Tecnológico de Monterrey, Campus Monterrey
Escuela de Ingeniería y Ciencias
Ingeniería en Ciencia de Datos y Matemáticas
Aplicación de Criptografía y Seguridad MA2005B
Profesor de Reto: Alberto F. Martínez Herrera
Fecha de Entrega del Reporte: Determinada por el profesor de reto.
Fecha de Presentación por equipos: Determinada por el profesor de reto.

Introducción

Como parte de las actividades que se realizarán para la presentación, se tendrán los siguientes puntos para ambos reportes técnico y ejecutivo.

Reporte (tanto técnico como ejecutivo)

Los puntos a cubrir son las siguientes:

1) **Portada del reporte (ambos casos).** Debe venir lo siguiente:
    a) Escudo del Instituto.
    b) Nombre oficial del Instituto (Instituto Tecnológico y de Estudios Superiores de Monterrey).
    c) Nombre de la Escuela (Escuela de Ingeniería y Ciencias).
    d) Nombre de la carrera (Ingeniería en Ciencias de Datos y Matemáticas)
    e) Nombre del reporte: DNSSEC compliance de dominios bajo .mx **. Versión (y aquí deben poner si es la versión técnica o la versión ejecutiva).**
    f) Nombre completo de los estudiantes y matrículas respectivas.
    g) Nombre del profesor de reto.
    h) Nombre del Socio Formador (NIC México).
    i) Fecha y lugar de elaboración. Respecto al lugar, poner Monterrey, Nuevo León. Fecha, la que determinen los profesores.

2) Respecto a la descripción del reto.

    Versión técnica:
        - Introducción: Objetivos del reto, activos involucrados, alcance y fortaleza de las pruebas realizadas. Todo lo anterior desde el punto de vista técnico. Pueden dar una breve semblanza de DNS y DNSSEC.
        - Desarrollo: Cómo generaron su entorno de pruebas, qué pruebas hicieron, cómo recopilaron la información
        - Resultados: Árbol DNS con los dominios que tengan DNSSEC. El valor agregado del reporte es que indiquen si los dominios analizados cuentan con DNSSEC de acuerdo a lo que establece la IETF (algoritmos, negación de existencia, cadena de confianza, gestión de claves, validez de las firmas, etc.)
        - Conclusiones desde el punto de vista técnico. El resumen de los resultados obtenidos, recomendaciones y evaluación final.
        - Referencias
        - Anexos (si es que es necesario)

Versión ejecutiva:

- Introducción: Acá se describe cual es el propósito de haber hecho estas pruebas, enfocado a alguien que no sepa del tema. Es decir, en qué le beneficia que DNSSEC exista.
- Desarrollo: Debe describirse qué se hizo, pero sin abundar en la parte técnica. Pueden incluir diagramas de elaboración propia de cómo lo hicieron, y que pueden ocupar en su presentación final. La idea es que este documento sea la versión en extenso -o escrita- de lo que van a presentar. Por ejemplo, mostrar el árbol DNS e indicar qué ventajas existen entre un dominio firmado vs aquel que carezca de firma.
- Resultados: El enfoque dado es el impacto de que DNSSEC exista como medida de protección hacia un usuario final. En qué me beneficia que un dominio (por ejemplo, el de un banco) esté firmado vs si esto no ocurre.
- Evaluación final, conclusiones y recomendaciones. Sugerencias para su mayor adopción bajo el dominio .mx, sobre todo en aquellos dominios que manejen información altamente sensible (los bancos, por ejemplo).
- Referencias
- Anexos (si es que es necesario)

3) Observaciones generales **(esto no va en el reporte, esto es para cuestiones de formato y presentación)**.

Si se requiere citar literal una ley o un artículo (o algún párrafo), dicho artículo o ley (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" (Aguirre, 2006).

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. **Toda figura o tabla que no sea de autoría propia debe ser citada apropiadamente.** Por ejemplo:

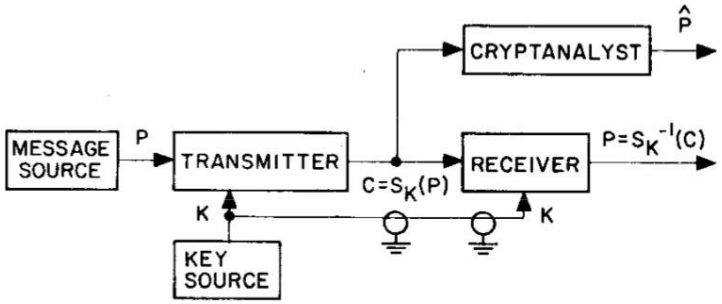

Fig. 3. Flujo de información en sistemas criptográficos convencionales (tomado de Diffie y Hellman, 1976).

De preferencia, dichas figuras o tablas hay que re-hacerlas.

En las tablas, si los datos son de una fuente bibliográfica, indicar dicha fuente bibliográfica. Incluso si la tabla o la figura respectiva se reconstruye/rehace, al ser tomada de una fuente, debe ser citada.

Por ejemplo:

Módulo clave pública	Tamaño clave privada
2048	112
3072	128
4096	152
6144	176
8192	200

Tabla 4: Fortaleza de clave en RSA, comparado con algoritmos de clave privada (Barker et al., 2019).

Bibliografía. Deberá aparecer en formato APA 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” (Shannon, 2001). Dicha herramienta es el cálculo de la Entropía, que en términos generales mide la incertidumbre (aleatoriedad) de la información que se analiza.

El reporte es en la plataforma de su preferencia. Se aconseja LaTeX, pero pueden usar Word. Respecto al formato general

a) Extensión: el reporte deberá ser de entre 16 y 20 páginas totales (incluyendo portada, imágenes y referencias) para la versión técnica y de 6 a 9 página totales para la versión ejecutiva. **Tomar en cuenta esto a la hora de ir elaborando cada etapa y así dar un espacio razonable. La razón de la brevedad del reporte ejecutivo es que debe ser rápido y ágil para que alguien que no sepa del tema entienda de lo que se está tratando, con el fin de que su toma de decisiones sea hecha de la misma manera.**
b) Proporción entre texto e imágenes: Se espera un documento en el que aproximadamente 65% de la extensión total sea texto con descripciones e ideas.
c) Tipo de documento si usan LaTeX: usar el estilo “report”.
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

Ramió Aguirre, J. (2006). Libro Electrónico de Seguridad Informática y Criptografía Versión 4.1: Capítulo 1. Presentación del Libro Electrónico.

Diffie, W., & Hellman, M. (1976). New directions in cryptography. *IEEE transactions on Information Theory*, *22*(6), 644-654.

Barker, E., Chen, L,. Roginsky, A., Vassilev, A., Davis, R. and Simon, S. (2019). NIST Special Publication 800-56b Revision 2-Recommendation for Pair-Wise Key Establishment Using Integer Factorization Cryptography, NIST Special Publication.

Shannon, C. E. (2001). A mathematical theory of communication (versión re-impresa). *ACM SIGMOBILE mobile computing and communications review*, *5*(1), 3-55.