Práctica: Criptografía Híbrida

La criptografía moderna, creada a partir de 1948 con la Teoría de la Información de Claude Shannon, se divide en simétrica y asimétrica, una de las principales diferencias, es que en esta última se utiliza la clave pública del destinatario del mensaje para cifrar el mensaje y el destinatario usa su clave privada para descifrarlo. Otra de las diferencias, es que la criptografía asimétrica puede proveer autenticidad, con lo que el destinatario puede corroborar la identidad del remitente. Sin embargo, se limita la cantidad de información a cifrar a diferencia de la criptografía simétrica que permite procesar información de cualquier tamaño ya que trabaja por bloques o por flujo, lamentablemente se presentan los problemas de distribución y almacenamiento de la llave.

No se puede decir cuál es mejor que otra, habrá que identificar claramente que servicios se pueden ofrecer con cada una de ellas y es posible mezclarlas para resolver los problemas que presentan de forma individual.

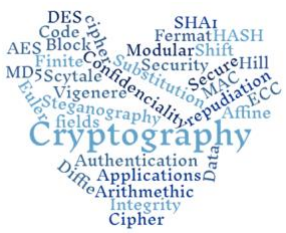
Algunos de los principales servicios criptográficos requeridos son

- Confidencialidad: protege la información ante revelaciones no autorizadas.
- Autenticación: verifica que un nodo o un usuario sea quien dice ser.
- Integridad: protege los datos del sistema ante modificaciones o alteraciones no deseadas.
- No repudio: impide que un emisor niegue haber enviado un mensaje o que un receptor niegue haberlo recibido.

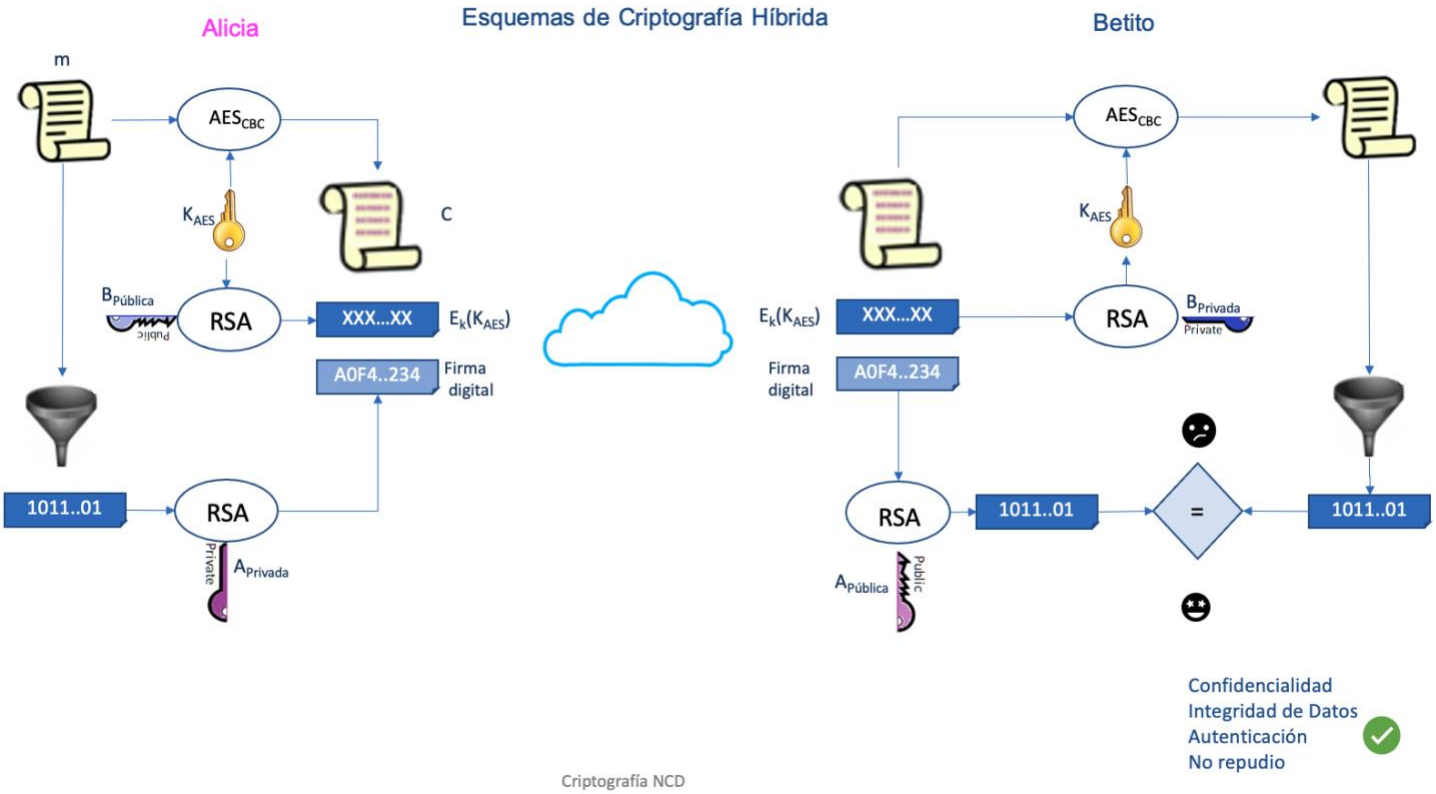
Los algoritmos de criptografía simétrica ofrecen confidencialidad para archivos de cualquier tamaño, el uso de las funciones hash brinda integridad de la información y si se complementa con criptografía asimétrica se puede ofrecer autenticación y no repudio.

