UNIVERSIDAD NACIONAL DE SAN AGUSTÍN

FACULTAD DE INGENIERÍA DE PRODUCCIÓN Y SERVICIOS

ESCUELA PROFESIONAL DE CIENCIA DE LA COMPUTACIÓN

FUNCIONES ELEMENTALES DE CRIPTOGRAFÍA

Curso:

Seguridad en Computación - Laboratorio Grupo A

***Docente*:**

Franklin Luis Antonio Cruz Gamero

Realizado por:	*CUI*
PAREDES ESCOBEDO, FERNANDA	**20182906**

Arequipa - Perú

2021

Actividades

Las actividades se pueden encontrar en el siguiente enlace: Repositorio en Github

Conclusiones

Emitir al menos ocho conclusiones en torno al preprocesamiento de texto claro:

1. Uno de los objetivos del preprocesamiento del texto claro es alterarlo mediante diversas funciones para hacerlo más resistente al criptoanálisis.

2. Para poder realizar las funciones se requieren nociones previas en programación y manejo de ficheros en cualquier lenguaje de programación.

3. De igual forma, para poder realizar algunas funciones, se requiere entender los sistemas de codificación ASCII y Unicode.

4. Para aplicar el método Kasiski se debe entender en qué consiste, así podemos determinar la longitud de la clave en un cifrado Vigenère, y podremos buscar las palabras repetidas en el texto.

5. Las operaciones de preprocesamiento deben seguir un orden, debido a que algunas funciones no admiten caracteres especiales, puesto que estos han debido de ser tratados en un método anterior.

6. Se requiere entender el funcionamiento del compilador según el lenguaje de programación que se esté usando, para poder evitar errores de compilación en las funciones de preprocesamiento.

7. Resulta un poco complicado realizar algunas funciones de preprocesamiento de texto en C++, debido a que se deben cambiar los caracteres de ANSI a UNICODE para poder realizar algunas funciones con caracteres especiales.

8. Para procesar otros archivos de texto claro se deben considerar todas las opciones que tiene ese texto. Por ejemplo, si en el texto hay diéresis o palabras en otro idioma, primero se deben convertir esas letras para poder ejecutar las otras funciones con normalidad.

Cuestionario Final

1. ***Describa los siguientes términos (áreas de la seguridad informática***)

- **Protección y seguridad de los datos:** La seguridad de datos es un aspecto esencial de TI en organizaciones de cualquier tamaño y tipo. Se trata de un aspecto que tiene que ver con la protección de datos contra accesos no autorizados y para protegerlos de una posible corrupción durante todo su ciclo de vida. Los tres elementos principales a proteger en cualquier sistema informático son el software, el hardware y los datos.

- **Criptografía:** La criptografía es una ciencia que estudia la información, cómo preservarla y protegerla. Su objetivo es definir algoritmos y protocolos que permitan proteger la información. A partir de la criptografía es posible identificar amenazas en la seguridad de la información tanto en protocolos y programación de esta como en errores humanos, como olvidar los cambios de contraseñas o compartir información indebida.

- **Seguridad y fortificación de redes:** La seguridad de redes consiste en las políticas y prácticas adoptadas para prevenir y supervisar el acceso no autorizado, el uso indebido, la modificación o la denegación de una red informática y sus recursos accesibles. La seguridad de redes involucra la autorización del acceso a datos en la red, que es controlada por el administrador de red. Los usuarios eligen o se les asigna una identificación y contraseña u otra información de autenticación que les permite acceder a información y programas dentro de sus autorizaciones. La seguridad de red cubre una variedad de redes de computadoras, tanto públicas como privadas, que se usan en trabajos cotidianos; realizar transacciones y comunicaciones entre empresas, agencias gubernamentales e individuos. Las redes pueden ser privadas, como dentro de una empresa, y otras que pueden estar abiertas al público. La seguridad de las redes está presente en organizaciones, empresas y otros tipos de instituciones. Hace como su nombre indica: protege la red, además de proteger y supervisar las operaciones que se realizan. La forma más común y simple de proteger un recurso de red es asignándole un nombre único y la contraseña correspondiente.

