María Julieta Comparan Velasco

Tópicos de Seguridad Web

Tarea 3.2: Cifrado simétrico y asimétrico

14/11/21

Cifrado simétrico y asimétrico

Tarea 3.2

Recordatorio: La criptografía mantiene seguro un mensaje por medio de la codificación de los mismos, para hacerlos de una forma en la que no se puedan leer, así, solamente lo ve la persona que el emisor quiera. Existe una terminología para todos estos procesos:

El mensaje original se llama **texto claro**

El mensaje codificado se llama **texto cifrado**

El proceso de convertir el texto claro en texto cifrado se llama **cifrado**

El proceso de recuperar el texto a partir del texto cifrado se llama **descifrado**

Las aplicaciones criptográficas necesitan generar claves para asegurar el candado de aquello que se quiera cifrar, una clave es como una llave física que se usa como para abrir o cerrar una puerta, y para cada tipo de cerradura digamos que existe una llave con la forma específica que se ajusta a esa cerradura, o por decirlo así, se ajusta con cierta longitud determinada capaz de girar y abrir tal cerradura.

O sea qué… cada algoritmo criptográfico necesita una clave con una extensión correcta (número correcto de bits). Claro que se puede hacer procesamiento con cualquier clave que tenga una longitud digamos ‘’apropiada’’, pero solo la que tenga el patrón correcto de bits hará que el algoritmo descifre la información cifrada.

Entonces en pocas palabras, el cifrar ayuda a garantizar confidencialidad, autenticación e integridad, y este cifrado se clasifica en simétrico y asimétrico.

Criptografía simétrica.

La criptografía simétrica usa **la misma clave** para **cifrar** y **descifrar** el mensaje de datos, o sea que se basa en un ‘’secreto compartido’’. Por eso la seguridad de este proceso depende de la posibilidad de que una persona no autorizada pueda conseguir la clave de sesión o la clave secreta.

Cifrado simétrico y asimétrico

Tarea 3.2

Los algoritmos criptográficos simétricos tienen dos versiones: **cifrador en bloque** y **cifrador en flujo**. Aquí una cifra es una palabra para describir un algoritmo de cifrado. Los cifradores en bloque codifican datos en bloques pequeños de longitud fija de 64 bits de longitud. Hay muchos **cifradores** en bloque que incluyen **DES**, **3-DES**, **RC2**, **RC5**, **RC6** y Rijndael (**AES**) que son algoritmos simétricos de cifrado.

Por ejemplo, **DES** es un algoritmo simétrico cuyas abreviaturas significa ‘’Estándar de cifrado de datos’’ y es un cifrador de bloque de 64 bits de longitud, donde en primer lugar se cifra el texto en claro, a continuación del resultado, se vuelve a cifrar, lo que da lugar a que el texto claro se cifre en 3 ocasiones, y el resultado es un cifrado grande de 192 bits, y un ejemplo de descifrado para estos casos puede ser una clave de 2192 posibles valores, aclarando, para una de 192 bits.

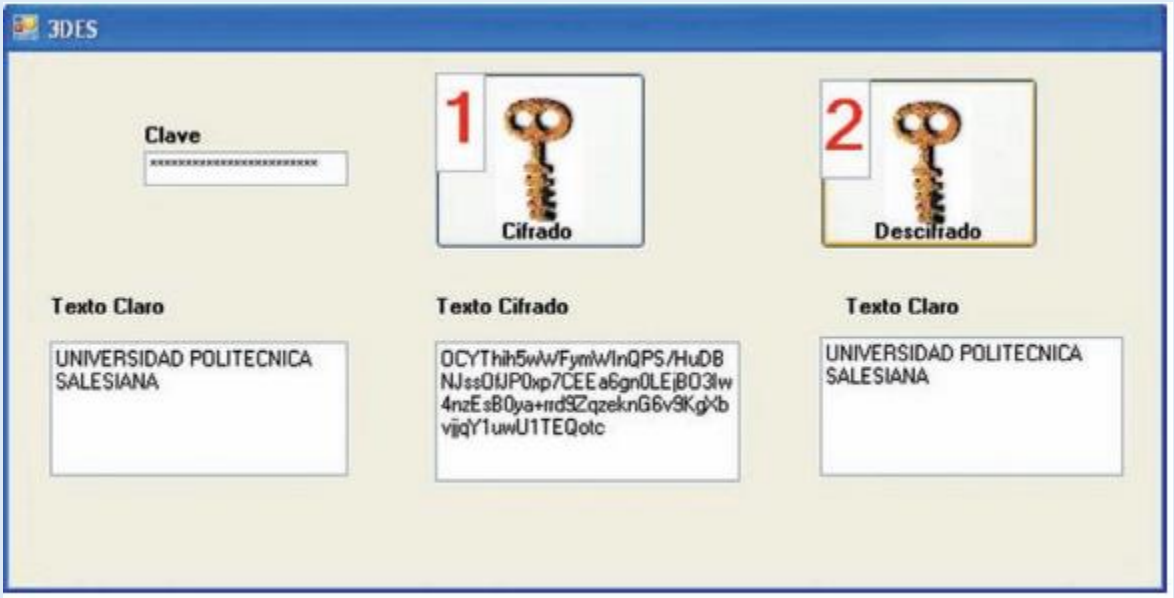

Figura A1. Cifrado Simétrico

Criptografía asimétrica.

