法由摘要恢复出原始信息，更无法伪造信息获得相同摘要，因此 SM3 算法被广泛用于实现数字签名、数据完整性检测及消息验证等功能。

基于 SM3 算法的特点，在信息安全领域，SM3 算法被用于保护密码学协议、数字证书和电子签名等数据的完整性。在区块链领域，SM3 算法被用于加密货币的区块生成和链上交易的校验，确保区块链的安全性。此外，SM3 算法还可以应用于密码学随机数的生成和伪随机序列的校验等领域，增加了数据的安全性和可靠性。

利用 SM2 算法和 SM3 算法对用户数据进行数字签名认证及完整性校验的过程如图 5 所示。

(1) 用户 A 发送的数据 A 经过 SM3 哈希算法运算生成摘要 A。

(2) 摘要 A 经过用户 A 的私钥加密生成数字签名。

(3) 用户 A 的明文数据和数字签名经加密算法（SM1/SM2/SM4）加密成密文后发送给用户 B。图 5 中加密算法以非对称加密算法 SM2 为例，即加解密使用不同密钥。

(4) 密文到达用户 B 处，经加密算法（SM1/SM2/SM4）解密后，还原成明文数据和数字签名。

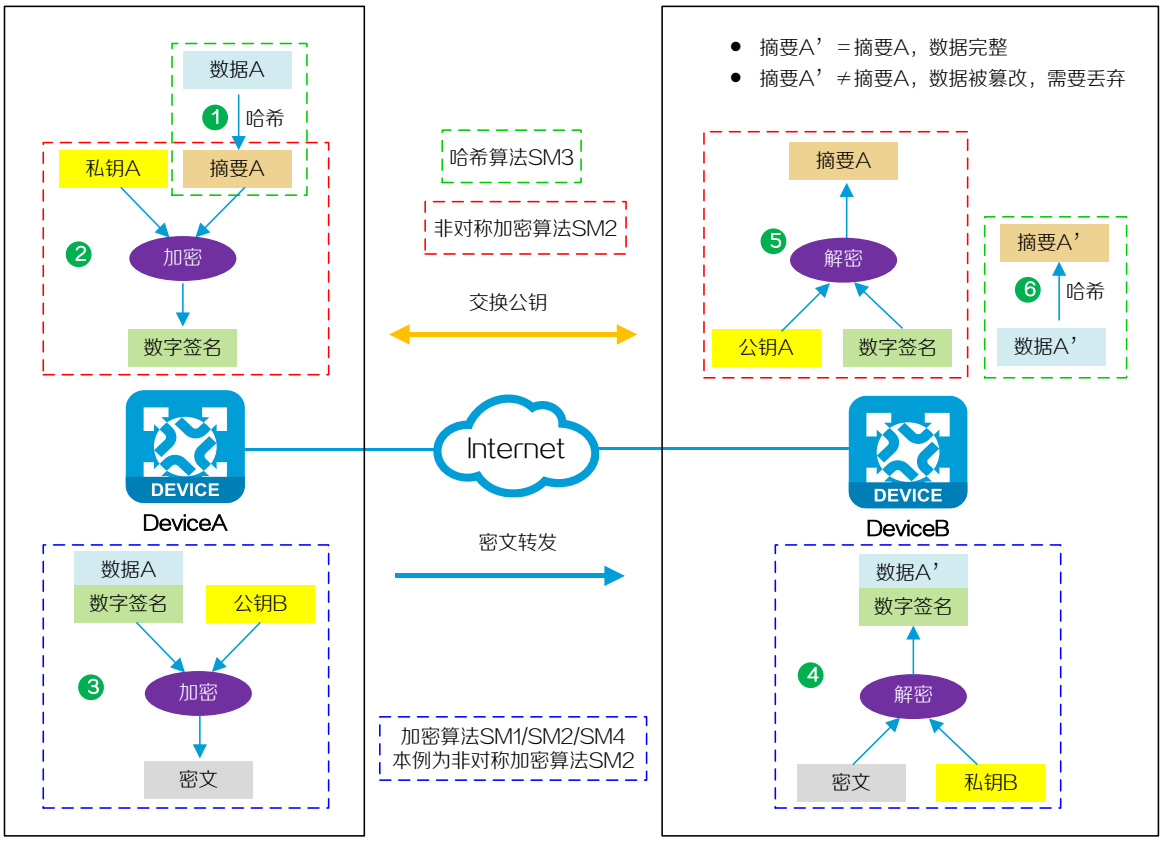
(5) 用户 B 使用用户 A 的公钥解密数据包中的数字签名：

- 解密成功，数据来源合法，得到摘要 A；
- 解密失败，数据来源非用户 A，丢弃本次数据。

(6) 收到的数据包中的明文数据经过 SM3 哈希运算生成摘要 A’。对比摘要 A 和摘要 A’：

- 摘要 A’＝摘要 A，数据完整；
- 摘要 A’≠摘要 A，数据被篡改，丢弃本次数据。

图5 SM2/SM3 算法数字签名认证及完整性校验原理示意图



