VB编程破解Windows屏幕保护密码(1) PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/255/2021_2022_VB_E7_BC_96_E7_A8_8B_E7_A0_c67_255028.htm 大家都知道，屏幕保护密码最多为16个字符。微软内置了16字节的密钥：48 EE 76 1D 67 69 A1 1B 7A 8C 47 F8 54 95 97 5F。Windows便用上述密钥加密你输入的密码。其加密过程为：首先将你输入的密码字符逐位转换为其16进制的ASC II 码值（小写字母先转为大写字母），再依次与对应密钥逐位进行异或运算，把所得16进制值的每一位当作字符，转换为其16进制ASCII码，并在其尾加上00作为结束标志，存入注册表HKEY_CURRENT_USERControl Paneldesktop下的二进制键ScreenSave_Data中。 懂得其加密原理后，便不难编程破解我的屏幕保护密码（即上网密码）了。本人用VB6.0编制了一读取注册表中ScrrenSave_Data值的函数GetBinaryValue(Entry As String),读出其值为31 43 41 33 33 43 35 35 33 34 32 31 00,去掉其结束标志00，把余下字节转换为对应的ASCII字符，并把每两个字符组成一16进制数：1C A3 3C 55 34 21，显然，密码为6位，将其与前6字节密钥逐一异或后便得出密码的ASCII码（16进制值）：54 4D 4A 48 53 48,对应的密码明文为TMJHSH，破解成功！用它拔号一试，呵，立刻传来Modem欢快的叫声。附VB源程序：(程序中使用了窗体Form1，文本框Text1，命令按钮Command1) 窗体代码： Option Explicit Dim Cryptograph As String Dim i As Integer Dim j As Integer Dim k As Integer Dim CryptographStr(32) As Integer Dim PWstr As String Dim PassWord As String Private Sub Command1_Click() PWstr = "" PassWord =

"" Text1.Text ="" Cryptograph = GetBinaryValue("ScreenSave_Data") k = Len(Cryptograph) For j = 1 To k － 1 For i = 32 To 126 If Mid(Cryptograph, j, 1) = Chr(i) Then CryptographStr(j) = i End If Next i Next j i = (k － 1) / 2 ‘ 密码位数为(h－1)/2,根据位数选择解密过程。 Select Case i Case 16 GoTo 16 Case 15 GoTo 15 Case 14 GoTo 14 Case 13 GoTo 13 Case 12 GoTo 12 Case 11 GoTo 11 Case 10 GoTo 10 Case 9 GoTo 9 Case 8 GoTo 8 Case 7 GoTo 7 Case 6 GoTo 6 Case 5 GoTo 5 Case 4 GoTo 4 Case 3 GoTo 3 Case 2 GoTo 2 Case 1 GoTo 1 Case Else End End Select 16: PWstr = PWstr amp.H" amp. Chr(CryptographStr(32))) Xor amp. Chr(("amp. Chr(CryptographStr(29)) amp.H97) 14: PWstr = PWstr amp.H" amp. Chr(CryptographStr(28))) Xor amp. Chr(("amp. Chr(CryptographStr(25)) amp.H54) 12: PWstr = PWstr amp.H" amp. Chr(CryptographStr(24))) Xor amp. Chr(("amp. Chr(CryptographStr(21)) amp.H47) 10: PWstr = PWstr amp.H" amp. Chr(CryptographStr(20))) Xor amp. Chr(("amp. Chr(CryptographStr(17)) amp.H7A) 8: PWstr = PWstr amp.H" amp. Chr(CryptographStr(16))) Xor amp. Chr(("amp. Chr(CryptographStr(13)) amp.HA1) 6: PWstr = PWstr amp.H" amp. Chr(CryptographStr(12))) Xor amp. Chr(("amp. Chr(CryptographStr(9)) amp.H67) 4: PWstr = PWstr amp.H" amp. Chr(CryptographStr(8))) Xor amp. Chr(("amp. Chr(CryptographStr(5)) amp.H76) 2: PWstr = PWstr amp.H" amp. Chr(CryptographStr(4))) Xor amp. Chr(("amp. Chr(CryptographStr(1)) amp.H48) For i = i To 1 Step －1 ‘ 所

得PWstr的值为密码的倒序列，将其倒置便得出密码。 PassWord = PassWord &amp. Mid(PWstr, i, 1) Next i Text1.Text = PassWord ‘ 在文本框内显示密码。 End Sub 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com