Los algoritmos asimétricos son diferentes a los simétricos, cuando se genera una clave simétrica, se escoge un número aleatorio de la longitud apropiada, pero al generar claves asimétricas el proceso es más difícil. Aquí los algoritmos asimétricos se llaman asimétricos porque en lugar de usar una sola clave para realizar la codificación y la

codificación, se utilizan **dos claves** diferentes, una para **cifrar** y otra para **descifrar,** estas dos claves se asocian matemáticamente, y su característica más importante es que una clave no puede descifrar lo que cifra.

Cuando se completa la generación de una clave asimétrica se define una clave de cifrado (**clave pública**) y una clave de descifrado (**clave privada**), la primera puede ser conocida por todo el mundo, pero, se debe tener cuidado en ocultar la clave privada.

Las claves asimétricas entonces tienen una propiedad ‘’sorprendente’’ de que lo que se está cifrando con una clave solo se puede descifrar con la otra. Existen algunos algoritmos asimétricos para esto, como Diffie-Hellman, que se basa en logaritmos discretos, o el RSA que es un algoritmo de uso común.

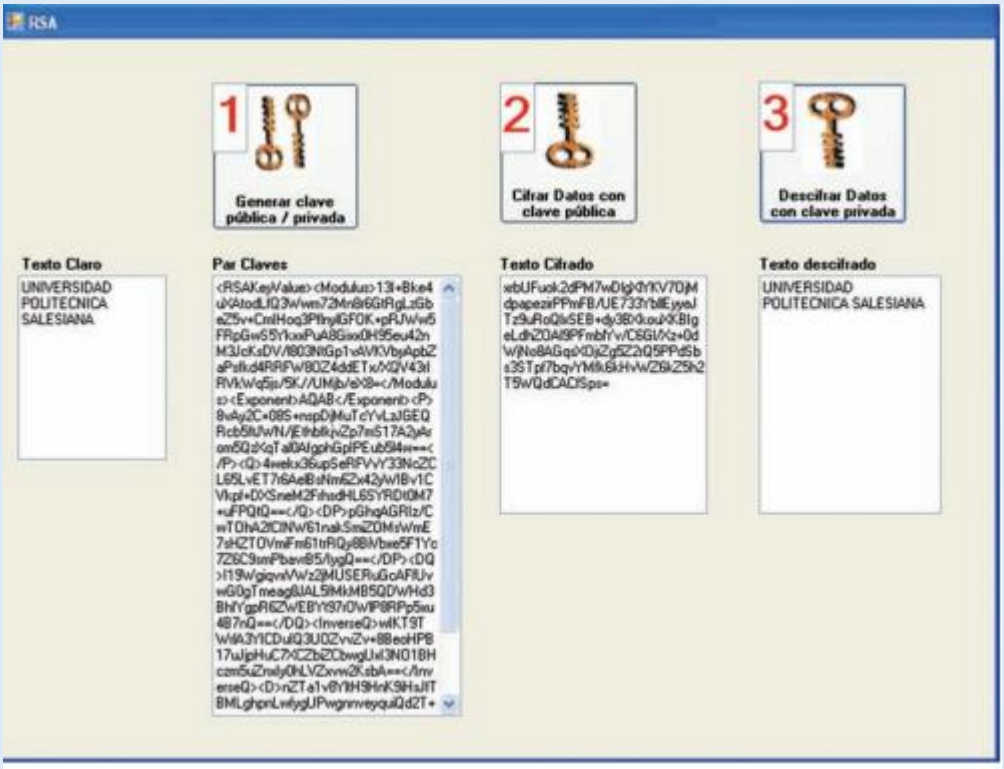

Figura A2. Cifrado Asimétrico

Conclusiones: El cifrado simétrico es más eficaz en lo que concierne a almacenamiento de información sensible en una base de datos, un registro o un archivo, pero, el cifrado asimétrico se usa frecuentemente también para pasar con seguridad una clave privada que luego se utilizará para cifrar o descifrar otra información, lo único malo de utilizar la criptografía asimétrica es que esta es lenta e intensa.

Fuentes bibliográficas:

[1]Nash Andrew, Infraestructura de Claves públicas, Ed. McGraw Hill, México 2004.

[2]http://www.rsa.com/node.aspx?id=29 72145

[3]De Jemas, .NET Framework Ed. McGraw Hill, México 2004.