Tecnológico de Monterrey, Campus Monterrey
Escuela de Ingeniería y Ciencias
Ingeniería en Ciencia de Datos y Matemáticas
Uso de Álgebras Modernas para seguridad y criptografía MA2006B

Profesor: Alberto Francisco Martínez Herrera

Actividad de Reto - Reporte Técnico (avance previo a la entrega final)

Fecha de Entrega Avance: Viernes 22 de Abril de 2022

Nota: Si bien los resultados y las conclusiones son preliminares, deberán ser consistentes con la descripción proporcionada de su solución.

Reporte Técnico

Las rúbricas a cubrir son las siguientes:

1) **Portada del reporte.** Debe venir lo siguiente:
    a) Nombre oficial del Instituto (Instituto Tecnológico y de Estudios Superiores de Monterrey).
    b) Nombre de la Escuela (Escuela de Ingeniería y Ciencias).
    c) Nombre de la carrera (Ingeniería en Ciencias de Datos y Matemáticas)
    d) Nombre del bloque (Análisis de Criptografía y Seguridad)
    e) Nombre del reporte: Implementación de un Esquema de Firma Digital para Administración de Compras: Caso Fundación Teletón**.**
    f) Nombre completo de los estudiantes y matrículas respectivas.
    g) Nombre de los profesores.
    h) Nombre del Socio Formador (Fundación Teletón).
    i) Fecha y lugar de elaboración. Respecto al lugar, poner Monterrey, Nuevo León. Fecha, 20 de Abril de 2022.

2) Índice de contenidos

3) Introducción al reto

    Esta parte debe ser redactada con máximo 1000 palabras. Deberá describir el problema que tiene la Organización Socio Formadora, en este caso Fundación Teletón, y como lo van a resolver. De preferencia, incluir una figura que le ayude al lector a visualizar el problema que se está resolviendo. Recalcar quienes serán los beneficiarios de esta solución de manera directa e indirecta y quienes podrían beneficiarse en un futuro, de acuerdo a lo que se ha tratado en las sesiones realizadas con la Organización Socio Formador.

4) Estado del Arte

    En esta parte, debe considerarse todo lo que se encontró, tanto a los algoritmos de firma digital así como las bibliotecas de funciones que hallaron. Incluir tablas para ambos casos. A manera de ejemplo:

Referencia	Algoritmo	Hash	Clave	Patente

Tabla 1. Guía para clasificar fuentes bibliográficas.

Se sugiere incluir de preferencia, artículos recientes, estándares, y sobre todo indicar la posible existencia de patentes vigentes. O en su defecto, indicar cuándo expiró la patente del algoritmo. Lo mostrado en la Tabla 1 ayudará a que Uds justifiquen el por qué eligieron el algoritmo que implementarán para la solución al reto.

En el caso de las bibliotecas de funciones, se les muestra la siguiente tabla a manera de ejemplo:

Referencia	Biblioteca/versión	Lenguaje/versión	Licencia	Soporte Clave Pública

Tabla 2. Guía para clasificar bibliotecas de funciones.

En algunos casos, como puede ser la biblioteca hashlib de Python, dicha biblioteca únicamente nos ayuda a calcular hashes, por lo que no tiene incluida implementaciones de clave pública, pero el resto de los datos solicitados sí los tiene, por lo que en ese caso se debe indicar lo pedido en la Tabla 2. La información mostrada en la Tabla 2 ayudará a que Uds justifiquen por qué eligieron la(s) biblioteca(s) de funciones.

Para ambos casos, se requiere que las referencias de ambas tablas sean descritas, es decir, un breve resumen del contenido de dichas referencias. En el caso de las bibliotecas de funciones, se sugiere que realicen la descripción desde el punto de vista de las licencias y posteriormente indiquen (con su respectiva descripción) qué bibliotecas están cubiertas por dichas licencias.

Las Tablas 1 y 2 anteriormente mostradas, podrán ser modificadas por los equipos a como más les convenga, pero deberán mostrar información que le ayude al lector a determinar cómo los integrantes del equipo eligieron el/los algoritmos criptográficos y la/las bibliotecas de funciones para elaborar el reto.

