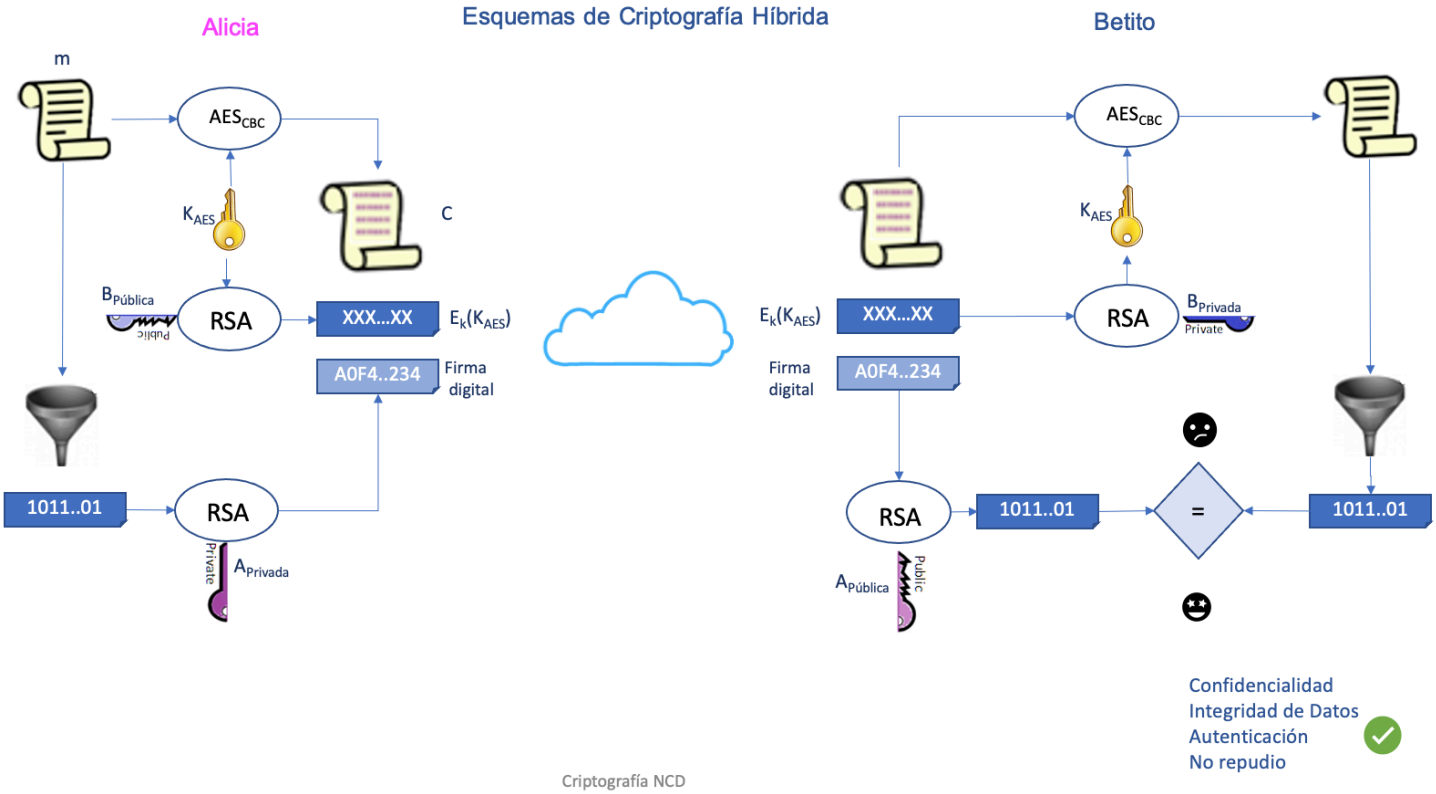
INSTITUTO POLITÉCNICO NACIONAL
ESCUELA SUPERIOR DE CÓMPUTO

Proyecto ETS Introduction to Cryptography

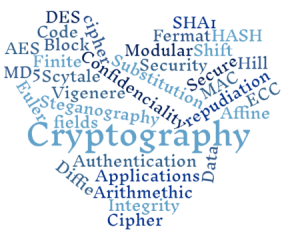
La criptografía moderna, creada a partir de 1948 con la Teoría de la Información de Claude Shannon, se divide en simétrica y asimétrica, una de las principales diferencias, es que en esta última se utiliza la clave pública del destinatario del mensaje para cifrar el mensaje y el destinatario usa su clave 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.



Criptografía NCD

1 Esquema Criptografía Híbrida



Dra. Nidia Asunción Cortez Duarte

Implementar el escenario de Criptografía Híbrida de la figura 1.
Se puede hacer uso de funciones existentes, sin embargo, deberán estar bien referenciadas.
Es necesario que UNO de los algoritmos utilizados se implemente desde cero, es decir, sin hacer uso de ninguna función cripgrográfica.
Debe contar con una interfaz gráfica que 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.

Cifrado/Descifrado

Proceso de Cifrado
1) Primero se genera una llave aleatoria y el IV de 16 bytes (transparente para el usuario).
2) A continuación se cifra el contenido del archivo con AES-128 usando los parametros previamente generados.
3) A continuación, dichos parametros se cifran con RSA haciendo uso de 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 los parametros del AES (descifrar con RSA usando la llave privada del receptor)
3) Finalmente, el contenido del archivo se descifra usando los la llave y el IV del AES.

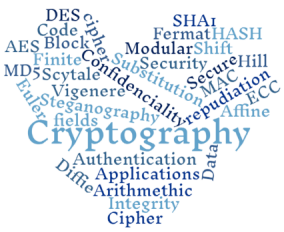
Firma/Verificación

Proceso de Firma / Verificación (Le pido que usted lo explique paso por paso en una diapositiva)

Entregables:

Elaborar diapositivas

- Portada
- Introducción con el árbol de la clasificación de la criptografía moderna
- Diagrama de cifrado/descifrado con criptografía simetrica [Elaborar a computadora]
