行保密教育。

第二十一条　违反本规定的行为，依照《商用密码管理条例》予以处罚。

第二十二条　《商用密码产品销售许可证》由国家密码管理局印制。

第二十三条　本规定自 2006 年 1 月 1 日起施行。

27.10　商用密码产品使用管理规定

（国家密码管理局公告第 8 号，2007 年 3 月 24 日公布，自 2007 年 5 月 1 日起施行）

第一条　为了规范商用密码产品使用行为，根据《商用密码管理条例》，制定本规定。

第二条　中国公民、法人和其他组织使用商用密码产品的行为适用本规定。

第三条　本规定所称商用密码产品，是指采用密码技术对不涉及国家秘密内容的信息进行加密保护或安全认证的产品。

第四条　国家密码管理局主管全国的商用密码产品使用管理工作。

省、自治区、直辖市密码管理机构依据本规定承担有关管理工作。

第五条　中国公民、法人和其他组织需要对不涉及国家秘密内容的信息进行加密保护或安全认证的，均可以使用商用密码产品。

使用商用密码产品，应当遵守国家法律，不得损害国家利益、社会公共利益和其他公民的合法权益，不得利用商用密码产品进行违法犯罪活动。

第六条　中国公民、法人和其他组织都应当使用国家密码管理局准予销售的商用密码产品，不得使用自行研制的或境外生产的密码产品。

国家密码管理局定期公布准予销售的商用密码产品目录。

第七条　需要使用商用密码产品的，应当到商用密码产品销售许可单位购买。

购买商用密码产品应当向商用密码产品销售许可单位出示本人身份证，说明直接使用商用密码产品的用户名称（姓名）、地址（住址）以及产品用途，提供用户组织机构代码证（居民身份证）复印件。

第八条　需要维修商用密码产品的，应当交该产品的生产单位或销售单位维修。

第九条　外商投资企业（包括中外合资经营企业、中外合作经营企业、外资企业、外商投资股份有限公司等）确因业务需要，必须使用境外生产的密码产品与境外进行互联互通的，经国家密码管理局批准，可以使用境外生产的密码产品。

外商投资企业申请使用境外生产的密码产品，应当事先填写《使用境外生产的密码产品登记表》，交所在地的省、自治区、直辖市密码管理机构。

省、自治区、直辖市密码管理机构自受理申请之日起 5 个工作日内，对《使用境外生产的密码产品登记表》进行审查并报国家密码管理局。

国家密码管理局应当自省、自治区、直辖市密码管理机构受理申请之日起 20 个工作日内，对《使用境外生产的密码产品登记表》进行审核。准予使用的，发给《使用境外生产的密码产品准用证》。

《使用境外生产的密码产品准用证》有效期 3 年。

第十条　使用境外生产的密码产品的外商投资企业的名称、地址、密码产品用途发生变更的，应当自变更之日起 10 日内，到所在地的省、自治区、直辖市密码管理机构办理《使

用境外生产的密码产品准用证》更换手续。

第十一条 外商投资企业终止使用境外生产的密码产品的，应当自终止使用之日起30日内，书面告知所在地的省、自治区、直辖市密码管理机构，并交回《使用境外生产的密码产品准用证》。