- **Seguridad en aplicaciones informáticas, programas y bases de datos:** La seguridad de las aplicaciones se refiere a las medidas de seguridad, a nivel de aplicación, cuyo propósito es impedir el robo o el secuestro de datos o códigos dentro de la aplicación. Abarca las consideraciones de seguridad que se deben tener en cuenta al desarrollar y diseñar aplicaciones, además de los sistemas y los enfoques para proteger las aplicaciones después de distribuirlas. Se refiere al proceso de desarrollar, añadir y probar características de seguridad dentro de las aplicaciones para evitar

vulnerabilidades de seguridad contra amenazas, tales como la modificación y el acceso no autorizados. La seguridad de datos se refiere a medidas de protección de la privacidad digital que se aplican para evitar el acceso no autorizado a los datos, los cuales pueden encontrarse en ordenadores, bases de datos, sitios web, etc. También protege los datos de una posible corrupción.

- **Gestión de seguridad en equipos y sistemas informáticos:** Todos los equipos conectados a un servidor pueden considerarse como un gran sistema multifacético. Usted es responsable de la seguridad de este sistema más grande. Debe proteger la red contra los desconocidos que intentan obtener acceso. También debe garantizar la integridad de los datos en los equipos de la red. Para controlar el acceso al sistema, debe mantener la seguridad física del entorno informático. Por ejemplo, un sistema cuya sesión está iniciada pero desatendida es vulnerable al acceso no autorizado. Un intruso puede obtener acceso al sistema operativo y a la red. El entorno y el hardware del equipo deben estar físicamente protegidos contra el acceso no autorizado.

- **Informática forense:** El término forense significa literalmente utilizar algún tipo de proceso científico establecido para la recopilación, análisis y presentación de la evidencia que se ha recopilado. Sin embargo, todas las formas de evidencia son importantes, especialmente cuando se ha producido un ataque cibernético. Es la disciplina que combina los elementos del derecho y la informática para recopilar y analizar datos de sistemas informáticos, redes, comunicaciones inalámbricas y dispositivos de almacenamiento de una manera que sea admisible como prueba en un tribunal de justicia.

- **Ciberdelito, ciberseguridad:** Ciberdelito es un término genérico que hace referencia a la actividad delictiva, llevada a cabo mediante equipos informáticos o a través de Internet. El ciberdelito puede hacer uso de diferentes métodos y herramientas, como el phishing, los virus, spyware, ransomware o la ingeniería social, normalmente con el objetivo de robar información personal o de realizar actividades fraudulentas. La ciberseguridad es la práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos. También se conoce como seguridad de tecnología de la información o seguridad de la información electrónica.

1. ***Describa los siguientes términos (áreas de la seguridad de la información)***

- **Gestión de la seguridad de la información:** esta consta de políticas, procedimientos, directrices, recursos y actividades asociados, gestionados colectivamente por una organización, con el fin de proteger sus activos de información. En general se usa un enfoque sistemático para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información de una organización para lograr los objetivos comerciales. Se basa en una evaluación de riesgos y los niveles de aceptación de riesgos de la organización diseñados para tratar y gestionar los riesgos de forma eficaz.

- **Asesoría y auditoría de la seguridad:** Una auditoría de seguridad informática o auditoría de seguridad de sistemas de información (SI) es el estudio que comprende el análisis y gestión de sistemas llevado a cabo por profesionales para identificar, enumerar y posteriormente describir las diversas vulnerabilidades que pudieran presentarse en una revisión exhaustiva de las estaciones de trabajo, redes de comunicaciones o servidores. Una vez obtenidos los resultados, se detallan, archivan y reportan a los responsables quienes deberán establecer medidas preventivas de refuerzo y/o corrección siguiendo siempre un proceso secuencial que permita a los administradores mejorar la seguridad de sus sistemas aprendiendo de los errores cometidos con anterioridad. Las auditorías de seguridad de SI permiten conocer en el momento de su realización cuál es la situación exacta de sus activos de información en cuanto a protección, control y medidas de seguridad.

