Tema 2 – Técnicas criptográficas básicas Criptografía simétrica y asimétrica

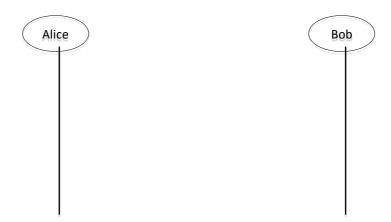


RELACIÓN DE EJERCICIOS

EJERCICIO 1:

Definir el protocolo de comunicación entre Alice y Bob, de forma que Alice envíe un mensaje M a Bob de manera segura usando criptografía híbrida (es decir, que haya SOLO confidencialidad).

Precondición: Alice y Bob no han establecido comunicación previamente.

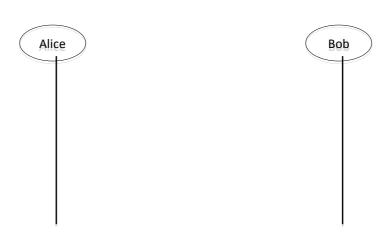


- 1. Definir el problema asumiendo que se aplica RSA para el intercambio de claves.
- 2. Volver a definir el problema aplicando DH para el intercambio de claves.

EJERCICIO 2:

Definir el protocolo de comunicación entre Alice y Bob, de forma que Alice envíe un mensaje M (de 2GB) a Bob de forma segura usando criptografía híbrida (es decir, que haya confidencialidad), pero esta vez aplicando firma digital para permitir a Bob verificar el origen real de los datos recibidos y su integridad.

Precondición: Alice y Bob no han establecido comunicación previamente.

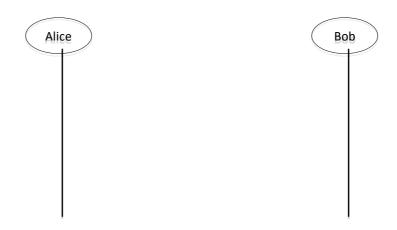


Tema 2 – Técnicas criptográficas básicas Criptografía simétrica y asimétrica



EJERCICIO 3:

Definir el protocolo de comunicación entre Alice y Bob, de forma que Alice envíe un mensaje M (de 2GB) a Bob de forma segura (es decir, que haya confidencialidad), pero esta vez aplicando MAC para permitir a Bob a verificar el origen real de los datos recibidos y su integridad. Precondición: Alice y Bob no han establecido comunicación previamente.



EJERCICIO 4:

Teniendo en cuenta el siguiente protocolo:

- 1. $T \rightarrow A$: $E_{KAT}\{B, K_{AB}, E_{KBT}\{C, K_{AB}, K_{BC}, E_{KCT}\{C, K_{BC}\}\}\}$ -- suponemos que A ya tiene la clave K_{AB} de una transacción previa
- 2. A \rightarrow B: E_{KBT}{C, K_{AB}, K_{BC}, E_{KCT}{C, K_{BC}}}
- 3. $B \rightarrow C$: $E_{KCT}\{C, K_{BC}\}$
- 4. $\mathbf{B} \rightarrow \mathbf{A}$: \mathbf{E}_{KAB} {"hola $\mathbf{ID} = A$ "}
- 5. $B \rightarrow C$: $E_{KCT}\{C, K_{BC}\}$
- 6. $C \rightarrow B$: E_{KBC} {"hola ID=B"}

y que T tiene compartido una clase secreta K_{CT} con C, K_{BT} con B y una clave K_{AT} con A, analizar el protocolo, contestando a las siguientes preguntas:

- 1. ¿Qué hace A cuándo recibe el mensaje de T (punto 1 y punto 2)?
- 2. ¿Qué hace B cuándo recibe el mensaje de A (punto 3, punto 4 y punto 5)
- 3. ¿Qué tipo de criptografía se está aplicando en este protocolo?
- 4. ¿Hay autenticación en los puntos 2, 3, 4, 5 y 6? Razonar la respuesta.

Tema 2 – Técnicas criptográficas básicas Criptografía simétrica y asimétrica



EJERCICIO 5:

Analizar el siguiente protocolo:

- 1. $T \rightarrow A: T, A, E_{KpubA}\{T, B, K_{AB}\}, E_{privT}\{H\{T, B, K_{AB}\}\}$
- 2. $A \rightarrow B$: A, B, E_{KAB} {"Estamos aprendiendo critpografía aplicada"}

contestando a las siguientes preguntas:

- 1. ¿Qué hace A cuando recibe el mensaje de T?
- 2. ¿Qué tipo de criptografía se está aplicando en este protocolo?
- 3. ¿Quién genera la clave de sesión?
- 4. ¿T se autentica a A? Razonar la respuesta.
- 5. ¿A se autentica con respecto a B? Razonar la respuesta.
- 6. ¿Crees que hay un coste de computación elevado en el punto 1?

EJERCICIO 6:

Teniendo en cuenta el siguiente protocolo:

A → B: B, "Hola B", MAC(____)
B → A: A, "Hola A", MAC(____)

contestando a las siguientes preguntas:

- 1. ¿Es necesario que A y B tengan una clave de sesión previamente acordada?
- 2. ¿Qué hace B cuando recibe el mensaje de A (punto 1)? Razonar la respuesta.
- 3. ¿Qué hace A cuando recibe el mensaje de B (punto 2)? Razonar la respuesta.
- 4. ¿Qué servicio de seguridad se está aplicando?
- 5. Rediseña el protocolo para que, en vez de usar una MAC, usen firma digital.

EJERCICIO 7:

Teniendo en cuenta el siguiente protocolo:

1. $A \rightarrow B$: B, "Hola B", MAC_{KAB}(B, "Hola B") – situación normal

Supongamos que un Man-in-the-Middle (MitM = Mallory) intercepta el canal de comunicación y modifica el mensaje "Hola B" justo en el punto 1, tal que:

1. $A \rightarrow Mallory \rightarrow B$: B, "Adios B", $MAC_{KAB}(B, "Hola B")$

Tema 2 – Técnicas criptográficas básicas Criptografía simétrica y asimétrica



Contestar a las siguientes preguntas:

- 1. ¿Qué hace B cuando recibe el mensaje de A (del protocolo alterado por Mallory)?
- 2. ¿Qué servicio de seguridad se está aplicando?
- 3. ¿Crees el MitM pueda rehacer el MAC (del punto 2 y 3)? Razonar la respuesta.
- 4. ¿Cómo se resolvería el problema del MitM en el protocolo de arriba?