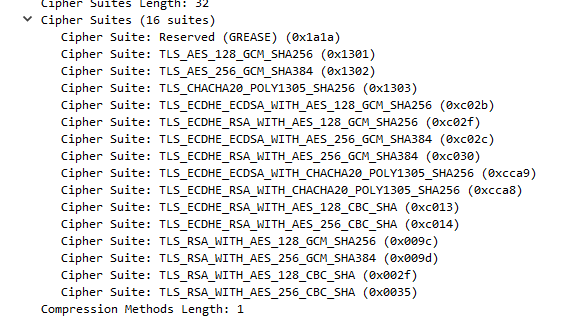
**NOMBRE:** **TURNO 2**

**1-Con la traza de “**[ConexionHTTPS\_elmundo.pcapng”](https://aulavirtual33.educa.madrid.org/ies.laarboleda.alcorcon/pluginfile.php/29598/question/questiontext/10054/2/61434/ConexionHTTPS_elmundo.pcapng)

1.1-Localiza los "cipher suites" que el cliente le ofrece, mostrando un pantallazo (1 punto).



1.2-Localiza la "cipher suit" que usa elmundo.es para realizar los cifrados, mostrando un pantallazo (1 punto).

1-Nombra y explica los pasos de [DHCP](https://aulavirtual33.educa.madrid.org/ies.laarboleda.alcorcon/mod/assign/view.php?id=27051) (1 punto)

disscover=manda un mensaje de broadcast con su direccion MAC preguntando quien es el DHCP

offer=El DHCP le responde al ordenador con un IP disponible, tambien le mandasu informacion.

renew=el Cliente responde al resvidor directamente por que ya sabe su MAC e IP y le dice que coge esa IP

=El servidor le da el OK

2-Explica el protocolo OSPF. (1 punto)

Es un protocolo de enrutamiento utilizado de manera masiva, es decir que es mas comun verlo en redes muy amplias. Recoge la informacion de la tabla de enrutamiento y se la manda al reto de routers. Para que todos sepan llegar a todos

3-Explica BPSK, QAM-16 y QAM-64 (1 punto)

4-Nombra las frecuencias utilizadas en 4G (1 punto)

5-¿Qué es Diffie-Hellman? (1 punto)

es un metodo de cifrado el cual mediante un complejo resultado matematico, determina cual es la clave. La clave se genera mediente unas claves publicas, de las cuales mezcla 2 (estan las claves A,B,C,D y la clave para descifrar la informacion seria= ac la mezcla de las claves ‘A’y ‘C’)

6-¿Qué es SHA-256? (1 punto)

Es un metodo de encriptacion de los datos en el cual se cifran con la clave publica de B y despues con otro metodo de encriptacion el cual solo saben el emisor y el receptor, por lo tanto el receptor lo descifra con el metodo qu eambos saben y despues con su clave privada.

7-¿Que es RSA? (1 punto)

Es un cifrado asimetrico que usa una clave privada y una publica, si cifro con la clave publica de B el la descifra con su clave privada y si cifro con mi clave privada y con su clave publica nos aseguramos que solo yo lo he enviado y que solo el lo pueda abrir.

8-Con la red 192.168.1.128/24 hacemos 3 subredes. ¿Cuál es la primera IP válida de la última subred? (1 punto)

2^3-2=6

192.168.1.00000000

192.168.1.11100000/27

|  |  |
| --- | --- |
| Primera IP valida | Ultima IP valida |
| 192.168.1.65 | 192.168.1.94 |