- **Análisis y gestión de riesgos:** El análisis de riesgos informáticos es un proceso que comprende la identificación de activos informáticos, sus vulnerabilidades y amenazas a los que se encuentran expuestos así como su probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar los controles adecuados para aceptar, disminuir, transferir o evitar la ocurrencia del riesgo. Busca garantizar la integridad, confidencialidad y accesibilidad a todos los datos informáticos de una organización, una tarea especialmente importante para las empresas en un escenario en que los sistemas de información se vuelven cada vez más indispensables.

- **Continuidad de negocio:** La continuidad del negocio describe los procesos y procedimientos puestos en marcha por una organización con el fin de garantizar que sus funciones esenciales puedan continuar tras producirse un incidente grave: pérdida de información informática, inutilización o colapso del software, inundación, incendio, ataque terrorista, paralización de un planta por una avería técnica, etc.

- **Buen gobierno:** Gobierno de TI es el alineamiento de las Tecnologías de la información y la comunicación (TI) con la estrategia del negocio. Hereda las metas y la estrategia a todos los departamentos de la empresa, y proporciona el mejor uso de la tecnología y de sus estructuras organizativas para alcanzarlas. Un buen gobierno consiste en un completo marco de estructuras, procesos y mecanismos relacionales.

- **Comercio electrónico:** El comercio electrónico, traducido del término en inglés *e-commerce,* puede ser definido como la actividad económica que permite el comercio de productos y servicios a partir de medios digitales, como páginas web, aplicaciones móviles y redes sociales. Por medio de la red virtual los clientes pueden acceder a diversos catálogos de servicios y productos en todo momento y en cualquier lugar. La relevancia de este tipo de comercio es tal que los negocios lo toman como parte de la estrategia de ventas gracias a su eficiencia.

- **Legislación relacionada con seguridad:** la legislación informática es un conjunto de reglas jurídicas de carácter preventivo y correctivo derivadas del uso de la informática. En el Perú, el las leyes tiene el objetivo de proteger la infraestructura de información, los datos e información del Estado y la tecnología utilizada para su procesamiento, frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

2. ***Describa alguna otra operación o función de preprocesamiento que se implemente sobre el texto claro en los criptosistemas, en que afecta la complejidad de estas funciones al desempeño del mismo***

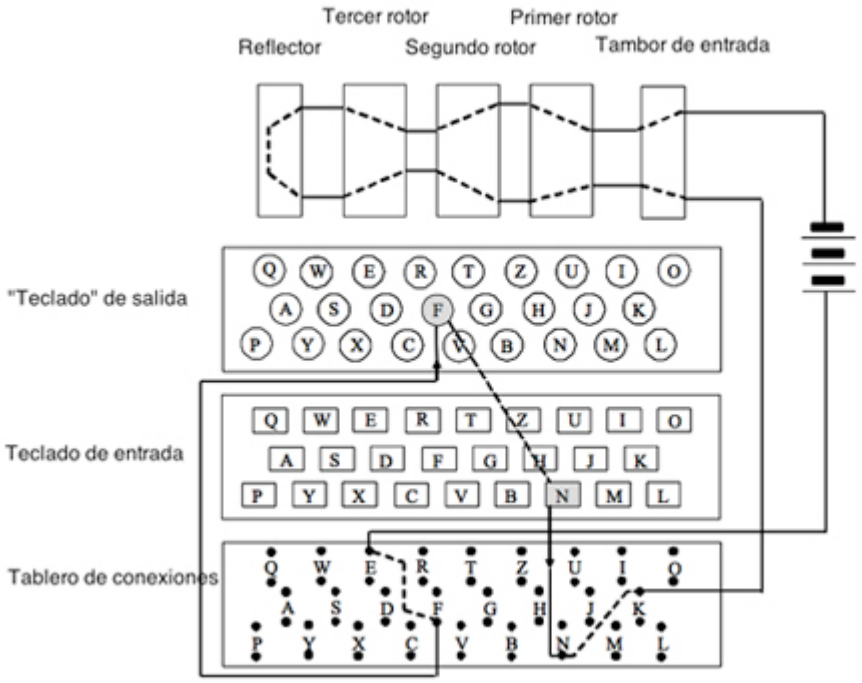
   Una función que permita remover caracteres duplicados que se repiten más de dos veces, es decir, una secuencia como “bbbbb”, se reduciría a “bb”.

