Si estás tratando de conectarte mediante SSH a un router o switch Cisco que tiene un protocolo de cifrado obsoleto, te dará un error similar a este:

```
Unable to negotiate with 192.168.1.1 port 22: no matching key exchange method found.
```

Tendrás que conectarte a él indicando el uso de los protocolos de cifrado que el propio switch/router te ofrezca. Para saber los que te ofrece, mira en la parte final del mensaje, a partir de «Their offer:». Pueden ser:

```
diffie-hellman-group-exchange-sha1
diffie-hellman-group14-sha1
diffie-hellman-group1-sha1
```

Entonces, para conectarte, tendrás que ejecutar este comando:

```
ssh -oKexAlgorithms=+diffie-hellman-group1-sha1 -l NombreDeUsuarioPreviamenteConfigurado 192.168.1.1
```

Peero, no será suficiente. Te dará una salida como esta:

```
no matching cipher found. Their offer: aes128-cbc,3des-cbc,aes192-cbc,aes256-cbc
```

Esto es porque no le hemos indicado el tipo de cifrado. A juzgar por esa salida, el switch/router nos permite estos diferentes cifrados posibles:

```
aes128-cbc
3des-cbc
aes192-cbc
aes256-cbc
```

Intentaremos entonces usar el cifrado más potente de entre los cuales nos ofrece, y se lo indicamos así:

```
ssh -oKexAlgorithms=+diffie-hellman-group1-sha1 -c aes256-cbc -l NombreDeUsuarioPreviamenteConfigurado 192.168.1.1
```

Es posible que, aún indicando todos los parámetros anteriores, aún nos de un error del tipo:

```
no matching host key type found
```

Simplemente revisa que tipo de host key ofrece el servidor SSH. Seguramente sea alguna de estas:

```
ssh-rsa
ssh-dss
```

Elige la que te ofrezca y conéctate de la siguiente manera:

```
ssh -oKexAlgorithms=+diffie-hellman-group1-sha1 -c aes256-cbc -oHostKeyAlgorithms=+ssh-rsa -l
NombreDeUsuarioPreviamenteConfigurado 192.168.1.1
```