5) Métodos y desarrollo de la solución propuesta

   En esta parte, los equipos deberán incluir cómo están elaborando el reto. Se debería incluir:

a) Cómo realizaron la parte de la generación de claves y cómo las están guardando y administrando. Recordar que la clave pública debe ayudar a generar un certificado que indicará quién tiene cada clave. Indicar si siguieron algún estándar para hacerlo, y sobre todo tanto los algoritmos elegidos así como las bibliotecas de funciones que ocuparon (o en su lugar, si esto lo implementaron desde cero). Referente a estándares e infraestructura, nos enfocamos en elementos tales como el uso de X.509, PKI o PKCS. En esta parte es importante indicar si están implementando una base de datos o alguna otra estrategia para almacenamiento y cómo están controlando la vigencia de los certificados (si es vigente, si está expirado o si fue revocado). Esto último es muy importante ya que tendrá incidencia directa en quién tiene derecho a firmar y quién no.
b) Cómo realizaron la parte de la generación de las firmas. Describir a detalle el/los algoritmos que eligieron. Se recuerda que la parte de generación de firmas nos debe permitir el que un usuario pueda firmar un documento en formato PDF. Aquí es muy importante indicar cómo leyeron el documento en PDF y como le calcularon su hash. Se espera que previamente Uds hayan usado una aplicación ya probada para calcular los hashes de los archivos probados, con el fin de que ese mismo hash obtenido en esa aplicación sea idéntico al hash generado en su solución. Todo esto, con el fin de que haya consistencia. Indicar las bibliotecas de funciones que ocuparon y/o si parte de lo que hicieron lo elaboraron desde cero.
c) Cómo realizaron la parte de la verificación de las firmas. Seguir el mismo procedimiento de descripción que en el punto anterior, pero acá indicar si su solución es capaz de verificar sólo una firma a la vez, o si es capaz de verificar varias firmas a la vez, e indicar si lo hacen secuencial o en paralelo (se firma el documento junto a la firma adjunta, o si las firmas son tratadas de manera independiente). Recordar que es posible que un documento pueda tener más de una firma, dependiendo del proceso interno existente en la OSF.
d) Para los 3 puntos, incluir figuras y diagramas de cómo lo están implementando, preferentemente usando diagramas de flujo o modelos basados en UML.
e) Indicar en qué sistema operativo se hizo, con qué interprete/compilador y el lenguaje de programación utilizado, además de la biblioteca y licencia utilizada.

6) Resultados y discusión

   En esta parte, se incluirán los resultados en base a la metodología que Uds siguieron. Se espera que en esta sección se describa primero como usaron los vectores de prueba para verificar los 3 componentes pedidos: generación de certificados, generación de firmas y verificación de firmas. En esta parte, indicar en

qué equipo hicieron dichas pruebas, con la descripción lo más detallada posible. Esa descripción incluye:

a) El equipo donde se hicieron las pruebas
b) Características del equipo (memoria, procesador)
c) Sistema Operativo
d) Plataforma donde se hicieron las pruebas (por ejemplo, si fue directo usando PyCharm o usaron el intérprete de Python por separado)
e) Lenguaje utilizado (por ejemplo, Python)
f) La plataforma donde desarrollaron la solución (por ejemplo, PyCharm, para Python)
g) La versión del lenguaje de programación.

La información anterior es muy importante ya que le dará al lector el contexto sobre el que deberá interpretar los resultados mostrados en las tablas que pondrán aquí, referentes al tiempo que tardaron sus soluciones en ejecutarse. Se muestra un ejemplo de una tabla donde se reportan dichos resultados (Tabla 3):

Algoritmo	Número de Pruebas	Media (en segundos)	Desviación estándar	Etapa
RSA2048/SHA1				Generación de claves
RSA2048/SHA1				Generación de firma
RSA2048/SHA1				Verificación de firma

Tabla 3. Ejemplo de guía para reportar resultados.

Para la parte de generación y verificación de firmas, parte de esas pruebas deberían usar los vectores ofrecidos ya sea en IETF o en los estándares del NIST, como se mostró en clase. Indicar si las pruebas las han automatizado y cómo lo hicieron.

Adicionalmente, deben incluir en esta sección cómo el programador o el usuario (dependiendo del enfoque que le hayan dado a la solución del reto) obtendrá de salida al momento de usar los componentes que Uds desarrollaron. Un ejemplo, que pongan la ventana donde el usuario sube su archivo para que firme y lo que obtiene de salida (cadena de caracteres, posiblemente en base 64, guardada en un archivo). Incluir todas las etapas.