- Diagrama de cifrado/descifrado con criptografía asimetrica [Elaborar a computadora]
- Diagrama de Criptografía Híbrida (puede usar el de la figura 1) en caso de que su implementación quedará exactamente igual, si usted concatenó diferente los parametros deberá actualizar el diagrama.
- Demostración de práctica
- Conclusiones



Dra. Nidia Asunción Cortez Duarte

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) 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) *(deberá cerrar su interfaz y abrir nuevamente cuando se trate de Betito)
B) Candy debe atacar para Confidencialidad y corregir para que vuelva a funcionar [probar primero con las llaves de Candy *fallará y después con las de Betito *debe funcionar]
C) Hacer que falle el servicio de Integridad y corregir para que vuelva a funcionar [Lo haces como Candy]
D) 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 termine) Betito intenta verificar con las llave de Candy y ahí descubre que realmente era un mensaje de Candy.
E) Finalmente dejar de compartir pantalla y decir sus conclusiones.

Para éste proyecto 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 elaborar un guión para ser precisos y no exceder los tiempos.

En cuanto tenga su vídeo debe enviar un correo a ncortezd@ipn.mx con el link correspondiente, como respuesta recibirá la hora de la revisión presencial de dicho proyecto (mismo día que el teórico), en donde deberá responder a varias preguntas (evaluación oral) con lo que concluye la revisión práctica.

La evaluación del ETS está conformada por:

- 20% vídeo demostración de su proyecto funcionando (Deadline: 1 día antes del examen escrito)
- 20% evaluación oral y demostración de funcionamiento específico solicitados por el profesor en la revisión de proyecto presencial (antes de las 15:00 del mismo día del examen)
- 60% Evaluación teórica (examen escrito)

Dra. Nidia Asunción Cortez Duarte