INSTITUTO POLITÉCNICO NACIONAL

ESCUELA SUPERIOR DE CÓMPUTO

# 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.

Practica final

Construir un escenario con todo lo que vimos durante el semestre que ofrezca: confidencialidad, autenticación, integridad y no repudio.

Incluir:

1. Portada (con el sello correspondiente) en donde se visualice claramente el nombre de todos los integrantes
2. Su propio escenario (previo VoBo.) elaborado a computadora
3. Tabla de servicios (con las referencias)
4. Justificación de los algoritmos, tamaño de llave y modo de operación.
5. Asperctos especiales de la programación y/o consideraciones especiales para ejecución.
6. Lenguaje de programación, bibliotecas utilizadas.
7. Ya tienen la tabla de cada algoritmo utilizado y la seguridad que ofrece en bits, ¿cuál será entonces la seguridad de TODA esta práctica?
8. Incluir la hoja a mano completa escaneada (con los sellos de VoBo y de revisado =)
9. Incluir todo su código (como texto con formato, NO imágenes)


Dra. Nidia A. Cortez Duarte

EN CASO DE NO OBTENER EL SELLO DURANTE LA REVISIÓN PRESENCIAL

Elaborar diapositivas

- Portada
- Introducción con el árbol de la clasificación de la criptografía moderna
- Diagrama de Criptografía Híbrida (el que ustedes elaboraron)
- Demostración de práctica
- Conclusiones individuales

Deberán elaborar un video (duración máxima 17 min), en donde se muestre su escritorio

Primero proyectar sus diapositivas y empezar a explicar

En la mitad de la pantalla puede mostrar su código o las diapositivas y en la otra mitad de pantalla su interfaz gráfica. Durante toda su explicación se debe poder ver su vídeo en miniatura

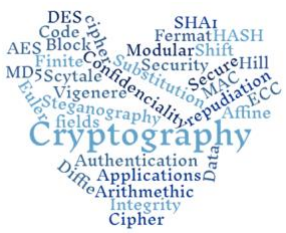
Previamente deben tener 3 carpetas de llaves: Alicia, Betito y Candy. (estas deben estar previamente generadas y no se debe mostrar dicho proceso en el vídeo)

Pruebas que deben incluir en su video.

A) 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) *(Si solo es un integrante, deberá cerrar su interfaz y abrir nuevamente cuando se trate de Betito así como utilizar una gorra o gafas o mascada)
B) Hacer que falle el servicio de Integridad y corregir para que vuelva a funcionar [Lo hace Candy]
C) Hacer que falle el servicio de Autenticación (para esto hacer usurpación con las llaves de Candy). 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.
D) Finalmente dejar de compartir pantalla y decir sus conclusiones individuales finales.

Nota: en cada paso nombrar el nombre del SERVICIO CRIPTOGRAFICO o ATAQUE tal y como lo vimos en clase.

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, el manejo de las llaves y el envio de mensajes. Sugiero que elaboren su guión para ser precisos y no excedan los tiempos. Dejaré de revisar los vídeos después del minuto 17 por favor ni me pregunten si puede durar mas.




Dra. Nidia A. Cortez Duarte