Incluir una sección de discusión, donde Uds indicarán a detalle si existen mejoras por realizar. Idealmente aquí se tendría que haber usado una solución de referencia para hacer comparaciones, pero si no es ese el caso, indicar el impacto que tendrá el tiempo promedio respecto a cómo se va a reflejar cuando el usuario (o los

programadores) lo usen. Para esto es importante que indiquen de manera lo más precisa posible donde se hicieron las pruebas.

No olvidar que todo lo que pongan en esta sección debe tener consistencia con todo lo que describan en el documento.

7) Conclusiones y recomendaciones a futuro

Describir en esta parte si se lograron cubrir los objetivos de la OSF, los resultados más importantes y las posibles mejoras o recomendaciones a futuro para enriquecer la solución, enfocadas a la parte de desarrollo, además de lo que se espera dar de beneficio a la OSF. Incluir aquí la liga donde está toda la solución.

8) Anexos

En esta parte, incluir figuras de apoyo (si tienen figuras extra), y sobretodo los vectores de prueba ocupados (algunos, no todos, ya que recuerden los vectores de prueba van por separado)

9) Observaciones generales

No olvidar que el reporte es uno solo de los entregables. Considerar que se debe entregar:

a) La solución completa (el código fuente)
b) Manual del programador (la documentación)
c) Vectores de prueba (los que ocuparon para hacer las pruebas, tanto propios como los de IETF o NIST)
d) Licencia de uso, que debe ser compatible con las licencias de las bibliotecas que usaron.

Si se requiere citar literal un estándar o un artículo (o algún párrafo), dicho artículo o estándar (o párrafo) deberán ir en un párrafo aparte, debe poner comillas dobles para encerrarlo, y la cita respectiva inmediatamente al cerrar las comillas. Un ejemplo es:

> Jorge Ramió Aguirre define Criptografía como:
>
> “La Criptografía es la rama inicial de las Matemáticas y en la actualidad también de la Informática y la Telemática, que hace uso de métodos y técnicas con el objeto principal de cifrar, y por tanto proteger, un mensaje o archivo por medio de un algoritmo, usando una o más claves” [1].

Figuras. Las figuras deberán aparecer donde están siendo descritas en el documento. Y de la siguiente forma (se proporciona un ejemplo):

En la Fig. 2 podemos ver que se muestra como se ocupa pip install para bajar el paquete dpkt en Python, el cual ya había sido previamente instalado.

Fig. 2. Instalación del paquete dpkt en Python.

Cuidar que la figura se vea en el reporte. **Lo mismo vale para las tablas.**

Bibliografía. Deberá aparecer de manera numérica en el texto y citada en el lugar donde están describiendo la información que consultaron en la referencia correspondiente. Un ejemplo:

> Una de esas herramientas es la que Claude E. Shannon publicó en el artículo llamado “A Mathematical Theory of Communication”, donde él establece las bases de la llamada “Teoría de la Información” [2]. Dicha herramienta es el cálculo de la Entropía, que en términos generales mide la incertidumbre (aleatoriedad) de la información que se analiza.

El formato en el que aparecerán las referencias es libre.

El reporte debe ser elaborado en LaTeX. Respecto al formato general

a) Extensión: el reporte total deberá ser de entre 30 y 35 páginas totales (incluyendo portada, imágenes, referencias y anexos).
b) Proporción entre texto e imágenes: Se espera un documento en el que aproximadamente 70% de la extensión total sea texto con descripciones e ideas.
c) Tipo de documento LaTeX: usar el estilo “article”.
d) Tamaño de fuente: 10 pt.
e) Interlineado: 1.5 espacios (si ocupan LaTeX, usar la línea \renewcommand{\baselinestretch}{1.5} en el preámbulo del documento).
f) Tamaño de hoja: Carta.
g) Márgenes superior e inferior: 20mm.
h) Márgenes izquierdo y derecho: 25mm.

Entrega de archivos. En los lugares correspondientes en Canvas.

Bibliografía

1. Ramió Aguirre, J. (2021). Libro Electrónico de Seguridad Informática y Criptografía Versión 4.1: Capítulo 1. Presentación del Libro Electrónico.
2. Shannon, C. E. (2001). A mathematical theory of communication. *ACM SIGMOBILE mobile computing and communications review*, *5*(1), 3-55.