# *GUÍA 4: MANEJO DE CLAVES – CIFRADO ASIMÉTRICO – FIRMA DIGITAL – SOLUCIONES*

**Ejercicio 1:**

**Ataques**

1. **de replay.**

El intruso (o tramposo) repite o dilata información maliciosa o fraudulenta.

1) Alice envía a Bob un cheque digital firmado por ella para que él cobre $100.
2) Bob (tramposo) lo reenvía al banco más de una vez. El banco siempre certifica que está autorizado, y Bob le saca toda la plata a Alice.

Solución: timestamps.

2. **Key reuse.**

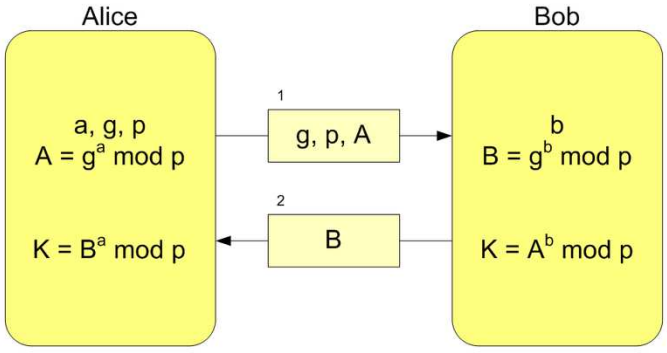
Como las claves de sesión se generan en forma seudoaleatoria, es posible predecir las claves de sesión y reusarlas.

1) En Needham Shroeder, si Mallory obtiene una clave de sesión anterior, y viene guardando los mensajes de Alice a Bob, puede enviarle a Bob un mensaje viejo $E_B(K,A)$ . Bob extrae K y verifica que es de "Alice". Luego sigue el protocolo y genera un número aleatorio $R_B$ , el cual encripta con la clave de sesión K. Envía eso a Alice: $E_K(R_B)$ . Mallory intercepta este mensaje, y ella (en lugar de Alice) envía a Bob: $E_K(R_B-1)$ . Bob se convence que se está comunicando con Alice, pero sigue la comunicación con Mallory.

Solución: timestamps. Buenos métodos de generación de claves aleatorias.

3. **Man in the middle**

El intruso actúa **sobre los dos canales** de comunicación (hacia A y hacia B). En general es también un "masquerading"




$K = A^b \bmod p = (g^a \bmod p)^b \bmod p = g^{ab} \bmod p = (g^b \bmod p)^a \bmod p = B^a \bmod p$

- Diffie Hellman.
- Alice envía el generador (g), el valor del número primo (p) y $g^a \bmod p$ .
- Mallory intercepta el mensaje de Alice, y no puede hallar $a$ . Pero puede, con el generador y el número primo generar un nuevo número $g^m \bmod p$ y enviarselo a Bob. Bob cree que es Alice, entonces sigue el protocolo enviándole $B=g^b \bmod p$ , a la vez que calcula $K=(g^m)^b \bmod p$ como clave de sesión.
- Mallory, le hace algo parecido a Alice, por lo que queda generada una clave con Alice y otra con Bob. Luego Alice usará esa clave para encriptar sus mensajes a Bob (pero en realidad se estará comunicando con Mallory) y Bob usará otra clave para encriptar mensajes a Alice (pero en realidad sólo se comunica con Mallory que se entera de todo.)

4. **Masquerading**

Una persona o programa se hace pasar por otra falsificando datos. Ej. Diffie Hellman, Spoofing, suplantación de identidad.

Un man in the middle es, habitualmente un masquerading. Pero un masquerading no necesariamente es un man in the middle.

# *GUÍA 4: MANEJO DE CLAVES – CIFRADO ASIMÉTRICO – FIRMA DIGITAL – SOLUCIONES*

**Ejercicio 2:**

Si Z intercepta los últimos mensajes, no puede desencriptar M porque debería tener la clave privada de B. Pero puede hacer un **man in the middle** de la siguiente manera:

1) Captura la clave pública de A y se la guarda.

$$A \rightarrow Z: \{ K_{UA} \}$$

2) Le pasa a B la clave pública suya.

$$Z \rightarrow B: \{ K_{UZ} \}$$

3) B le pasa a Z su clave pública, creyendo que se la pasa a A.

$$B \rightarrow Z: \{ K_{UB} \}$$

4) Z se queda con la $K_{UB}$ y le envía a A la clave pública suya.

$$Z \rightarrow A: \{ K_{UZ} \}$$

5) Así, Z tiene el control de la comunicación, porque tanto A como B encriptarán sus mensajes con $K_{UZ}$ y sólo Z los puede desencriptar con su clave privada y, si lo desea, reenviar al otro con modificaciones.