第十二条 外商投资企业申请使用的密码产品需要从境外进口的，应当申请办理《密码产品进口许可证》。

密码产品入境时，外商投资企业应当向海关如实申报并提交《密码产品进口许可证》，海关凭此办理验放手续。

第十三条 用户不得转让其使用的密码产品。

第十四条 违反本规定的行为，依照《商用密码管理条例》予以处罚。

第十五条 《使用境外生产的密码产品登记表》、《使用境外生产的密码产品准用证》、《密码产品进口许可证》由国家密码管理局统一印制。

第十六条 本规定自2007年5月1日起施行。

27.11 境外组织和个人在华使用密码产品管理办法

（国家密码管理局公告第9号，2007年3月24日公布，自2007年5月1日起施行）

第一条 为了规范境外组织和个人在中国境内使用密码产品以及含有密码技术的设备（以下统称密码产品）的行为，根据《商用密码管理条例》，制定本办法。

第二条 境外组织和个人在中国境内使用密码产品的行为适用本办法。外国驻华使馆、领事机构，国际组织驻华代表机构等享有相应特权和豁免权的机构除外。

第三条 本办法所称境外组织，是指依照外国法律在中国境外成立的组织，包括这些组织在中国境内设立的分支机构、办事机构、代表机构等。

本办法所称境外个人，是指依照《中华人民共和国国籍法》不具有中国国籍的人。

本办法所称密码产品，是指采用密码技术对信息进行加密保护或安全认证的产品，包括境外生产的密码产品和中国生产的密码产品。

第四条 国家密码管理局主管境外组织和个人在中国境内使用密码产品的管理工作。

省、自治区、直辖市密码管理机构依据本办法承担有关管理工作。

第五条 境外组织或个人在中国境内使用密码产品，应当事先填写《境外组织或个人使用密码产品申报登记表》，交所在地的省、自治区、直辖市密码管理机构。

省、自治区、直辖市密码管理机构应当自受理申请之日起5个工作日内，对《境外组织或个人使用密码产品申报登记表》进行审查并报国家密码管理局。

国家密码管理局应当自省、自治区、直辖市密码管理机构受理申请之日起20个工作日内，对《境外组织或个人使用密码产品申报登记表》进行审核。准予使用的，发给《境外组织或个人使用密码产品准用证》。

《境外组织或个人使用密码产品准用证》有效期3年。

第六条 境外组织或个人使用的密码产品需要从境外进口的，应当申请办理《密码产品进口许可证》。

密码产品入境时，境外组织或个人应当向海关如实申报并提交《密码产品进口许可证》，

海关凭此办理验放手续。

第七条　境外组织或个人使用中国生产的密码产品，应当到中国商用密码产品销售许可单位购买，并出示《境外组织或个人使用密码产品准用证》。

第八条　使用密码产品的境外组织或个人的名称（姓名）、地址（住址）、密码产品用途发生变更的，应当自变更之日起 10 日内，到所在地的省、自治区、直辖市密码管理机构办理《境外组织或个人使用密码产品准用证》更换手续。

第九条　境外组织或个人终止使用密码产品的，应当自终止使用之日起 30 日内，书面告知所在地的省、自治区、直辖市密码管理机构，并交回《境外组织或个人使用密码产品准用证》。

第十条　境外组织和个人不得转让其使用的密码产品。

第十一条　境外组织和个人在中国境内使用密码产品，应当遵守中国法律，不得危害中国国家安全、损害社会公共利益、破坏社会公共秩序。

第十二条　违反本办法的行为，依照《商用密码管理条例》予以处罚。

第十三条　《境外组织或个人使用密码产品申报登记表》、《境外组织或个人使用密码产品准用证》、《密码产品进口许可证》由国家密码管理局统一印制。

第十四条　香港特别行政区、澳门特别行政区、台湾地区的组织和个人在内地使用密码产品的行为，参照本办法进行管理。

第十五条　本办法自 2007 年 5 月 1 日起施行。

第28章 国内标准

28.1 通用性标准

28.1.1 祖冲之序列密码算法（GM/T 0001）

GM/T 0001-2012《祖冲之序列密码算法》

本规范包含3个部分：算法描述、基于祖冲之算法的机密性算法、基于祖冲之算法的完整性算法。

第1部分为算法描述，描述了祖冲之序列密码算法，可用于指导祖冲之算法相关产品的研制、检测和使用。本部分主要包括算法整体结构、线性反馈移位寄存器 LFSR、比特重组 BR、非线性函数 F、密钥装入和算法运行内容，并在附录中给出了算法计算实例。

第2部分为基于祖冲之算法的机密性算法，可适用于3GPP LTE通信中的加密和解密，可用于指导基于祖冲之算法的机密性算法的相关产品的研制、检测和使用。本部分主要包括算法输入与输出和算法工作流程内容，并在附录中给出了算法计算实例。

第3部分为基于祖冲之算法的完整性算法，可适用于3GPP LTE通信中消息的完整性保护，可用于指导基于祖冲之算法的完整性算法的相关产品的研制、检测和使用。本部分主要包括算法输入与输出和算法工作流程内容，并在附录中给出了算法计算实例。

