ICS 35.020
L 80

中华人民共和国国家标准

GB/T 17964—2000
idt ISO/IEC 10116:1997

信息技术　安全技术
n 位块密码算法的操作方式

Information technology—Security techniques—
Modes of operation for an n-bit block cipher

2000-01-03 发布　　2000-08-01 实施

国家质量技术监督局　发布

前　言

本标准等同采用国际标准 ISO/IEC 10116:1997《信息技术　安全技术　n 位块密码算法的操作方式》。

本标准描述 n 位块密码算法的四种操作方式，即：电子密本(ECB)方式、密码块链接(CBC)方式、密码反馈(CFB)方式和输出反馈(OFB)方式。

本标准在技术内容上与国际标准保持一致。

本标准的附录 A、附录 B、附录 C 和附录 D 均是提示的附录。

本标准由中华人民共和国信息产业部提出。

本标准由中国电子技术标准化研究所归口。

本标准起草单位：中国电子技术标准化研究所。

本标准主要起草人：罗韧鸿、向维良。

ISO/IEC 前言

ISO(国际标准化组织)和 IEC(国际电工委员会)是世界性的标准化专门机构。国家成员体(它们都是 ISO 或 IEC 的成员国)通过国际组织建立的各个技术委员会参与制定针对特定技术范围的标准。ISO 和 IEC 的各技术委员会在共同感兴趣的领域内进行合作。与 ISO 和 IEC 有联系和其他官方和非官方国际组织也可参与标准的制定工作。

对于信息技术领域,ISO 和 IEC 建立了一个联合技术委员会,即 ISO/IEC JTC1。由联合技术委员会提出的标准草案需分发给国家成员体进行表决。发布一项标准,至少需要 75%的参与表决的国家成员体投票赞成。

国际标准 ISO/IEC 10116 是 ISO/IEC JTC1“信息技术”联合技术委员会的 SC27“安全技术”分委员会制定的。

该第 2 版替代第 1 版(ISO/IEC 10116:1991)。

附录 A 至附录 D 均为提示的附录。

中华人民共和国国家标准

信息技术　安全技术
n 位块密码算法的操作方式

GB/T 17964—2000
idt ISO/IEC 10116:1997

Information technology—Security techniques—
Modes of operation for an n-bit block cipher

1　范围

本标准描述 n 位块密码算法的四种操作方式。

注：附录 A 包含了对每一种操作方式的性质的说明。

本标准确定了四种规定的操作方式，以便在 n 位块密码的应用中（例如数据传输的保护、数据存储、鉴别），本标准将对诸如操作方式规范和适用的参数值提供一个有用的参照。

2　定义

下列定义适用于本标准。

2.1　块链接　block chaining
一种信息加密方法，每一密文块在密码上依赖于前一个密文块。

2.2　密文　ciphertext
经过变换，信息内容被隐藏起来的数据。

2.3　密码同步　cryptographic synchronization
加密与解密过程的协调一致。

2.4　解密　decipherment
一个相应加密过程的逆。

2.5　加密　encipherment
为了产生密文，即隐藏数据，由密码算法对数据进行的（可逆）变换。

2.6　反馈缓存（FB）　feedback buffer (FB)
用于为加密过程存储输入数据的变量。在启动点，FB 的值为 SV。

2.7　初始化值　initialization value
用于定义一个加密过程的启动点的值。

2.8　密钥　key
控制密码变换操作（例如加密、解密）的符号序列。

2.9　n 位块密码　n-bit block cipher
明文块和密文块的长度均为 n 位的块密码。

2.10　明文　plaintext
未加密的信息。

2.11　启动变量（SV）　starting variable (SV)
确定操作方式的启动点的变量。

注：本标准未规定从初始化值导出启动变量的方法。这种方法需在操作方式的应用中描述。

国家质量技术监督局 2000-01-03 批准　　2000-08-01 实施