SM4 算法的实现和应用

与 SM1 算法分类相同，SM4 算法同样为分组对称加密算法，但 SM4 算法实现公开。

分组加密算法是将明文数据按固定长度进行分组，用同一密钥逐组加密，密文解密时同样使用相同密钥逐组解密。SM4 算法实现简单，因此加解密速度较快，消耗资源少，主要用于大数据量的加密和解密，例如静态储存或数据信号传输通道中数据的加解密。

在网络安全领域，SM4 算法被用于保护网络传输和存储的敏感数据，如银行卡信息、密码等。在物联网领域，SM4 算法被用于物联网设备之间的通信和数据加密，确保物联网数据的隐私安全。此外，SM4 算法还可以应用于区块链领域，保护加密货币的交易安全等领域，为相关系统和数据的安全提供了保障。

加解密模式

SM4 算法支持 ECB、CBC、CFB 等多种分组模式，下文将介绍 ECB 和 CBC 两种基础模式。

- ECB 模式

SM4 算法基于 ECB 模式对数据加解密的过程如图 6、图 7 所示。

(1) 发送端将明文按固定长度分组，对每个明文分组分别使用相同的密钥进行加密生成密文分组。完整的密文由所有密文分组按序排列组合而成。

(2) 接收端将密文按固定长度分组，对每个密文分组分别使用相同的密钥进行解密生成明文分组。所有明文分组按序排列组合而成完整的明文数据。

ECB 模式实现简单，各段数据间互不影响，有利于并行运算，但相同的明文块会被加密成相同的密文块，不能提供严格的数据保密性。

图6 基于 ECB 模式加密明文示意图

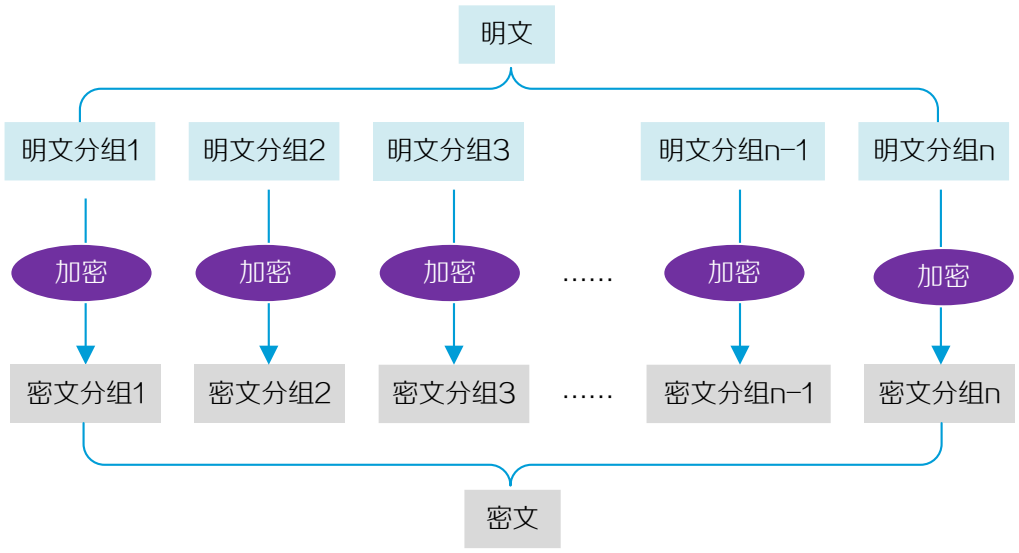
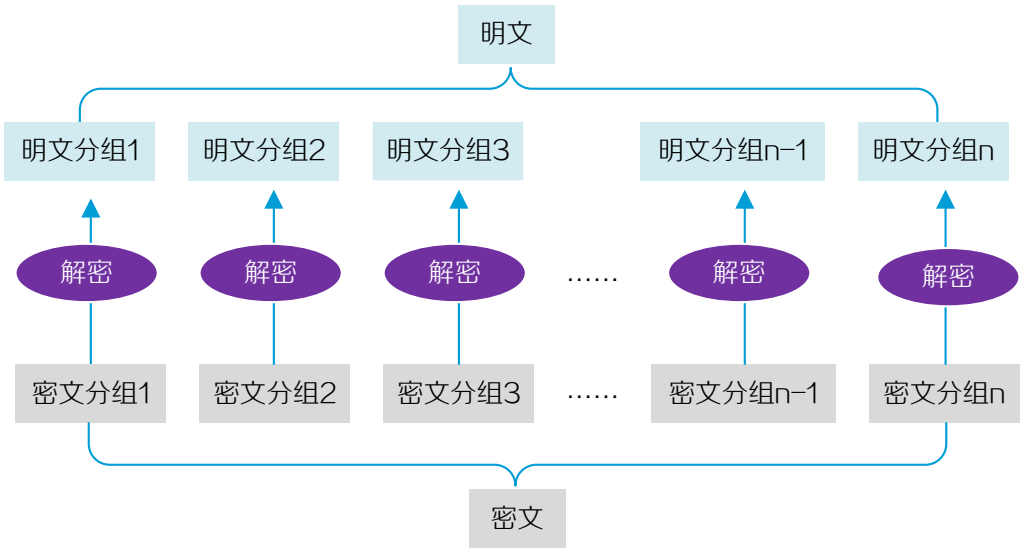