28.1.2 SM4 分组密码算法（GM/T 0002）

GM/T 0002-2012《SM4 分组密码算法》

本规范规定了SM4分组密码算法（原SMS4）的算法结构和算法描述，并给出了运算示例，适用于密码应用中使用分组密码的需求。

SM4密码算法是一个分组算法，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，数据解密和数据加密的算法结构相同，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。

本规范对轮函数F和算法进行了详细的介绍。轮函数F包括轮函数结构和合成置换T，算法描述包括加密算法、解密算法和密钥扩展算法，并在附录中给出了运算示例。

28.1.3 SM2 椭圆曲线公钥密码算法（GM/T 0003）

GM/T 0003-2012《SM2 椭圆曲线公钥密码算法》

本规范包括5个部分：总则、数字签名算法、密钥交换协议、公钥加密算法、参数定义。

第1部分为总则，给出了SM2椭圆曲线公钥密码算法涉及的必要数学基础知识与相关密码技术，以帮助实现其他各部分所规定的密码机制，适用于基域为素域和二元扩域的椭圆曲线公钥密码算法。本部分主要包括域和椭圆曲线、数据类型及其转换、椭圆曲线系统

参数及其验证、密钥对的生成、公钥的验证等内容，并在附录中给出了椭圆曲线的背景知识、数论算法、曲线示例和椭圆曲线方程参数的拟随机生成及验证。

第 2 部分为数字签名算法，规定了 SM2 椭圆曲线公钥密码算法的数字签名算法，包括数字签名生成算法和验证算法，并给出了数字签名与验证示例及其相应的流程，适用于商用密码应用中的数字签名和验证，可满足多种密码应用中的身份认证和数据完整性、真实性的安全需求。本部分主要包括数字签名算法、数字签名的生成算法及流程、数字签名的验证算法及流程等内容，并在附录中给出了数字签名与验证的示例。

第 3 部分为密钥交换协议，规定了 SM2 椭圆曲线公钥密码算法的密钥交换协议，并给出了密钥交换与验证示例及其相应的流程。适用于商用密码应用中的密钥交换，可满足通信双方经过两次或三次信息传递过程，计算获取一个由双方共同决定的共享秘密密钥（会话密钥）。本部分主要包括算法参数与辅助函数、密钥交换协议及流程等内容，并在附录中给出了密钥交换及验证示例。

第 4 部分为公钥加密算法，规定了 SM2 椭圆曲线公钥密码算法的公钥加密算法，并给出了消息加解密示例和相应的流程。适用于国家商用密码应用中的消息加解密，消息发送者可以利用接收者的公钥对消息进行加密，接收者用对应的私钥进行解密，获取消息。本部分主要包括算法参数与辅助函数、加密算法及流程、解密算法及流程等内容，并在附录中给出了消息加解密示例。

第 5 部分为参数定义，规定了 SM2 椭圆曲线公钥密码算法的曲线参数，并在附录中给出了数字签名与验证、密钥交换与验证、消息加解密示例。

28.1.4 SM3 密码杂凑算法（GM/T 0004）

GM/T 0004-2012《SM3 密码杂凑算法》

该规范规定了 SM3 密码杂凑算法的计算方法和计算步骤，并给出了运算示例，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。同时，本规范还可为安全产品生产商提供产品和技术的标准定位以及标准化的参考，提高安全产品的可信性与互操作性。

SM3 算法可概述为：对长度为 n（n < 2^64）位的消息 m，SM3 杂凑算法经过填充和迭代压缩，生成杂凑值，杂凑值长度为 256 位。本规范从算法概述、迭代演练等方式对 SM3 算法进行描述，并通过具体示例进行剖析展示。

28.1.5 SM2 密码算法使用规范（GM/T 0009）

GM/T 0009-2012《SM2 密码算法使用规范》

本规范定义了 SM2 密码算法的使用方法，以及密钥、加密与签名等数据格式。适用于 SM2 密码算法的使用，以及支持 SM2 密码算法的设备和系统的研发和检测。

本规范介绍了 SM2 公钥和私钥的数学本质。SM2 私钥是一个大于或等于 1 且小于 n−1 的整数（n 为 SM2 算法的阶，其值参见 GM/T 0003），简记为 k，长度为 256 位；SM2 公钥是 SM2 曲线上的一个点，由横坐标和纵坐标两个分量来表示，记为（x，y），简记为 Q，每个分量的长度为 256 位。