Universidad Nacional de San Agustín de Arequipa
Facultad de Ingeniería, Producción y Servicios
Escuela Profesional de Ciencia de la Computación

Laboratorio #1

Funciones Elementales de Criptografía

Alumna: Chullunquía Rosas, Sharon Rossely Alisson
Docente: Franklin Luis Antonio Cruz Gamero
Fecha: 15 de septiembre de 2021

Arequipa, Perú

Índice de Contenidos

Índice de Figuras

1. Preprocesamiento

El código del preprocesamiento se encuentra en el siguiente repositorio: GitHub

2. Conclusiones

- Es fundamental realizar un preprocesamiento del texto plano antes de realizar el cifrado, ya que este nos evita evidenciar algún rastro del texto claro.
- Las frecuencias de cada trigrama son importantes para desencriptar el mensaje cifrado, ya que puede permitirnos obtener la llave del cifrado.
- En un texto preprocesado podemos identificar sílabas a partir de los caracteres que más se repiten.
- Los espacios en blanco de un texto plano evidencian la longitud de cada palabra, por lo que es necesario eliminarlo del texto plano.
- El preprocesamiento basado en UNICODE-8 ayudan a crear cyphers que comparten un conjunto global de caracteres.
- En un texto plano español podemos encontrar caracteres únicos del lenguaje español, por lo que se puede relacionar con los caracteres de baja frecuencia del texto preprocesado.
- El método de Kasiski nos puede permitir encontrar palabras cortas.
- Al obtener las distancias entre los trigramas repetidos, podemos hallar la longitud de la clave mediante la operación de máximo común divisor de las distancias.

3. Cuestionario Final

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

   - **Protección y seguridad de los datos:**
     La protección de datos consiste en la preservación de la información fundamental frente a posibles ataques informáticos que puedan corromper la información, o hasta incluso hacerla perder.La protección de datos se enfoca en la recuperación y copia de seguridad de los datos. Cuando nos referimos a la seguridad de los datos, hacemos alusión a la defensa de la información digital, la cual es atacada por amenazas internas y externas, siendo estas generadas accidentalmente o maliciosamente. El enfoque de la seguridad de los datos está en mantener a salvo los datos e incorpora la seguridad de la infraestructura.[1]
   - **Criptografía:**
     La criptografía es el área de construcción de sistemas criptográficos. Es un campo de la matemáticas y de la informática que se enfoca en técnicas para la comunicación segura entre dos partes mientras un tercero está presente. La criptografía

se basa en métodos como cifrado, descifrado, generación de números pseudo-aleatorios, firma, etc.[2]

A continuación, se muestra en la imagen 6, en la cual se trata de ilustrar una comunicación segura, donde Alice y Bob representan las 2 partes que mantienen una comunicación, y el tercero presente sería Eve1 o Mallory.Este tercero busca ver la conversación entre Alice y Bob, pero no lo logra ya que se esta aplicando la encriptación de mensajes.

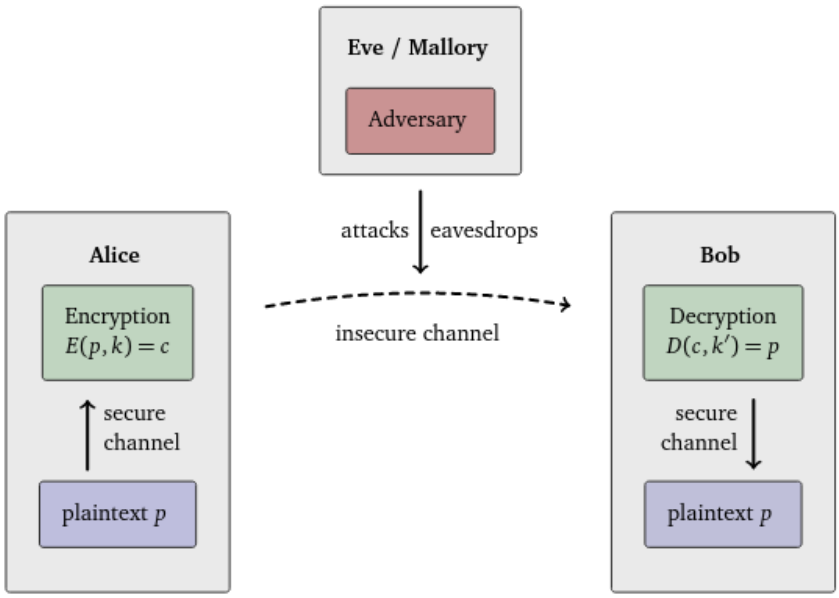

Figura 1: Una idea básica para una comunicación segura [2]

- **Seguridad y fortificación de redes:**

  Este campo reside en medidas que permiten prevenir, detectar, disuadir y corregir violaciones de seguridad que implica la transmisión de la información.[3]

