Lectura 6/7

Instituto Tecnológico de Costa Rica. Escuela de Ingeniería en Computación. Redes - IC-7602. Grupo 2. Profesor: Gerardo Nereo Campos Araya Estudiante: Daniel Araya Sambucci - 2020207809 Fecha de entrega: 5/10/23

Preguntas:

- Explique en que consiste sistemas de cifrado por sustitución y por transposición, ¿Cuáles son sus diferencias?

El sistema de cifrado por sustitución consiste en que cada letra o grupo de letras se reemplaza por otra letra o grupo de letras para disfrazarla. Por otra parte, el sistema de cifrado por transposición consiste en un reordenamiento de las letras, lo que la diferencia de por sustitución al no disfrazar las letras. Un tipo de cifrado por transposición común es la transposición columnar, donde la clave se encarga de ordenar las columnas. Otra diferencia consiste en el camino que se puede tomar para resolverlos. En un cifrado por sustitución se pueden aprovechar las propiedades estadísticas de los lenguajes naturales, como por ejemplo en el inglés que la letra más común es la e y usar eso para analizar las letras que más se repitan en las palabras. En un cifrado por transposición se debe ser consciente de que el cifrado es un sistema de ese tipo. Se puede usar la frecuencia de letras para ver si se ajustan al patrón usual del texto plano, ya que cada letra se representa a sí misma y la distribución de frecuencia permanece intacta. Ya con esto el siguiente paso es adivinar la cantidad de columnas y finalmente ordenarlas.

- ¿Cómo funciona el DNS?

DNS consiste en un esquema jerárquico de nombres basado en dominios y un sistema de base de datos distribuido para implementar este esquema de nombres. Su función consiste principalmente en usarlo para asociar los nombres de host con las direcciones IP. Para asociar un nombre con una dirección IP, un programa de aplicación llama a un procedimiento de biblioteca llamador resolvedor y le pasa el nombre como parámetro. Entonces el resolverdor envía la consulta con el nombre al servidor DNS local, que después busca el nombre y devuelve una respuesta cin la dirección IP al resolvedor, que a su vez la devuelve al solicitante. Estos mensajes de solicitud y respuesta son enviados como paquetes UDP.

- ¿Por qué el DNS es tan robusto y se utiliza actualmente después de tantos años sin mayores cambios?

EL DNS al ser un sistema de naturaleza distribuida y descentralizada los nombres de dominios está distribuidos por todo el mundo, permitiendo redundancia y evitando un único punto de fallo. Además, la forma en que se agregan nuevos dominios y otros factores permiten una escalabilidad acorde al crecimiento exponencial de internet. Así mismo, su simplicidad permite una eficiente administración.

- ¿Cuál es el impacto del DNS en la forma en cual consumimos internet?

Se pueden utilizar dominios con usos definidos. Esto permite poder "catalogar" el contenido en internet y dar una accesibilidad más fácil, de la mano con los nombres de dominios fáciles de recordar por una persona. Así mismo, al ser una herramienta de recopilación de datos y publicidad en línea, se puede utilizar para redirigir a los usuarios y rastrear el comportamiento en línea.