1. Autrum Transfer Protocol (ATP), es un protocolo creado durante los años 90 para el envío de mensaje (este utilizaba el puerto TCP/666), este se volvió muy popular entre las personas jóvenes de la época que tenían acceso a una red, este protocolo era capaz de transportar cualquier carácter visible ASCII, parte de lo emocionante de este protocolo era lograr enviar los mensajes de forma cifrada y el proceso era enteramente manual, lo cual quiere decir que las personas involucradas en la transmisión conocían las llaves para cifrar y descifrar mensajes. ATP se ha puesto de moda en el 2022, el problema es que ATP es un protocolo sumamente débil en términos de seguridad y además usa un puerto poco convencional como lo es TCP/666, con el fin de evaluar sí es posible implementar una versión segura de este protocolo, se le solicita responder las siguientes preguntas:

a. ¿Es posible enviar datos que no sean HTTPs sobre el puerto 443? Justifique su respuesta. (10 pts)

Sí, encriptado datos con una llave pública se pueden enviar datos que no sean https.

b. Suponiendo que creamos el protocolo ATP over SSL (ATPs), describa un subprotocolo para el establecimiento de una conexión SSL. (40 pts)

SSL crea una conexión segura y cifrada entre un navegador y un servidor, y protege la capa de comunicación entre ambos, por lo que este subprotocolo utilizaría algoritmos de cifrado para establecer la conexión de una manera segura. Cuando un dispositivo se conecte con el servidor este subprotocolo genera 2 claves de cifrado para la comunicación, son claves que funcionan como claves de sesión y como encriptadoras.

c. Si existe el protocolo ATPs, ¿Es posible transportar ATPs sobre HTTPs? Justifique su respuesta. (10 pts)

Sí, se pueden encriptar con una llave pública los datos ATPs para poder enviarlos sobre HTTPs.

d. Desde un punto de vista de firewalls, ¿Porqué sería muy conveniente usar el puerto TCP/80 en lugar de puerto TCP/666?.

Al ser para envío de mensaje de caracteres ASCII se puede ver como un texto sin formato y el puerto 80 es seguro para este tipo de datos, mientras que el puerto TPC/666 solo garantiza la llegada de los datos en orden.

2. Explique detalladamente el funcionamiento de RSA. (30 pts)

El cifrado RSA tiene una clave pública a la que se puede acceder libremente y de una clave privada, que solo debe conocer una persona. El cifrado se realiza con la clave pública. Pero para descifrar se necesita la clave privada.

- Para generar las claves se utiliza 2 números primos(p y q).
- Con estos tenemos n, n = p x q y z (p - 1) x (q - 1).
- Seleccionar un número primo con respecto a z, llamándolo d.
- Encontrar e tal que e x d = 1 mod z.

Con esto se tiene la clave pública consiste en el par (e, n), y la clave privada consiste en (d, n). Con esto se dividen los datos que se van a encriptar en bloques.