图7 基于 ECB 模式解密密文示意图



- CBC 模式

SM4 算法基于 CBC 模式对明文加密的过程如图 8 所示。

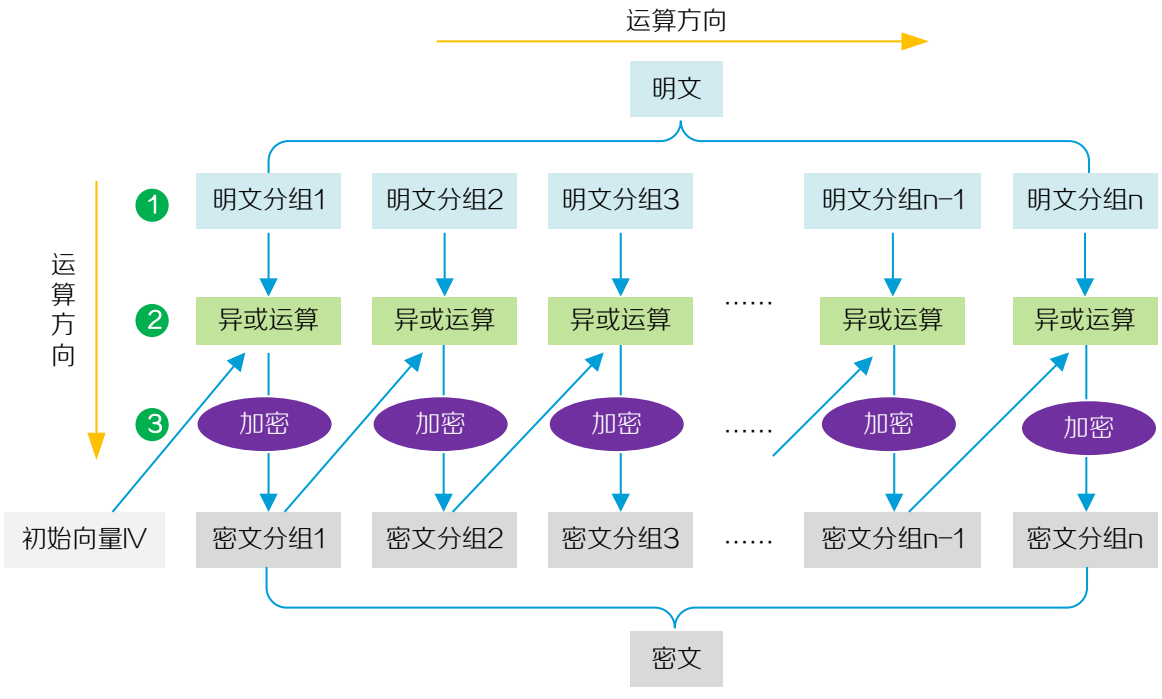
(1) 将明文按固定长度分组。

(2) 明文分组 1 与初始向量 IV 进行异或运算，异或运算的结果经密钥加密后得到密文分组 1。

(3) 剩余的明文分组依次与前一个密文分组进行异或运算后再加密，得到对应的密文分组。

(4) 完整的密文由所有密文分组按序排列组合而成。

图8 基于 CBC 模式加密明文示意图



SM4 算法基于 CBC 模式对密文解密的过程如图 9 所示。

(1) 将密文按固定长度分组后，对密文分组进行倒序处理。

(2) 对密文分组 n 先使用密钥进行解密，密文分组 n 解密后的数据与密文分组 n-1 进行逻辑逆运算，得到明文分组 n。

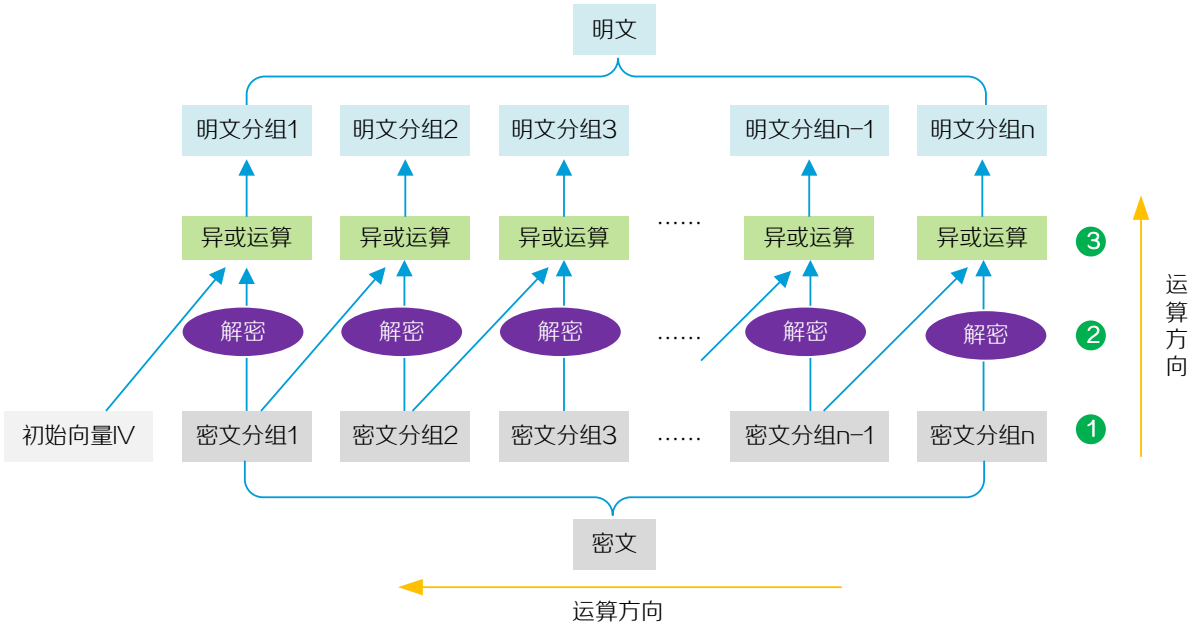
(3) 同理，剩余的密文分组解密后再与前一个密文分组进行逻辑逆运算，得到对应的明文分组。

(4) 最后，密文分组 1 用密钥解密后的数据是与初始向量进行逻辑逆运算，然后得到明文分组 1。

(5) 完整的明文由所有明文分组按序排列组合而成。

CBC 模式安全性高于 ECB，但明文块不能并行计算，且误差会传递下去。

图9 基于 CBC 模式解密明文示意图



国密算法与国际标准算法的对比

国密算法和国际标准算法都是现代密码学中常用的加密算法，但在技术和优劣方面存在一些区别。常见国密算法与国际标准算法各参数性能的对比如下：

表1 加密算法 DES、AES、SM1、SM4 对比

对比项	DES 算法	AES 算法	SM1 算法	SM4 算法
计算结构	难，基于标准的算数和逻辑运算，不含	极难，基于字节代换、行代换等，不含非	未公开	极难，基于基本轮函数+迭代，含非线性

对比项	DES 算法	AES 算法	SM1 算法	SM4 算法
	非线性变换	线性变换		变换
分组长度	64位	128位	128位	128位
密钥长度	64位（3DES为128位）	128/192/256位	128位	128位
计算轮次	16轮（3DES为48轮）	20/12/14轮	未公开	32轮
安全性	较低（3DES较高）	较高	与AES相当	较高

