GUÍA 4: MANEJO DE CLAVES – CIFRADO ASIMÉTRICO – FIRMA DIGITAL

En los ejercicios de esta guía, considerar:

- K_{sx} es clave privada de x; K_{px} es clave pública de x;
- E_x es encripción con clave pública de x;
- D_x es desencripción con clave privada de x;
- S_x es firma con clave privada de x;
- V_x es verificación con clave pública de x;
- K_{xy} o K_s es clave de sesión compartida entre x e y;
- $\{M\}_{KS}$ es encripción de M con clave simétrica KS
- Mallory efectúa ataques activos y Eve efectúa ataques pasivos.

Ejercicio 1:

Escribe un ejemplo de los siguientes ataques que pueden darse contra un protocolo. ¿Pueden evitarse?

1) Replay
2) Key Reuse
3) Man in the middle
4) Masquerading (suplantación de identidades)

Ejercicio 2:

Considera el siguiente protocolo para enviar un texto plano M entre A y B:

1) $A \rightarrow B: \{ K_{pA} \}$
2) $B \rightarrow A: \{ K_{pB} \}$
3) $A \rightarrow B: \{ E_B(M) \}$
4) $B \rightarrow A: \{ E_A(M) \}$

Si un adversario (Z) intercepta el primer mensaje, ¿cómo hace para obtener el texto plano M?

Ejercicio 3:

¿Cuál es el problema con el siguiente protocolo? Solucionarlo.

1) $A \rightarrow B: S_A\{N1, K_s\}$
2) $B \rightarrow A: \{N1 + 1\}_{Ks}$

Ejercicio 4:

Considera el siguiente protocolo de autenticación mutua en el cual A y B se autentican mutuamente intercambiando 4 mensajes:

1) $A \rightarrow B: N1$
2) $B \rightarrow A: N2$
3) $A \rightarrow B: (N2)_{Ks}$
4) $B \rightarrow A: (N1)_{Ks}$

Donde:

- N1 y N2 son números generados en forma aleatoria (nonce)

- A y B son los ID de las partes intervinientes

- Ks es una clave simétrica ya compartida entre A y B

A autentica con éxito a B al recibir el cuarto mensaje y B autentica con éxito a A al recibir el tercer mensaje. Como Ks es una clave ya compartida entre A y B solamente, cualquiera que encripte un mensaje usando Ks se asegura que posee K y por lo tanto queda autenticado.

¿Qué situación *NO* debe permitir A para evitar que un tercero no autorizado se autentique correctamente?

Ejercicio 5:

En el protocolo original de Needham Schroeder, cuando se roban claves de sesión es posible un ataque de replay.

La siguiente es una variante del protocolo de Needham Schroeder:

1. Alice → Bob: Alice
2. Bob →Alice: $\{ \text{Alice}, \text{rand}_X \}_{KBT}$
3. Alice → Trent: $\{ \text{Alice}, \text{Bob}, \text{rand}_A, \{ \text{Alice}, \text{rand}_X \}_{KBT} \}$
4. Trent → Alice: $\{ \text{Alice}, \text{Bob}, \text{rand}_A, k_{session}, \{ \text{Alice}, \text{rand}_X, k_{session} \}_{KTB} \}_{KAT}$
5. Alice → Bob: $\{ \text{Alice}, \text{rand}_X, k_{session} \}_{KTB}$
6. Bob →Alice: $\{ \text{rand}_B \}_{Ks}$
7. Alice → Bob: $\{ \text{rand}_B - 1 \}_{Ks}$

Mostrar que con esta variante se resuelve el problema de ataque de repetición.

Ejercicio 6:

Considera el protocolo de intercambio de claves Diffie Hellman y escribe la secuencia de pasos para que en lugar de ser 2 los participantes que generan una clave compartida sean 3.

Ejercicio 7:

Considera un protocolo normal de intercambio de claves Diffie – Hellman con autenticación. El objetivo es proveer autenticación mutua con intercambio de claves. Asumimos que cada parte tiene una clave privada para firmar en algún esquema de firma y un certificado con la correspondiente clave pública. El protocolo procede de la siguiente manera:

1) A→B: g^x
2) B→A: $\{B, certB, S_B(g^x, g^y), g^y\}$
3) A→B: $\{A, certA, S_A(g^x, g^y) \}$

Finalmente, Alice y Bob pueden calcular la clave compartida y secreta $K = g^{xy}$.

a) Explicar el por qué de las firmas en el protocolo anterior.

b) Mostrar que un atacante activo, Mallory, puede interferir con el protocolo mediante un ataque **man in the middle** tal que al final tendremos la siguiente situación:

- Alice cree que se está comunicando de forma segura con Bob
- Pero Bob cree que se está comunicando de forma segura con Mallory

Ejercicio 8:

En este problema se comparan los servicios que provee la firma digital y los códigos de autenticación de mensajes (MAC).

Se asume que Oscar puede observar los mensajes que Alice y Bob se envían, pero no conoce ninguna clave, salvo las públicas.

GUÍA 4: MANEJO DE CLAVES – CIFRADO ASIMÉTRICO – FIRMA DIGITAL

Determinar si el ataque se puede detectar o proteger con la Firma Digital, con el código de autenticación MAC, con ambos o con ninguno. Clasificar el tipo de ataque (man in the middle, replay, message integrity, cheating, etc.)

a) Alice envía un mensaje ***x*** = *"Trasferir $1000 a Mark"* en plano y también envía *sign(x)* a Bob. Oscar intercepta el mensaje y reemplaza "*Mark"* con "*Oscar"*. ¿Puede Bob detectar esto?

b) Alice envía un mensaje ***x*** = *"Trasferir $1000 a Oscar"* en plano y también envía *sign(x)* a Bob. Oscar observa el mensaje y la firma y lo reenvía 100 veces a Bob. ¿Puede Bob detectar esto?

c) Oscar afirma que él envió un mensaje x con firma válida *sign(x)* a Bob. Alice afirma que fue ella. ¿Puede Bob dirimir la cuestión?

d) Bob dice que recibió un mensaje ***x*** = *"Trasferir $1000 de Alice a Bob"* con firma válida *sign(x)* de parte de Alice. Pero Alice dice que ella nunca mandó eso. ¿Puede Alice aclarar su situación?

Ejercicio 9:

El siguiente protocolo usa criptografía de clave pública. Trent tiene una base de datos con todas las claves públicas de los participantes.

1) A→T: {A, B}
2) T→A: {S_T(B, K_{pB}), S_T (A, K_{pA})}
3) A→B: {E_B(S_A(K_s,time$_A$)), S_T(B, K_{pB}), S_T (A, K_{pA})}

a) Explicar qué hace Bob después del paso 3 para ratificar que puede comunicarse con Alice con seguridad.

b) Explicar cómo hace Bob para impersonarse como Alice frente a Carol (masquerading)