

32-33

数据库

CCED

FOXBASE

表格数据

数据交换

应用与发展

如何实现 CCED 表格数据和 FOXBASE 数据互相调用

兰州 姚华星

TP311.13

我们知道, CCED 的表格功能十分强大, FOXBASE 的数据处理能力更是有目共睹。如何实现 CCED 的表格数据和 FOXBASE 数据互相调用呢?下面为大家介绍一种方法。

一、利用 CCED 表格数据建立 FOXBASE 数据库

利用 CCED 表格数据建立 FOXBASE 数据库,不但可避免重复劳动,提高效率,而且能使已有的资料得到充分利用,不再浪费。

方法如下:

1. 在 CCED 中调出该文件,数据一律左对齐(数据类型不限),删除多余空格(以一列中最长一个数据的宽度为基准),删除表格线、表头和表尾部分。

2. 敲 F1 存盘退出,并改名为 .TXT 文件。

3. 运行 FOXBASE 建立一个空数据库结构。数据库结构中某个字段的宽度与 CCED 中某列数字宽度相对应,字符末尾空格也应计算在内。

字段宽度的计算方法为:

某字段宽度 = 末字符所在列数字 - 首字符所在列数字 + 1

4. 用 APPEND FROM <数据库名> SDF 命令,存盘后,即产生一个完整的数据库,可在 FOXBASE 下调用。

举例:

第一步:假设现有 CCED 表格如下:

学生成绩表

序号	班级	姓名	性别	语文	数学	英语	总分
1	2	伍峰	男	91.5	99.0	95.0	285.5
2	4	张玉水	女	93.5	97.0	98.0	288.5
3	6	宁坤	男	92.5	98.0	100.0	290.5
4	5	张玺	男	94.5	96.0	99.0	289.5
5	2	王霞	女	90.5	99.0	96.0	285.5
6	5	姜莉	女	89.5	100.0	97.5	287.0
7	5	陈脉沁	女	91.5	98.0	99.5	289.0
8	4	甘海萤	女	95.0	94.0	94.0	283.0
9	1	李先龙	男	90.0	99.0	98.5	287.5
10	1	蒋丽君	女	91.0	98.0	97.5	286.5

第二步:经过删除标题、多余空格、表格线、表头和表尾部分后,整理成如下形式,并改名为 YHX.TXT 存盘。

1	2	伍峰	男	91.5	99.0	95.0	285.5
2	4	张玉水	女	93.5	97.0	98.0	288.5
3	6	宁坤	男	92.5	98.0	100.0	290.5
4	5	张玺	男	94.5	96.0	99.0	289.5
5	2	王霞	女	90.5	99.0	96.0	285.5
6	5	姜莉	女	89.5	100.0	97.5	287.0
7	5	陈脉沁	女	91.5	98.0	99.5	289.0
8	4	甘海萤	女	95.0	94.0	94.0	283.0
9	1	李先龙	男	90.0	99.0	98.5	287.5
10	1	蒋丽君	女	91.0	98.0	97.5	286.5
第1列	第2列	第3列	第4列	第5列	第6列	第7列	第8列

第三步:运行 FOXBASE, 建立数据库 LS.DBF, 结构为:

序号	字符型	8
班级	字符型	6
姓名	字符型	10
性别	字符型	4
语文	数字型	8 小数点 1
数学	数字型	8 小数点 1
英语	数字型	8 小数点 1
总分	数字型	5 小数点 1

敲入指令 APPEND FROM YHX.TXT SDF, 存盘, 即产生一个名为 LS.DBF 的数据库文件。

二、利用 FOXBASE 数据库建立 CCED 表格数据

利用 CCED 的应用程序 DBST.EXE 可以方便地使 FOXBASE 数据库中数据为 CCED 表格所用,使得报表输出变得更加容易、灵活。无论多么复杂的规则或不规则报表,用户均可修改样本表格达到自己满意的要求。

方法如下:

1. 运行 DBST。

2. 根据提问逐一回答,产生参数表文件、样本文件及输出文件。

33-35

计算机

信息传输安全机

信息传输

一、引言

计算机信息传输,除满足传输信息的完整性、真实性和可仲裁性的要求外,在很多场合还有保密性的要求。国外的信息传输多采用美国的对称密码(DES)或非对称密码(RSA)所构成的公开密钥体制。但这两种体制都不尽人意。我们采用混合型密码的加密算法理论,开发研究成功一种新型信息传输安全识别机。它具有以下几个特点:

