**RELACIÓN DE EJERCICIOS**

**EJERCICIO 1:**

Especificar (de manera formal) la fase de “sesión” de TLS (v1.2), considerando la existencia de dos nodos, uno funcionando como cliente (A) y el otro como servidor (B):

1. **A 🡪 B: Client Hello**
2. **B🡪 A: Server Hello**
3. **A🡪 B: ClientKeExchange, ChangeCipherSpec**
4. **B 🡪A: ServerKeyExchange, ChangeCipherSpec**

Una vez definida la fase de sesión, completar el protocolo de TLS (v1.2) para contemplar el envío seguro por la fase de “conexión”, de forma que A le envía a B el siguiente mensaje: “*Hola servidor B, te envío este secreto por TLSv1.2*”.

5.A🡪B: Ek(M)

**EJERCICIO 2:**

Especificar (de manera formal) la fase de “sesión” de TLS (v1.3), considerando la existencia de dos nodos, uno funcionando como cliente (A) y el otro como servidor (B):

1. **A 🡪 B: ClientHello, ClientKeyExchange**
2. **B🡪 A: ServerHello, ServerKeyExchange, ChangeCipherSpec**
3. **A🡪A: ChangeCipherSpec**

Una vez definida la fase de sesión, completar el protocolo de TLS (v1.2) para contemplar el envío seguro por la fase de “conexión”, de forma que A le envía a B el siguiente mensaje: “*Hola servidor B, te envío este secreto por TLSv1.3*”.

5.A🡪B: Ek(M)

**EJERCICIO 3:**

Considerando que A (el cliente) y B (el servidor) usan TLSv1.2, especificar de manera formal el protocolo de intercambio de clave establecido entre A y B, bajo las siguientes condiciones iniciales:

* A y B deciden negociar la clave de sesión de forma que el cliente (A) envía cifrado con RSA el *pre-shared master key*, y
* A no sabe de antemano la clave pública.

La formalización seguiría el siguiente formato:

1. **A 🡪 B: ClientHello**
2. **B🡪A:ServerHello:(Kpub, Nb)**
3. **B🡪A: ClientKeyExchange: (Epub(pre-shared master key), Na)**

Realizar el mismo ejercicio, pero en lugar de usar RSA, aplicar DH.

A🡪B: Na

B🡪A:G, N, Yb, EprivB(G, N, Yb, Nb)

A🡪B:Ya

**EJERCICIO 4:**

Considerando que A (el cliente) y B (el servidor) usan TLSv1.2, especificar de manera formal el protocolo de intercambio de clave establecido entre A y B, bajo las siguientes condiciones iniciales:

* A y B deciden negociar la clave de sesión con DHE firmado con RSA, y
* A no sabe de antemano la clave pública.

La formalización seguiría el siguiente formato:

1. **A 🡪 B: …**
2. **…**

**EJERCICIO 5:**

Accediendo a la siguiente URL:

* <https://www.rfc-editor.org/rfc/rfc8446#page-133>

Contestar (con vuestras palabras y haciendo siempre referencias a otras fuentes si procede) a las siguientes preguntas:

1. ¿Qué significa y aborda el RFC 8446? ¿Y quién lo ha definido?
2. ¿Con qué puertos de la capa de transporte trabaja la versión 1.3 de TLS?
3. ¿En qué consiste el método o el modo 0-RRT?
4. ¿La versión de TLSv1.2 incluye la opción de 0-RRT?
5. Destacar la/s ventaja/s y la/s desventaja/s que conlleva el uso del modo 0-RRT.
6. ¿Crees que los algoritmos de curva elípticas están contemplados dentro de TLSv1.3?
7. Analizar y describir cada elemento que contiene los siguientes “*cipher suites*”:
   * TLS\_AES\_128\_GCM\_SHA256 = {0x13,0x01}
   * TLS\_AES\_256\_GCM\_SHA384 = {0x13,0x02}
   * TLS\_AES\_128\_CCM\_8\_SHA256 = {0x13,0x05}
8. Analizar el flujo de información definido en la página 119 del RFC-8446 y correspondiente al flujo gestionado por el nodo cliente, y, por otro lado, analizar también el flujo de información definido en la página 120 gestionado por el servidor.

**EJERCICIO 6:**

Accediendo a las siguientes URL:

* <https://datatracker.ietf.org/doc/rfc9308/>
* <https://datatracker.ietf.org/doc/rfc9114/>

Analizar y describir (con vuestras palabras y haciendo siempre referencias a otras fuentes si procede) en qué consiste el protocolo QUIC. Para ello, hay que contestar a las siguientes preguntas:

1. ¿Qué significa las siglas de QUIC? ¿Quién fue su desarrollador?
2. ¿Qué objetivo tiene el documento RFC 9308? ¿Y quién lo ha definido?
3. ¿Con qué puertos de la capa de transporte trabaja QUIC?
4. ¿En qué se diferencia con el protocolo de TLS-v1.3 y cuál sería su relación?
5. Investiga y razona si el protocolo QUIC es realmente seguro.
6. ¿En qué se diferencia QUIC con DTLS?

**EJERCICIO 7:**

Es importante conocer el ecosistema que conforma el mundo de la ciberseguridad, y saber las labores fundamentales de algunas organizaciones nacionales. Para ello, contestar a las siguientes preguntas:

1. ¿Qué es INCIBE[[1]](#footnote-1) y cuáles son sus objetivos?
2. Dentro de INCIBE se encuentra el INCIBE-CERT[[2]](#footnote-2), ¿en qué consiste y cuáles son sus objetivos principales?
3. Analizar la siguiente entrada de INCIBE-CERT:
   * “[*Múltiples vulnerabilidades en OpenSSL*](https://www.incibe-cert.es/alerta-temprana/avisos-seguridad/multiples-vulnerabilidades-openssl-3)”:
   * <https://www.incibe-cert.es/alerta-temprana/avisos-seguridad/multiples-vulnerabilidades-openssl-3>
4. ¿Crees que hay otras vulnerabilidades relacionadas con TLS? ¿Dónde estarían publicados dentro de INCIBE-CERT?
5. ¿Crees que hay otras organizaciones (nacionales o internacionales) con repositorios oficiales que publican vulnerabilidades similares? Si es así, nombra al menos un par de ellos.

**EJERCICIO 8:**

Considerando el artículo “*Raccoon Attack: Finding and Exploiting Most-Significant-Bit-Oracles in TLS-DH(E)*” disponible en: <https://raccoon-attack.com/RacoonAttack.pdf>. Contestar a las siguientes preguntas:

1. ¿En qué consiste el ataque *Raccoon*?
2. ¿A qué versión (o versiones) de TLS afecta?
3. ¿Crees que hay más ataques al protocolo TLS? Si es así, nombrar y describir (con vuestras palabras) al menos un ataque (sin olvidar de incluir las correspondientes referencias).

1. INCIBE: <https://www.incibe.es> [↑](#footnote-ref-1)
2. INCIBE-CERT: <https://www.incibe-cert.es> [↑](#footnote-ref-2)