

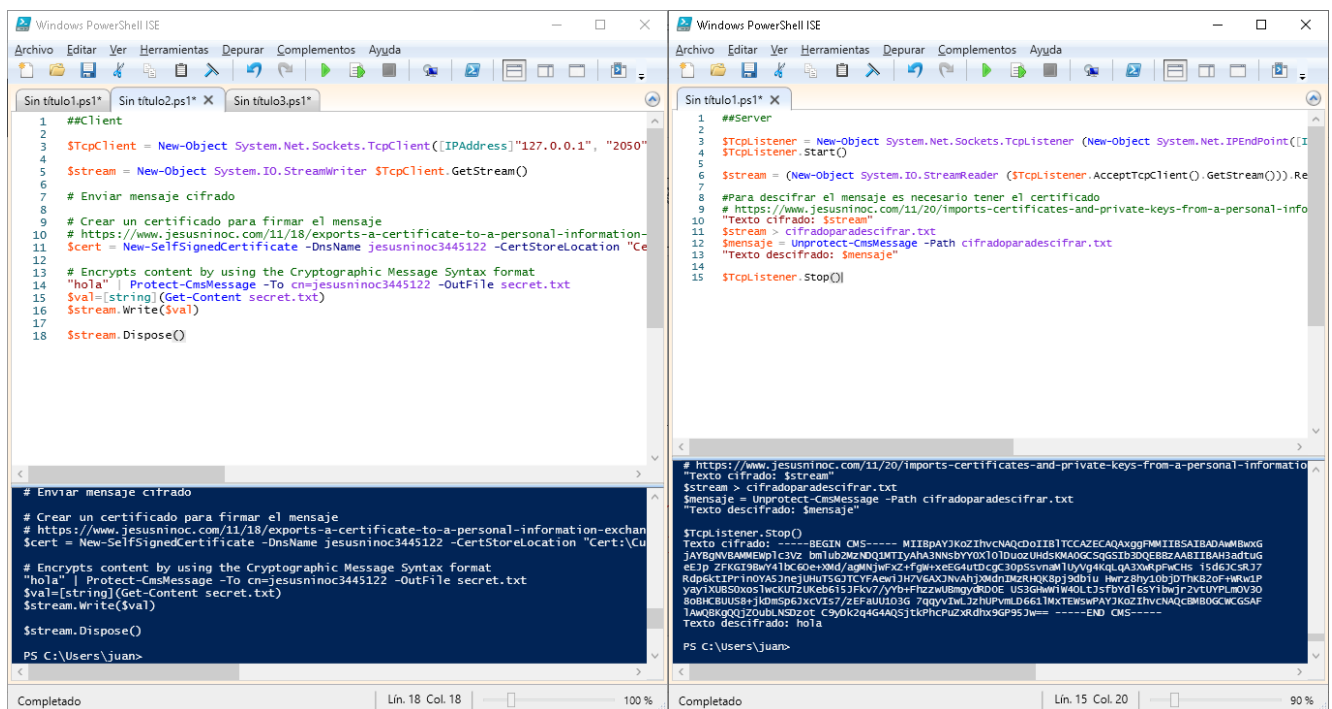
Cifrar el contenido de una comunicación por TCP en PowerShell utilizando Cryptographic Message Syntax

Servidor

[crayon-6a9d679652513063843510/]

Cliente

[crayon-6a9d679652518678761926/]



```
1 ##Client
2
3 $TcpClient = New-Object System.Net.Sockets.TcpClient([IPAddress]"127.0.0.1", "2050")
4
5 $stream = New-Object System.IO.StreamWriter $TcpClient.GetStream()
6
7 # Enviar mensaje cifrado
8
9 # Crear un certificado para firmar el mensaje
10 # https://www.jesuninoc.com/11/18/exports-a-certificate-to-a-personal-information-exchange
11 $cert = New-SelfSignedCertificate -DnsName jesuninoc3445122 -CertStoreLocation "Cert:\CurrentUser\My"
12
13 # Encrypts content by using the Cryptographic Message Syntax format
14 "hola" | Protect-CmsMessage -To cn=jesuninoc3445122 -OutFile secret.txt
15 $val=[string](Get-Content secret.txt)
16 $stream.Write($val)
17
18 $stream.Dispose()
```

```
1 ##Server
2
3 $TcpListener = New-Object System.Net.Sockets.TcpListener (New-Object System.Net.IPEndpoint([IPAddress]"127.0.0.1", "2050"))
4 $TcpListener.Start()
5
6 $stream = (New-Object System.IO.StreamReader ($TcpListener.AcceptTcpClient().GetStream())).Read()
7
8 #Para descifrar el mensaje es necesario tener el certificado
9 # https://www.jesuninoc.com/11/20/imports-certificates-and-private-keys-from-a-personal-information-exchange
10 "Texto cifrado: $stream"
11 $stream > cifradoparadescifrar.txt
12 $mensaje = Unprotect-CmsMessage -Path cifradoparadescifrar.txt
13 "Texto descifrado: $mensaje"
14
15 $TcpListener.Stop()
```

Enviar mensaje cifrado

Crear un certificado para firmar el mensaje

https://www.jesuninoc.com/11/18/exports-a-certificate-to-a-personal-information-exchange

\$cert = New-SelfSignedCertificate -DnsName jesuninoc3445122 -CertStoreLocation "Cert:\CurrentUser\My"

Encrypts content by using the Cryptographic Message Syntax format

"hola" | Protect-CmsMessage -To cn=jesuninoc3445122 -OutFile secret.txt

\$val=[string](Get-Content secret.txt)

\$stream.Write(\$val)

\$stream.Dispose()

PS C:\Users\juan>

Completado Lin. 18 Col. 18 100 %

https://www.jesuninoc.com/11/20/imports-certificates-and-private-keys-from-a-personal-information-exchange

"Texto cifrado: \$stream"

\$stream > cifradoparadescifrar.txt

\$mensaje = Unprotect-CmsMessage -Path cifradoparadescifrar.txt

"Texto descifrado: \$mensaje"

\$TcpListener.Stop()

Texto cifrado: -----BEGIN CMS----- MIIBPAYJKoZIhvcNAQcDoIIB1TCCAZCAQAggFMIIBSATBADAAMBgkqhkiG9w0BAQsR... (base64 encoded CMS data) ...-----END CMS-----

Texto descifrado: hola

PS C:\Users\juan>

Completado Lin. 15 Col. 20 90 %