Modelo de funcionamiento de SeguriTELNET

El cliente genera un mensaje K1 y lo encripta con la llave pública del servidor

El servidor web desencripta el mensaje K1 con su propia llave privada

El servidor web genera otro mensaje K2. Posteriormente concatena K1 con K2 y los encripta con la llave pública del cliente

El cliente puede estar seguro de realizar la conexión al servidor deseado al comparar el mensaje K1. Para la sesión utiliza como llave K2

El servidor tiene la seguridad de estar conectado al cliente, pues sólo dicho cliente puede desencriptar K2 y utilizarla como llave de sesión

Computadoras Personales

El canal es encriptado utilizando K2 como llave de sesión