   En el preprocesamiento se pueden seguir varios pasos que permitan que el cifrado resultante sea más resistente frente a ataques por criptoanálisis. Todos estos cambios se tendrán que tener en cuenta cuando se realice el descifrado para poder obtener el texto claro original. Afecta a la complejidad pues se dificulta el criptoanálisis, esto debido a que se aumenta la calidad del texto cifrado con cierto cifrador, ya sea por su resistencia frente a ataques, extensión o cualquier otra circunstancia. Por ejemplo, cuando se implementa la función para eliminar espacios en blanco, se consigue que las palabras no se puedan distinguir por los contornos

3. ***Describa la máquina enigma, luego muestre usando un simulador en internet la encriptación de la frase QUERIDA HIJA, para tres posiciones distintas de los rotores***

Máquina Enigma

La máquina Enigma era un dispositivo electromecánico, es decir, tenía una parte eléctrica y otra mecánica. El mecanismo consistía en una serie de teclas, con las letras del alfabeto, al igual que una máquina de escribir, que en realidad eran interruptores que accionaban los dispositivos eléctricos y hacían mover unos cilindros rotatorios. La máquina inventada en 1918 por el ingeniero alemán Arthur Scherbius, consistía en aplicar el Cifrado de Vigenère o, dicho de otra forma, se aplicaba un algoritmo de sustitución de unas letras por otras. Estaba compuesta, básicamente, por tres elementos conectados entre sí por cables: un teclado para introducir el mensaje original, una unidad modificadora y un tablero con lámparas donde se iluminaba la letra correspondiente del mensaje cifrado. La parte fundamental era la unidad modificadora, responsable del proceso de codificación, e integrada por tres tipos de elementos: clavijero, rotores y reflector. Las Enigma disponían de tres rotores, conectados entre sí en serie. Discos gruesos, cada uno con 26 puntos de entrada (uno por cada letra del alfabeto) y otros tantos de salida. El cableado interior, diferente en cada disco, hacía que la señal que entraba por una posición saliese por otra distinta: la desviaba convirtiéndola en otra letra. Además cada rotor giraba automáticamente a un ritmo determinado. El primer rotor giraba una posición cada vez que se pulsaba una letra del mensaje original. El segundo rotor avanzaba una posición cada vez que el primero completaba una vuelta completa. Y el tercero hacía lo propio cuando la completaba el segundo.



Simulador

1. Rotores en posición AAA

2. Rotores en posición XYZ

3. Rotores en posición FER

4. Describa la aplicación de Unicode-8

UTF-8 (8-bit Unicode Transformation Format) es un formato de codificación de caracteres Unicode e ISO 10646 que utiliza símbolos de longitud variable. UTF-8 fue creado por Robert C. Pike y Kenneth L. Thompson. Está definido como estándar por la <RFC 3629> de la Internet Engineering Task Force (IETF). Las principales ventajas son:

- UTF-8 permite codificar cualquier carácter Unicode.
- Es compatible con US-ASCII, la codificación del repertorio de 7 bits es directa.
- Fácil identificación. Es posible identificar claramente una muestra de datos como UTF-8 mediante un sencillo algoritmo. La probabilidad de una identificación correcta aumenta con el tamaño de la muestra.
- UTF-8 ahorrará espacio de almacenamiento para textos en caracteres latinos, donde los caracteres incluidos en US-ASCII son comunes, cuando se compara con otros formatos como UTF-16.
- Una secuencia de bytes para un carácter jamás será parte de una secuencia más larga de otro carácter por contener información de sincronización.

