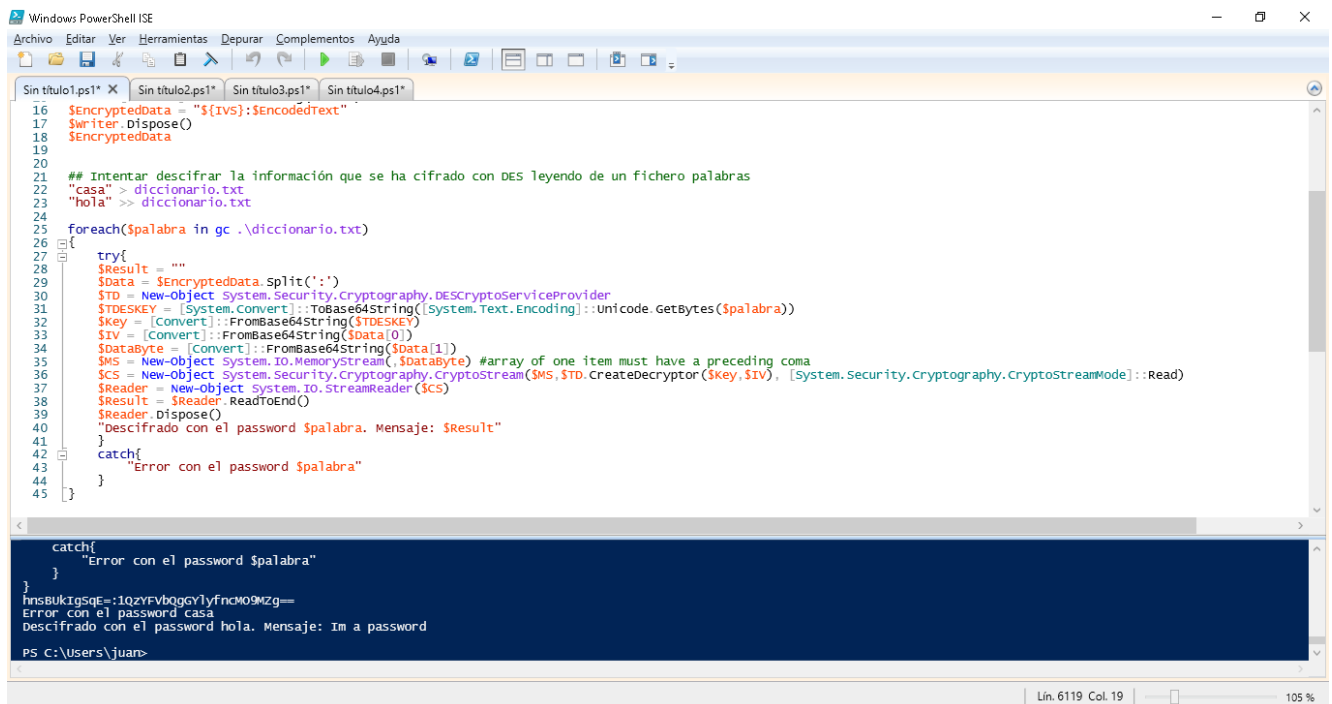


Descifrar un mensaje cifrado con DES comprobando contraseñas de un diccionario

[crayon-6a9d581b06cda271836830/]



```
Windows PowerShell ISE
Archivo Editar Ver Herramientas Depurar Complementos Ayuda

Sin titulo1.ps1* X Sin titulo2.ps1* Sin titulo3.ps1* Sin titulo4.ps1*

16 $EncryptedData = "${IVS}:$EncodedText"
17 $Writer.Dispose()
18 $EncryptedData
19
20
21 ## Intentar descifrar la información que se ha cifrado con DES leyendo de un fichero palabras
22 "casa" > diccionario.txt
23 "hola" >> diccionario.txt
24
25 foreach($palabra in gc .\diccionario.txt)
26 {
27     try{
28         $Result = ""
29         $Data = $EncryptedData.Split(':')
30         $TD = New-Object System.Security.Cryptography.DESCryptoServiceProvider
31         $TDSEKEY = [System.Convert]::ToBase64String([System.Text.Encoding]::Unicode.GetBytes($palabra))
32         $Key = [Convert]::FromBase64String($TDSEKEY)
33         $IV = [Convert]::FromBase64String($Data[0])
34         $DataByte = [Convert]::FromBase64String($Data[1]) #array of one item must have a preceding coma
35         $MS = New-Object System.IO.MemoryStream($DataByte)
36         $CS = New-Object System.Security.Cryptography.CryptoStream($MS,$TD.CreateDecryptor($Key,$IV), [System.Security.Cryptography.CryptoStreamMode]::Read)
37         $Reader = New-Object System.IO.StreamReader($CS)
38         $Result = $Reader.ReadToEnd()
39         $Reader.Dispose()
40         "descifrado con el password $palabra. Mensaje: $Result"
41     }
42     catch{
43         "Error con el password $palabra"
44     }
45 }

catch{
    "Error con el password $palabra"
}

hnsBukIgsqE=:1QzyFvbGgYlyfncM09Mzg==
Error con el password casa
Descifrado con el password hola. Mensaje: Im a password

PS C:\Users\juar>
```