Criptografía Asimétrica

I. Conceptos Básicos

La criptografía Asimétrica, conocida también como criptografía de dos claves o criptografía de clave pública, es aquella en la cual el método criptográfico utilizado consta de un par de claves que serán usadas en el tratamiento de los mensajes. Dichas claves pertenecen al autor del mensaje siendo la de tipo pública, aquella que se puede entregar a cualquier otra persona, mientras que la otra de tipo ”privada”será de uso exclusivo para el dueño, quién deberá evitar, bajo cualquier circunstancia, compartirla.

El funcionamiento de este metodo va de la siguiente manera:

- El remitente usa la clave pública del destinatario para cifrar el mensaje.
- Usando la clave privada, el destinatario podrá descifrar el mensaje.
- De la misma manera, el propietario podrá cifrar mensajes para que aquellos que dispongan de la clave pública puedan descifrarlo.
- De esta manera se garantiza la confindencialidad del mensaje ya que nadie, salvo el destinatario, puede descifrarlo.

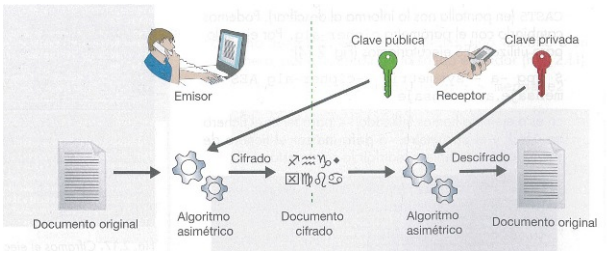

Figura 1. Esquema de la Criptografía Asimétrica

I-A. *Ventajas de la Criptografía Asimetrica*

- Una las ventajas mas resaltantes es la facilidad y seguridad con la que las llaves publicas se pueden distribuir.
- No existe el desbordamiento en el tratamiento de claves y canales.
- Otra ventaja en menor medida, es que a pesar de que en el trasfondo de la Criptografía Asimetrica exista un algoritmo capaz de generar claves, es casi imposible que dos personas obtengan la misma pareja de claves.

I-B. *Desventajas de la Criptografía Asimétrica*

- Para generar una clave de la misma longitud se necesita mayor tiempo de proceso.(Supone un problema de lentitud)
- Es muy probable que este sistema falle si las claves son muchos menores que las simetricas.
- El mensaje cifrado ocupa un espacio mayor al mensaje original.
- Generalmente el uso continuo de las claves privadas conlleva a recibir ataque criptográficos con sistemas capaces de analizar paquetes cifrados (Caso Sony diciembre 2010).
- Es necesario proteger la clave privada. Generalmente esto se hace almacenando todas las llaves privadas dentro de un archivo privado ”llavero”que estará protegido con cifrado simétrico.
- Hay que transportar la claves privadas, suponieno el riesgo mismo de extraviar el llavero

II. Diffie-Hellman

El protocolo de cifrado Diffie-Hellman (recibe el nombre de sus creadores) es un sistema de intercambio de claves entre partes, que no han contactado previamente, a través de un canal inseguro y sin autenticación. Este protocolo se utiliza principalmente para intercambiar claves simétricas de forma segura para posteriormente pasar a utilizar un cifrado simétrico, menos costoso que el asimétrico. Se parte de la idea de que dos interlocutores pueden generar de forma conjunta una clave sin que esta sea comprometida.

II-A. *Funcionamiento*

1. Se escoge un número primo p y un generador g, siendo este último coprimo de p. Ambos números son públicos.
2. Escogemos un número a menor que p, en este caso a, y calculamos:

   $$A = g^a modp$$

   Enviamos A, p y g al otro interlocutor.
3. El otro interlocutor escoge un numero b menor que p y calcula:

   $$B = g^b modp$$

   Retornandonos B.
4. Ahora, ambos podemos calcular:

   $$K = g^(a - b) modp$$

   Siendo para nosotros $B^a modp = K$ y para nuestro interlocutor $A^b modp = K$. Usamos K como clave.
5. Al ser p y g públicos cualquier atacante puede llegar a conocerlos, esto no supone una vulnerabilidad. Aunque capturase A y B, le resultaría computacionalmente imposible obtener a y b con la consecuencia de tampoco acceder a K.

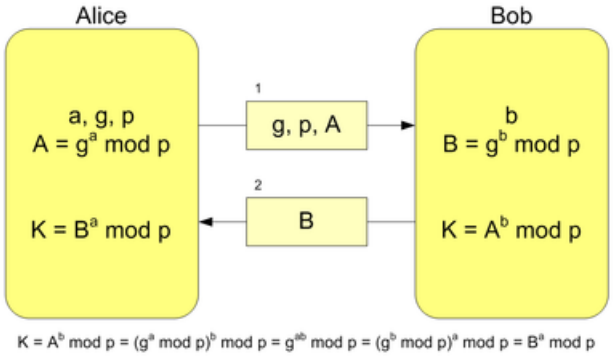

Figura 2. Funcionamiento del sistema Diffie-Hellman

II-B. Vulnerabilidades

Este protocolo es vulnerable al ataque ”man in the middle”; el cual consiste en que un tercero se coloca en el medio del canal y hace creer a ambos que es el otro. De esta forma se podría acordar una clave con cada parte y servir de .[en]lace.[en]tre los dos participantes. Para que este ataque sea funcional se necesita saber que método de cifrado simétrico se va a emplear. Ocultar el algoritmo de cifrado no cumple con el principio de Kerkckhoffs de que la efectividad de un sistema no debe depender de que su diseño permanezca en secreto por lo que conocer el sistema que se va a emplear se hace trivial.

Para evitar esto se puede emplear un protocolo de autenticación de las partes mediante por ejemplo TLS(Transport Layer Security).

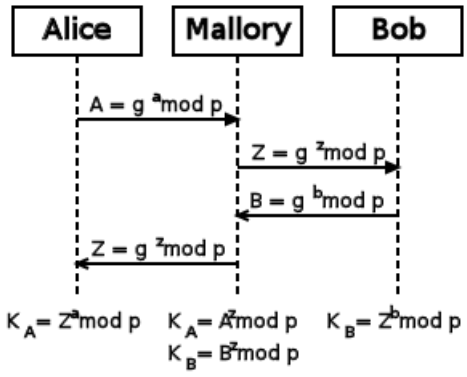

Figura 3. Esquema de la intrusión Man-in-the-middle