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, no existe una limitación técnica que limite el enviar datos distintos a HTTP's por el puerto 443, existen estándares que recomiendan cómo se deberían usar los puertos pero es más una convención que una regla inquebrantable.

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

Una vez realizado el handshake, el servidor y el cliente pueden comunicarse por texto plano lo cual no tiene ningún nivel de seguridad por lo que se necesita realizar el protocolo SSL handshake para establecer una conexión que cuente con seguridad. Se inicia con un intercambio entre el cliente y el servidor, el cliente envía un Client Hello al servidor con el IP y el puerto que se obtuvo en el handshake inicial. El servidor verifica la información(versión del protocolo, el Id de la session, la lista de Cipher Suites soportados por el cliente) proporcionada mediante el Client Hello y responde con un Server Hello con distinta información(el cipher suites elegido, ID sesion y otros bytes random) y el certificado digital del servidor sin la llave privada. El cliente verifica el certificado con una lista de lo que debe aprobar para ser válido y el servidor envía una solicitud del certificado del cliente, el cliente le envía el certificado encriptado el servidor verifica el certificado y ambos se intercambian un mensaje de finalizado. Para posteriormente iniciar a intercambiar mensajes encriptados usando las llaves de sesión creadas.

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

Sí, ya que no hay limitantes a la hora de enviar caracteres ASCII por HTTPs, lo que sucederá es que se estaría cifrando al ATPs por la seguridad del HTTPs y al llegar al destino se desencripta primero el HTTPs y posteriormente si se tiene la llave el ATP.

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

Es muy conveniente usar el puerto TCP/80 ya que es un puerto estandar por lo que la mayoría de firewalls espera que le lleguen peticiones por ese puerto y por lo general no se le ponen reglas de bloqueo al TCP/80, todo lo contrario a el puerto 666 que aunque no existe una limitante para usarlo no es tan común como el 80 por lo que podrían existir reglas que lo bloqueen fácilmente y solo dejen el paso de peticiones como el 80 o 443.

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

Es un método que se basa en los principios de la teoría de los números, se deben calcular los siguientes parámetros primero

1. Seleccionar dos números primos grandes, p y q (generalmente de 1024 bits).
2. Calcular n = p X q y z = (p - 1) X (q - 1).
3. Seleccionar un número primo con respecto a z, llamándolo d. 4. Encontrar e tal que e X d = 1 mod z.

Una vez hecho eso se divide el texto llano (una cadena de bits) en bloques, para que cada mensaje de texto llano, P, caiga en el intervalo $0 \leq P < n$. Esto puede hacerse agrupando el texto llano en bloques de k bits, donde k es el entero más grande para el que $2k < n$ es verdadero. Para encriptar un mensaje, P, se calcula $C = Pe \pmod{n}$. Para desencriptar C, se calcula $P = Cd \pmod{n}$. Para ejecutar la encriptación, se necesitan e y n. Para llevar a cabo la desencriptación, se requieren d y n. Por lo que la clave pública consiste en el par (e, n), y la clave privada consiste en (d, n).