Unicode es un estándar de codificación de caracteres universal que asigna un código a cada carácter y símbolo en todos los idiomas del mundo. Dado que ningún otro estándar de codificación admite todos los idiomas, Unicode es el único estándar de codificación que garantiza que pueda recuperar o combinar datos utilizando cualquier combinación de idiomas. Una codificación basada en Unicode como UTF-8 puede soportar muchos idiomas y puede acomodar páginas y formularios en cualquier mezcla de esos idiomas. Su uso también elimina la necesidad de que la lógica del server-side determine individualmente la codificación de caracteres para cada página servida o cada envío de formulario entrante. Esto reduce significativamente la complejidad de tratar con un sitio o aplicación multilingüe. Una codificación Unicode también permite mezclar muchos más idiomas en una sola página que cualquier otra opción de codificación.

Bibliografía

[1] G. PowerData, “Seguridad de datos: En qué consiste y qué es importante en tu empresa.” [Online]. Available: Seguridad de Datos

[2] “¿Qué es la criptografía y cómo incide en la seguridad informática?,” Aug. 14, 2020. [Online]. Available: Criptografía

[3] “Seguridad de redes,” *Wikipedia*, Apr. 17, 2021. [Online]. Available: Seguridad de redes

[4] “What is Application Security?,” *VMware*. [Online]. Available: Seguridad de las aplicaciones

[5] G. PowerData, “Seguridad de datos: En qué consiste y qué es importante en tu empresa.”. [Online]. Available: Seguridad de datos

[6] “Gestión de seguridad de equipos (descripción general) - Guía de administración del sistema: servicios de seguridad,” *Gestión de seguridad de equipos (descripción general)*. Gestión de seguridad en equipos

[7] Y. Gonzales. “Informática forense: Qué es, cómo realizar un análisis forense,” *Ático34 Protección de datos para empresas y autónomos*, Jul. 03, 2020. [Online]. Available: Informática Forense

[8] L. C, “¿Qué conoces del ciberdelito?”. [Online]. Available: ¿Qué conoces del ciberdelito?

[9] Kaspersky, “¿Qué es la ciberseguridad?”, Aug. 09, 2021. [Online]. Available: Ciberseguridad

[10] “Sistema de gestión de seguridad de la información,” *Gobierno del Perú*. [Online]. Available: Gestión de la seguridad de la información

[11] “Auditoría de seguridad de sistemas de información,” *Wikipedia*, Aug. 17, 2020. [Online]. Available: Auditoría de seguridad

[12] Hacknoid, “Importancia de la gestión de riesgos informáticos - Hacknoid,” *HACKNOID*, Aug. 26, 2019. [Online]. Available: Gestión de riesgos

[13] EditorR, “Importancia de la seguridad de la información en un plan de continuidad del negocio,” *ISOTools*, Nov. 12, 2015. [Online]. Available: Continuidad del negocio

[14] F. Valencia, C. Marulanda, and M. López, “Gobierno de las Tecnologías de la Información. Uso y Prácticas en las Entidades Públicas del Triángulo del Café, Colombia,” *Información tecnológica*, vol. 29, no. 3, pp. 249–256, Jun. 2018, doi: 10.4067/s0718-07642018000300249.

[15] E. H. Higuerey, “¿Qué es el comercio electrónico y cuáles son sus ventajas?,” *Rock Content*, Jun. 01, 2019. [Online]. Available: Comercio electrónico

[16] Apaza, “Política Nacional de Ciberseguridad”. [Online]. Available: Legislación en seguridad

[17] Velasco, “La máquina Enigma, el sistema de cifrado que puso en jaque a Europa” *Hipertextual*, Jul. 11, 2011. [Online], Available: Enigma

[18] “Enigma Machine Emulator,” *101 Computing*, Apr. 22, 2019. [Online]. Available: Simulador de la máquina Enigma

[19] “Choosing & applying a character encoding”. [Online]. Available: Unicode