Sha1 程序逻辑流程

SHA1 分步骤演示面板(对应1.pdf)

1输入明文 -> 页面自动转换为16进制输出到2 ，点击按钮 3《填充”1”按钮》，把16进制输出为二进制并填充”1” ,输出到输出框4

点击按钮5 输出16进制到输出框6

点击按钮7 《填充长度与分组》输出 16进制到8的输出框

计算首个数据块的摘要 点击按钮9《初始化》输出五个16进制分别到 输出框 10 11 12 13 14

点击按钮15《扩充第0-15组 明文》分别输出四组数据到 16 17 18 19的输出框

点击按钮 20 《扩充第16-79组 明文》输出 16机制数到 输出框 21

点击按钮22《读取变量初始值》分别输出5组数据到 23 24 25 26 27的输出框

点击按钮28 《4轮共80步计算》 分别输出5组数据到 29 30 31 32 33的输出框

点击按钮34 《求和运算》分别输出5组数据到 35 36 37 38 39的输出框

++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++

SHA1扩展试验(对应2.pdf)

去除 5 和6的输出和描述

9 10 11 12 13 为默认的参数输出，并且所用的灰色（除《算法演示》 《运行》）

测试向量输入框 1 输入值后，点击按钮4 《运行》 信息摘要 输出框2输出结果

点击《算法演示》后 按钮《开始》可以点击

点击《开始》后，《状态表（q）》可以点击 《第一轮函数变换》可点击

点击《第一轮函数变换》可以点击 《第二轮函数变换》可点击

点击《第二轮函数变换》可以点击 《第三轮函数变换》可点击

点击《第三轮函数变换》可以点击 《第四轮函数变换》可点击

点击《第四轮函数变换》可点击 按钮 18 19 20 21 22

点击按钮 18 输出值到输出框23

点击按钮 19 输出值到输出框24

点击按钮 20 输出值到输出框25

点击按钮 21 输出值到输出框26

点击按钮 22 输出值到输出框27

++++++++++++++++++++++++++++++++++++++++++++++++++

状态表为4.Pdf 是2.pdf 《状态表（q）》的输出结果

+++++++++++++++++++++++++++++++++++++++++++++++++++

3．Pdf 是对应 2.pdf的《第 \*轮 函数变换》按钮

《第 一轮函数变换》按钮 对应3.pdf 主要为17框的范围为0-19 （初始值为0）

《第 二轮函数变换》按钮 对应3.pdf 主要为17框的范围为20-39 （初始值为20）

《第 三轮函数变换》按钮 对应3.pdf 主要为17框的范围为40-59 （初始值为40）

《第 四轮函数变换》按钮 对应3.pdf 主要为17框的范围为60-79 （初始值为60）

点击按钮1 《开始》自动填入值 2 3 4 5 6 14 16 17

点击按钮 7 自动填入值到11

点击按钮 8自动填入值到 20

点击按钮 9自动填入值到 10

点击按钮 25自动填入值到 12

点击按钮 26自动填入值到 13

点击按钮 27 自动填入值到 15

点击按钮 27 自动填入值到 15

点击按钮 28 自动填入值到 18 19 21 22 并且使 23 按钮可操作（其余的所用情况下 按键23不能操作）

点击 23 自动填入2 3 4 5 6 14 16 17（按钮17 自动加1 ，1和23 不能操作 ）

点击24按钮 自动退出3.pdf