$$A \rightarrow B(Z): \{ E_Z(M)\}$$
$$A(Z) \rightarrow B: \{ E_B(M')\}$$
$$B \rightarrow A(Z): \{ E_Z(R)\}$$
$$B(Z) \rightarrow A: \{ E_A(R')\}$$

**Ejercicio 3:**

Cualquiera puede obtener, con la clave pública de A, el N1 y el Ks. Puede servir para garantizar identidad. Entonces habría que combinar encripción con firma:

1) Alice firma el mensaje con su clave privada y lo encripta con la clave pública de Bob:

$$A \rightarrow B: E_B\{S_A\{N1, K_s\}\}$$

2) Sólo Bob, con su privada, puede obtener $S_A\{N1, K_s\}$
3) Bob, con la clave pública de Alice obtiene $\{N1, K_s\}$. Sabe que sólo Alice lo pudo armar. El protocolo continúa igual.

$$B \rightarrow A: \{N1 + 1\}_{Ks}$$

**Ejercicio 4:**

A no debería permitir que Z envíe el mismo nonce, porque cualquiera se autenticaría correctamente reenviando el mismo mensaje.

**Ejercicio 5:**

Recordamos Needham y Schroeder:

1. **Alice → Trent: $\{A, B, rand_A\}$**

Alice inicia la comunicación con Trent.

2. **Trent →Alice: $\{rand_A, B, K_{Sesion}, \{A, K_{Sesion}\}_{KBT}\}_{KAT}$**

Trent genera una clave de sesión para las comunicaciones entre Alice y Bob.

Alice cuando recibe el mensaje, con $K_{AT}$ efectúa la desencripción de lo que Trent le envió y obtiene:

$rand_A$ →que le confirma que este mensaje se corresponde con el 1.

B

$K_{Sesion}$ -→ para sus futuros mensajes con Bob.

$\{A, K_{Sesion}\}_{KBT}$ -→ mensaje que le reenviará a Bob y que Alice no puede abrir.

3. **Alice → Bob : $\{A, K_{Sesion}\}_{KBT}$**

Bob recibe el mensaje de Alice, y con la clave $K_{BT}$ (sólo conocida por él y Trent) lo abre obteniendo A y $K_{sesion}$.

4. **Bob →Alice: $\{ rand_B\}_{Ksesion}$**

Alice recibe el mensaje y lo puede abrir porque la clave de sesión es la que ella también obtuvo de Trent.

5. **Alice → Bob: $\{ rand_B - 1 \}_{Ksesion}$**

Bob recibe el mensaje y lo puede abrir y confirma $rand_B$.

**Ataque:**

Si Mallory consigue tener acceso a claves de sesión vieja ($K_{sesion}$), puede hacer lo siguiente:

1. Mallory(en nombre de Alice) → Bob: $\{ Alice, k_{session}\}_{KTB}$

Mallory le envió a Bob un mensaje viejo de los que interceptó entre Alice y Bob.

Bob lo recibe, y con la clave que comparte con Trent, lo abre y le envía a Mallory (creyendo que es Alice:

2. Bob → Mallory (en nombre de Alice):$\{rand_B\}K_{sesion}$

Como Mallory ve que puede desencriptar ese mensaje porque consiguió esa clave de sesión, entonces puede generar $rand_B$ -1 y engañar a Bob.

3. Mallory(en nombre de Alice) → Bob: $\{ rand_B -1 \}_{Ksesion}$

Bob confirma $rand_B$ -1

Como Bob no inició el protocolo, no tiene manera de darse cuenta que el primer mensaje que Mallory le envió ($\{ Alice, k_{session}\}_{KTB}$) es en realidad un mensaje viejo. ( Bob aparece en escena recién en el paso 3 del protocolo)

En esta nueva versión:

1. **No están hechos los pasos 1 y 2.**

Asumimos que Mallory pudo obtener, de intercambios anteriores, $K_S$ y los mensajes intercambiados.

Entonces efectúa una repetición del mensaje 5:

Mallory(en nombre de Alice) → Bob: $\{ Alice, rand_X, k_{session}\}_{KTB}$

Cuando Bob recibe eso, si él mismo no envió recientemente el mensaje 2, (Bob→Alice: $\{ Alice, rand_X\}_{KBT}$)entonces se da cuenta que el mensaje que le acaba de llegar es falso. Lo rechaza.

Si él había enviado recientemente un mensaje 2, como el que le envía Mallory es anterior, seguramente **$rand_X$** y **$rand_X$** no coinciden, por lo tanto también lo rechaza.