表2 SM2、RSA 算法对比

对比项	RSA 算法	SM2 算法
计算结构	难，基于可逆幂模运算	极难，基于椭圆曲线上点群离散对数难题
计算复杂度	亚指数级	完全指数级
密钥长度（相同安全性能下）	较长	较短

对比项	RSA 算法	SM2 算法
密钥生成速度	慢	较RSA算法快百倍以上
安全性	一般	较高

表3 杂凑算法 SM3、SHA 对比

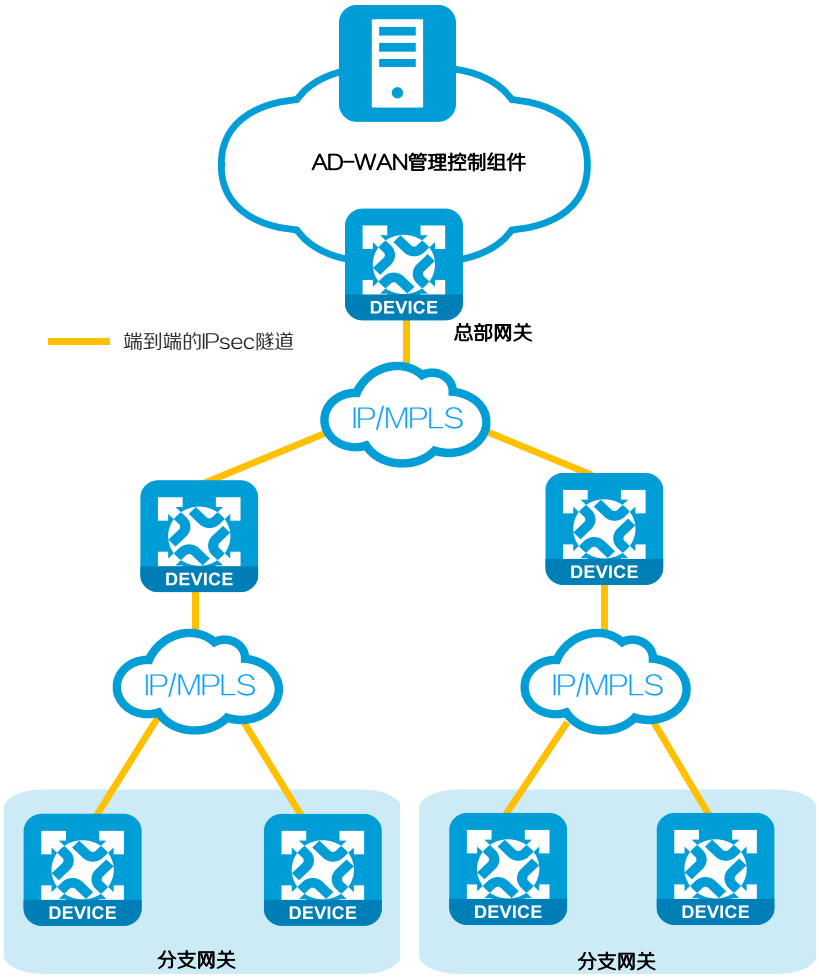
对比项	SHA1 算法	SHA256 算法	SM3 算法
计算结构	函数结构类似，但SM3算法设计更复杂		
摘要长度	160位	256位	256位
运算速度	较快	略低于SHA1	略低于SHA1
安全性	一般	较高	高于SHA256

国密算法的典型应用场景有哪些？

AD-WAN 纵向 IP/MPLS 组网

国密算法可以与 AD-WAN 技术结合，应用于 IP/MPLS 纵向网场景。通过 AD-WAN 智能运维平台，实现国密配置一键下发，在网络中构建国密数据加密通道，实现基于国密的端到端的 IPsec 隧道保护。

