ICS 35.240.40
A 11

中华人民共和国国家标准

GB/T 27927—2011

银行业务和相关金融服务 三重数据加密算法操作模式 实施指南

Banking and related financial services—Triple DEA-Modes of operation—Implementation guidelines

(ISO/TR 19038:2005,MOD)

2011-12-30 发布　　2012-05-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准修改采用 ISO/TR 19038:2005《银行业务和相关金融服务　三重数据加密算法操作模式实施指南》(英文版)。

本标准根据 ISO/TR 19038:2005 重新起草,与 ISO/TR 19038:2005 的技术性差异为:

a) 将标准中的“TDEA”按照我国习惯修改为“三重数据加密算法”(在本文中简称“3-DEA”)(标准正文中部分需要区分之处保留“三重 DEA”的说法);

b) 为便于使用者理解标准正文,增加一条术语:“错误传播”(见 3.20);

c) 在 5.5 中为无编号、无标题的表编号为:表 1DEA 功能块执行时间表,以下表号顺延。

d) 在 6.6.1.1 中,将与 7.4 中 TCFB 惟一的不同之处是,反馈到移位函数的数据块是 O_i 而不是 C_i”修改为“与 6.4 中 TCFB 惟一的不同之处是,反馈到移位函数的数据块是 O_i 而不是 C_i”(勘误);

e) 为便于理解,在 B.3.2 的标题中将“stream cipher”翻译为“伪随机向量序列$\{O_i\}$”。

为便于使用,本标准还做了下列编辑性修改:

a) 将原文中的“本技术报告”改为“本标准”;

b) 删除 ISO/TR 19038:2005 的前言,修改了 ISO/TR 19038:2005 的引言。

本标准的附录 A、附录 B、附录 C 为资料性附录。

本标准由中国人民银行提出。

本标准由全国金融标准化技术委员会(SAC/TC 180)归口。

本标准负责起草单位:中国金融电子化公司。

本标准参加起草单位:中国人民银行、中国工商银行、中国银行、交通银行、中国银联股份有限公司、华北计算技术研究所、北京工商大学、中国人民银行太原中心支行。

本标准主要起草人:王平娃、陆书春、李曙光、吕毅、杨颖莉、刘运、刘志军、林中、张启瑞、刘先、仲志晖、李彦智、周亦鹏、钱湘隆、李劲松、赵志兰、贾树辉、景芸、马小琼、张龙龙。

引　言

为加强 DEA(数据加密算法)的强度和延长其生命周期,推荐使用三重数据加密算法(3-DEA)运算模式。3-DEA 的操作模式大大加强了密码保护的强度,由于这些算法基于 DEA,因此,用户和厂商可以较快熟悉它们。由于 3-DEA 操作模式能向下兼容已有的 DEA 操作模式,金融机构可使用 3-DEA 延长 DEA 的安全生命周期,保护对标准 DEA 技术的投资。

每种操作模式均有其优势和特性。对特定操作模式的选择、实施和使用取决于金融机构的安全要求、风险接受度和操作要求,这些不在本标准范围之内。如果参与方使用相同操作模式和共享保密密钥,那么本标准需要给使用本文所规定的 3-DEA 操作模式的各方提供互操作的基础根据。

本标准并不替代 DEA 算法标准和 ISO/IEC 18033 中规定的 3-DEA 算法。DEA 是 3-DEA 操作模式的基础。3-DEA 使用了先进的计算技术和密码分析技术,提供了更高的安全性。3-DEA 可用硬件、软件或软硬件混合实现。

本标准提供了 ISO/IEC 10116 中规定的操作模式的实施指南。

金融机构有责任建立全面的安全流程,其中包含必要的控制措施以确保上述过程以安全的方式实施,并且应对实施过程进行审计以确认该过程符合安全流程。

银行业务和相关金融服务
三重数据加密算法操作模式
实施指南

1 范围

本标准给用户提供了为增强数据加密保护而安全有效地实施 3-DEA 操作模式的技术支持和详细资料。本处描述的 3-DEA 操作模式用于加密运算和解密运算。本标准所描述的模式是使用 ISO/IEC 18033-3 中规定的 3-DEA 运算的分组密码操作模式(在 ISO/IEC 10116 中规定)的实现。

3-DEA 操作模式可用于金融批发业务和金融零售业务的应用系统。本标准为产品的互用性和使用 3-DEA 操作模式的应用标准的开发提供了基础。本标准将和其他使用 DEA 的 ISO 标准一起使用。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

ISO/IEC 9797-1 信息技术 安全技术 用块密码算法作密码校验函数的数据完整性机制

ISO/IEC 10116 信息技术 安全技术 n 位块密码算法的操作方式

ISO/IEC 18033-3 信息技术 安全技术 加密算法 第 3 部分:分组运算器

3 术语和定义

下列术语和定义适用于本文件。

3.1

生日现象 birthday phenomenon

一个有 n 个成员的相对较小的小组中至少两个人可能拥有共同生日的现象。

示例:当 $n=23$,该概率超过 1/2。如果一个人从 m 个可相互替代的可能数字随机地挑出一个,在 n 个实验对象中($n<m$),至少出现一对相同值的概率由以下公式估算出:

$$p=1-E^{-n^2/2m}$$

在以上实验中,试验的期望数在被发现相同值之前大约是 $(\pi m/2)^{1/2}$。其表明对于使用混合密钥的 64 比特分组加密运算,如果一个人拥有 2^{32} 明文/密文对和 2^{32} 个由随机输入产生的密文块的文本字典,那么应该认为未知密码文本块将可从该字典中搜索到(见参考文献[11])。

3.2

块;分组 block

二进制串 binary string

示例:分割成给定的长度的明文或密文,每个片断称作一个块(分组)。明文(密文)从左向右逐块加密(解密)。在本标准中,对于 TCBC、TCBC-I、TOFB 和 TOFB-I 模式,明文和密文分割成 64 比特的块,然而对于 TCFB 和 TCFB-P 模式,支持 1 位、8 位及 64 比特明文和密文块的加密和解密。