1. 安全性强。新型信息传输安全机,采用的个人识别码 PIN 可达到十进制数的 16 位,同时产生最少 144 位的加密密钥。

2. 计算速度远比美国的 DES、RSA 快得多。

3. 可仲裁性好。新型信息传输安全机独立建立一个黑匣子,一旦双方发生纠纷,黑匣子可为公证机关提供具有法律效力的数据。

4. 新型信息传输安全机采用的 PIN 可达到十进制数的 16 位,一般 32 位的 PC 机是不可能进行穷举的。同时还设置了一个防穷举陷阱,一旦有人穷举,立即进入陷阱,整个程序将破坏。

二、新型信息传输安全机的工作原理

当发送方(甲方)随机选定好 PIN(本机要求至少要 10 位以上)后,通过离散转换成大于 144 位的加密密钥 $E(K_E) = E$ 和解密密钥 $D(K_d) = D$,再用特殊指数函数密码理论,将解密密钥 $D(K_d)$ 转换成公开密钥 $H(D(K_d)) = H$ 。这样构成了双向单向函数的加密方法。第一次从 PIN 转换成 $E(K_E)$ 和 $D(K_d)$ 是一个单向函数,第二次用特殊指数函数密码理论将 $D(K_d)$ 转换成公开密钥,又是一个单向函

3. 若对输出报表不满意,可在 CCED 中调出该样本文件重新修改,直至满意后存盘,再重新用 DBST 产生输出文件。

例如,现有 FOXBASE 数据库如下形式:

序号	英文	音标	词性	中文
1	eight	[eit]	num.	八
2	me	[mi:]	pron.	我(宾格)
3	speak	[spi:k]	vt. & vi.	说,说话
4	green	[gri:n]	adj.	绿色的
5	week	[wi:k]	n.	周,星期
6	see	[si:]	vt.	看见,看到
7	goodbye	['gud'bai]	interj.	再见
8	excuse	[iks'kju:z]	vt.	原谅

第一步:运行 DBST.EXE,根据提问逐一回答,

数。对方得到公开密钥 $H = H(D(K_d))$ 后,不可能用公开密钥 H 去反推算出用户的加密密钥和个人识别码 PIN。他只能用穷举的方法破译对方的 PIN。但本识别机中设有防穷举的陷阱,只要发现有人用计算机进行穷举,机器立即停止运行,并提出警告,若再继续进行穷举,会立即破坏整个程序。

甲方用自己的个人识别码 PIN,对明文 M 进行加密成 C ,同时产生一组大于 144 位的公开密钥 H ,乙方收到甲方发来的信息 C 后,用甲方的公开密钥 H 对传输信息 C 进行解密得到明文 M 。因为乙方用甲方的公开密钥 H ,对甲方发来的加密信息 C 进行解密后得到明文 M ,证明传输来的信息 C 是从甲方发来的,其他人发来的信息,不可能用甲方的公开密钥进行解密。因为通过传输线传输的信息,全部用甲方的 PIN 产生的加密密钥进行加密的,从而保证了传输信息的完整性和真实性。但是,若乙方用自己拥有的识别机(卡)进行伪造签名,谎称这信息是从甲方发来的,这时只能靠公证机关用黑匣子中的数据进行仲裁了。

三、黑匣子的作用与管理

1. 黑匣子的作用

产生参数表文件、样本文件及输出文件。

第二步:若对输出报表不满意,在 CCED 中调出该样本文件,修改后存盘,重新运行 DBST 即产生修改后的输出文件如下。

英语单词表

序号	英文	音标	词性	中文
1	eight	[eit]	num.	八
2	me	[mi:]	pron.	我(宾格)
3	speak	[spi:k]	vt. & vi.	说,说话
4	green	[gri:n]	adj.	绿色的
5	week	[wi:k]	n.	周,星期
6	see	[si:]	vt.	看见,看到
7	goodbye	['gud'bai]	interj.	再见
8	excuse	[iks'kju:z]	vt.	原谅

TP335