图10 AD-WAN 纵向网场景



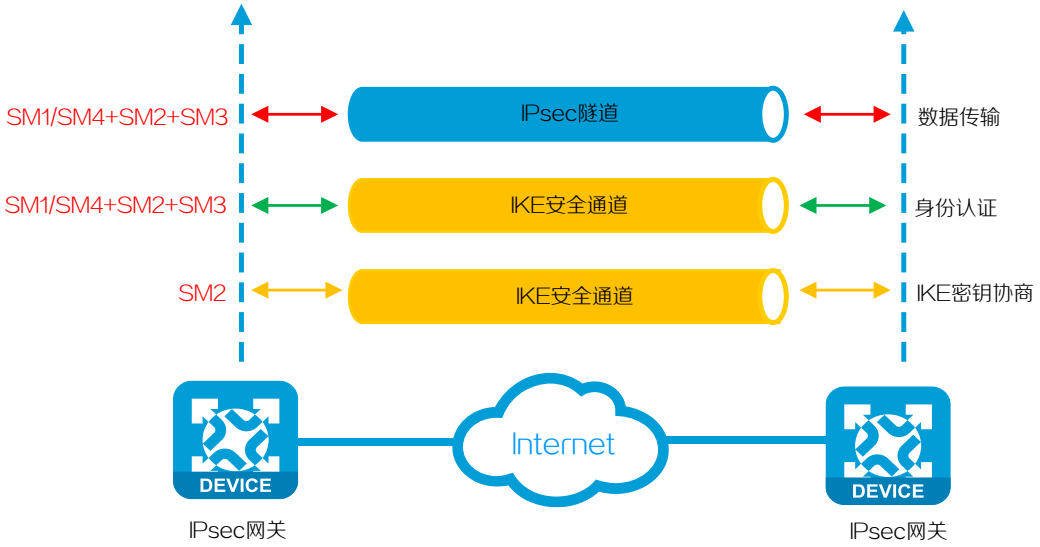
国密算法在端到端的 IPsec 隧道中的工作原理如下：

(1) 在 IKE 密钥协商阶段，使用 IKE 协议进行密钥协商过程中，采用 SM2 算法生成会话密钥。

(2) 在身份认证阶段，本端使用 SM2 和 SM3 算法生成身份信息的数字签名，并使用 SM1 或 SM4 算法和会话密钥对身份信息和数字签名进行加密；对端收到加密的身份信息后，使用相同的会话密钥解密，然后通过 SM2 和 SM3 算法进行身份认证。

(3) 在数据传输阶段，本端使用 SM2 和 SM3 算法生成用户数据的数字签名，并使用 SM1 或 SM4 算法以及会话密钥对用户数据和数字签名进行加密；对端收到加密的用户数据后，使用相同的会话密钥解密，然后通过 SM2 和 SM3 算法进行数据完整性检查。

图11 国密算法在端到端的 IPsec 隧道中的工作原理



4G/5G VPDN 业务组网

4G/5G VPDN（Virtual Private Dialup Network，虚拟专有拨号网络）业务是在 4G/5G 无线网络中采用拨号方式实现的一种虚拟专有网络业务。它利用 L2TP 技术为客户构建与互联网隔离的隧道，以满足客户分支和总部内网通信的需求。VPDN 组网同时支持将 L2TP 和 IPsec 技术结合，通过 L2TP 完成用户认证确保接入安全，并利用 IPsec 保障通信数据安全。

(1) 4G/5G VPDN 组网中分支网关由 4G/5G 路由设备担任，通过拨号接入运营商网络。

(2) 运营商对 4G/5G 路由设备的 APN（Access Point Name，接入点名称）、账户、SIM/USIM 卡信息进行认证。

(3) 4G/5G 路由设备认证通过后被运营商判断是 VPDN 用户，同时由运营商 AAA 服务器向 LAC（L2TP Access Concentrator，L2TP 访问集中器）设备下发 L2TP 隧道属性，LAC 设备将基于下发的 L2TP 隧道属性信息向该 VPDN 用户所属总部的 LNS（L2TP Network Server，L2TP 网络服务器）设备发起隧道建立请求。

(4) L2TP 隧道建立后，LAC 设备会通过此隧道向 LNS 设备透传用户的认证信息。LNS 设备向总部内网的 AAA 服务器发起对 VPDN 用户的二次认证，认证通过后为 VPDN 用户分配一个企业内网 IP 地址。分支终端用户和总部可以开始通信。

(5) 分支网关与总部网关设备上均安装有国密板卡，通过 IPsec 协商建立起端到端的 IPsec 隧道，使用国密算法对传输的数据报文进行加密保护和数据完整性检查。

(6) 经 IPsec 加密后的数据报文在 LAC 设备处进行 L2TP 封装后，通过 L2TP 隧道传输到 LNS。

(7) LNS 收到数据报文后首先对 L2TP 报文进行解封装，然后经过 IPsec 解密还原出数据报文，根据报文目的 IP 地址转发报文。

图12 4G/5G VPDN 业务组网