2. **Están hechos los pasos 1 y 2.**

# *GUÍA 4: MANEJO DE CLAVES – CIFRADO ASIMÉTRICO – FIRMA DIGITAL – SOLUCIONES*

Mallory envía su mensaje después de que Alice comenzó el protocolo.
Es decir:

1) A→B: A
2) B→A: $\{ A, rand_X \}_{KBT}$
3) A → Trent : { A, B, $rand_A$, $\{ A, rand_X \}_{KBT}$ }
4) Trent → A: { A, B, $rand_A$, $k_{session}$, $\{ A, rand_X, k_{session} \}_{KTB}$ }$_{KAT}$

Este mensaje, M no lo puede abrir porque no tiene $k_{AT}$.
Por lo tanto, a Bob le envía un mensaje viejo:

5) M(en nombre de A) → B: $\{ A, rand_X, k_{session} \}_{KTB}$

Bob abre el mensaje, y ve que $rand_x$ no coincide con $rand_x$, por lo tanto no continua el protocolo.

Otra opción es que Mallory empiece el protocolo como si fuera Alice.
Es decir:

1) Mallory ( en nombre de A)→B: A
2) B→M (en nombre de A) : $\{ A, rand_X \}_{KBT}$
3) M saltea los pasos 3 y 4, y efectúa directamente el paso 5,

M(en nombre de A) → B: $\{ A, rand_X, k_{session} \}_{KTB}$

Pero como también lo tuvo que hacer con un mensaje viejo, nuevamente Bob abre el mensaje, y ve que $rand_x$ no coincide con $rand_x$.

### Ejercicio 6: Group Diffie Hellman

Conocidos (g, p) los pasos serían::

1. $A \rightarrow B : g^x \bmod p = X$
2. $B \rightarrow C : g^y \bmod p = Y$
3. $C \rightarrow A : g^z \bmod p = Z$
4. $A \rightarrow B : \left(g^z\right)^x \bmod p = Z'$
5. $B \rightarrow C : \left(g^x\right)^y \bmod p = X'$
6. $C \rightarrow A : \left(g^y\right)^z \bmod p = Y'$

Después de esto, A, B y C tienen todos la clave k:

$\left(g^{yz}\right)^x \bmod p = k \quad = \quad \left(g^{xz}\right)^y \bmod p = k \quad = \quad \left(g^{xy}\right)^z \bmod p = k$

### Ejercicio 7: Universidad de Saarland

a) Las firmas garantizan que fue Alice quien envió $g^x$ y que fue Bob quien envió $g^y$.
b) Eso podría ocurrir si:

1. A→B(pero lo captura M): $g^x$
2. M → B: $g^x$
3. B→M: {B, certB, $S_B(g^x,g^y)$,$g^y$}
4. M(en nombre de B) →A: {B, certB, $S_B(g^x,g^y)$,$g^y$}
5. A→B(pero lo captura M): {A, certA, $S_A(g^x,g^y)$ }
6. M→B: {M, certM, $S_M(g^x,g^y)$ }

La firma que hace M es posible porque pudo ver en plano los valores $g^x$ y $g^y$ en los pasos 1 y 3.

### Ejercicio 8:

MAC: es una función de hash de una sola via con el agregado de una clave secreta.
El que tiene la clave puede verificar el valor de hash.
Firma: es una encripción con una clave privada, que puede desencriptarse con una clave pública.

1. Puede Bob detectarlo con MAC o con firma. Es message integrity.
2. Es replay. Bob no puede detectarlo ni con MAC ni con firma.
3. Es un caso cheating. Se puede detectar con firma ya que sólo podrá desencriptarse con la pública del que lo hizo. Con MAC, tanto Oscar como Alice deberán revelar su clave privada para verificar el valor de hash y mostrar que es x.

# *GUÍA 4: MANEJO DE CLAVES – CIFRADO ASIMÉTRICO – FIRMA DIGITAL – SOLUCIONES*

**4.** Es un caso de trampa (Bob is cheating). Con firma digital, Alice tiene que forzar a Bob a probar su reclamo enviándole una copia del mensaje y otra de la firma. Si Alice puede mostrar que se puede verificar con la clave pública de Bob, entonces fue Bob mismo el que envió el mensaje. Con MAC, no es posible verificar nada ya que Bob puede decir que él no sabe cómo se encriptó porque no tiene la clave con la que se hizo.

**Ejercicio 9:**

a) Tras el paso:

$\{E_B(S_A(K_s,time_A)), S_T(B, K_{UB}), S_T (A, K_{UA})\}$

Bob con su privada obtiene $S_A(K_s,time_A)$. Con la publica de Trent obtiene la clave pública de Alice que le permite verificar $S_A(K_s,time_A)$ y obtener la clave de sesión. A su vez, el valor timeA le sirve para detectar replay.

b) Bob puede hacer lo siguiente, una vez que completó el protocolo con Alice:

1. B → T: {B,C}
2. T → B: $\{S_T(B, K_{UB}), S_T (C, K_{UC})\}$
3. B(como alice)→C: $\{E_C(S_A(K_s,time_A)), S_T(C, K_{UC}), S_T (A, K_{UA})\}$

Carol se convence que está hablando con Alice.