En la figura 1 se muestra un escenario haciendo uso de algoritmos criptográficos simétricos y asimétricos que permite ofrecer desde uno hasta todos los servicios anteriormente descritos.

Deadline: 26 enero 21 7:00 am



M. en C. Nidia A. Cortez Duarte



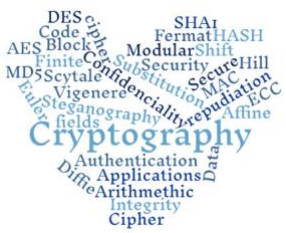
1 Esquema Criptografía Híbrida

Por parejas implementar este escenario de Criptografía Híbrido haciendo uso de las prácticas anteriormente utilizadas.E

En su interfaz se debe ofrecer un menú que permita

- Cifrado/Descifrado
- Firma/ Verificación

El usuario será capaz de seleccionar el proceso requerido de acuerdo a los servicios que necesite ofrecer. Uno de dos o dos de dos.



M. en C. Nidia A. Cortez Duarte

Cifrado/Descifrado

Se ofrece CONFIDENCIALIDAD

Proceso de Cifrado

1) Primero se genera una llave aleatoria de 16 bytes (transparente para el usuario).

2) A continuación se cifra el contenido del archivo con AES-128 usando la llave generada previamente.

3) A continuación, dicha llave se cifra con RSA y la llave pública del destinatario.

4) Finalmente ambos cifrados forman el mensaje que se va a transmitir.

Proceso de Descifrado

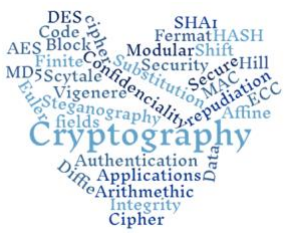
1) Aquí, lo primero que hay que hacer es conseguir la llave del AES y descifrarla con RSA usando la llave privada del receptor

3) Finalmente, el contenido del archivo se descifra usando esta llave para el AES

Firma/Verificación

Proceso de Firma (describir)

Proceso de Verificación (describir)



M. en C. Nidia A. Cortez Duarte

Pruebas que deben incluir en su video.

A) Generar un par de llaves para Candy
B) Mostrar el sistema y seleccionar ambas opciones
   Alicia mostrará su escritorio mientras va describiendo todo el proceso de cifrado y firma, especificando los servicios que se van ofreciendo en cada paso que realice. Betito mostrará su escritorio para describir todo el proceso de descifrado y verificación especificando los servicios que se van ofreciendo en cada paso que realice. (En este punto, todo funciona bien)
C) Hacer que falle el servicio de Confidencialidad y corregir para que vuelva a funcionar [lo hace Betito]
D) Hacer que falle el servicio de Integridad y corregir para que vuelva a funcionar [Lo hace Betito]
E) Hacer que falle el servicio de Autenticación (para esto hacer usurpación con las llaves de Candy) [esto lo hace el mismo alumno que está representando a Alicia]. Betito verifica, deberá fallar (se debe mostrar alguna excepción y no que el programa simplemente truene) Betito intenta verificar con las llave de Candy y ahí descubre que realmente era un mensaje de Candy.
F) Finalmente cada uno dice sus conclusiones individuales.

Durante el video es importante que se muestre el escritorio así como el video de los dos integrantes del equipo. Uno explicando y el otro muy atento ☺

Para esta práctica se evaluará tanto el funcionamiento a detalle de lo solicitado así como la explicación de todos los algoritmos y servicios criptográficos implementados, es decir, vale el doble ;)

M. en C. Nidia A. Cortez Duarte