- **Seguridad en aplicaciones informáticas,programas y bases de datos:**

  Esta área se enfoca en la toma de medidas para garantizar la seguridad, como el bloqueo de la cuenta principal root, con el fin de que no cualquier usuario pueda tener el control total; o como el acceso limitado a determinados recursos del sistema.[4]

- **Gestión de seguridad en equipos y sistemas informáticos:**

  Consiste en mantener un registro de todos los accesos, y más aun de aquellos que son denominados como sospechosos. En un espacio de trabajo, uno es responsable del sistema que conforma todos los equipos conectados a un servidor de la organización; se tiene la responsabilidad de proteger la red, asegurando la integridad de los datos intercambiados.[5]

Figura 2: Gestión de seguridad en equipos y sistemas informáticos

- **Informática forense:**

  La informática forense consiste en la práctica de la recopilación, análisis e información sobre datos informáticos de modo legal y admisible.

  La informática forense es el uso de técnicas especializadas para la autenticación, recuperación y análisis de los datos cuando se presenta un caso en el que se involucra cuestiones relacionadas con el examen de datos residuales, la reconstrucción del uso de una computadora y la autenticación de datos a través de un análisis técnico.

  La informática forense demanda conocimientos especializados que va más por encima de las técnicas normales de recopilación y conservación de datos disponibles para el personal de soporte del sistema o usuarios finales.[6]

Figura 3: Informática forense

- **Ciberdelito, ciberseguridad:**

  El ciberdelito es cualquier acto criminal que implica el uso de una herramienta digital o internet. Por ejemplo, robos de identidad, estafas en internet, robo de cuentas bancarias son considerados como delitos cibernéticos o ciberdelitos.

  La ciberseguridad es un conjunto de conceptos de seguridad, políticas, acciones, prácticas idóneas, seguros y tecnologías que puedan ser utilizados con el fin de salvaguardar los activos de una determinada organización.[7]

Figura 4: Ciberseguridad

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

   - **Gestión de la seguridad de la información:**

     Un Sistema de Gestión de Seguridad de la Información proporciona un modelo para crear, implementar, hacer funcionar, supervisar, revisar, mantener y mejorar la protección de los activos de información para alcanzar los objetivos de negocio.

   - **Asesoría y auditoría de la seguridad:**

     Es un proceso que consiste de gestión y análisis de sistemas, el cual es realizado por personas especializadas en el área, con el fin de identificar, enumerar y describir las diversas vulnerabilidades que pueden encontrarse en una exhaustiva revisión de los servidores o redes de comunicaciones.

     Cuando son obtenidos los resultados se detalla, archiva y reporta a los responsables de establecer medidas de refuerzo siguiendo un proceso secuencial para mejorar la seguridad de los sistemas.[8]

   - **Análisis y gestión de riesgos:**

     El Análisis y gestión de riesgos comprende la identificación de activos informáticos y de las diferentes amenazas que pueden afectar a nivel informático, ocasionando intrusiones o robos que como consecuencia pueda exponer los datos o el mal funcionamiento del sistema, logrando de esta manera una inactividad empresarial. El análisis y gestión de los riesgos toma medidas de prevención frente a esta serie de eventos negativos.[9]

Figura 5: Análisis y gestión de riesgos

- **Continuidad de negocio:**
  La continuidad de negocio es la capacidad, que tiene una empresa u organización, de preservar las funciones fundamentales durante y después de un evento negativo para la organización.[10]
- **Buen gobierno:**
  Buen gobierno es el conjunto de prácticas, normas, códigos de ética y elementos de conducta empresarial que promueven la existencia de diferentes relaciones como armónicas, ecuánimes y transparentes entre todos los integrantes de una empresa. Para las TIC, buen gobierno es un marco para la toma de decisiones y la asignación de responsabilidades para impulsar el comportamiento esperado respecto al uso de las TIC.[11]
- **Comercio electrónico:**
  El comercio electronico es cualquier forma de intercambio de información que se encuentra centrada en la transmisión de datos sobre las redes de comunicación, tales como el internet. Esta definición, además de incluir la compra y venta electrónica, tambien incluye el uso de la red para actividades anteriores y posteriores a la venta.[12]

Figura 6: Comercio electrónico

- **Legislación relacionada con seguridad:**
  Dentro de la legislación relacionada con la seguridad, tenemos la ley de Protección de Datos Personales, la cual se distingue por delimitar principios generales, relativos a la protección de datos. Esto comprende desde los derechos de los titulares hasta las figuras de usuarios y los responsables de los registros y bancos de datos. Las sanciones, el control y la acción de protección de los datos personales están vinculados a esta. También está la ley de Delitos Informáticos, que comprende de la interrupción de comunicaciones mediante ataques DDoS, acceso ilegítimo a sistemas informáticos o envio de código malicioso.[13]

3. **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 operación o función de preprocesamiento que afecta la complejidad de estas funciones al desempeño del mismo, podría decirse que es la inserción de cadenas

en el texto claro, ya que al momento de la inserción en cada cierto número de carácteres del texto plano, este va modificando el tamaño del archivo y por lo tanto las posiciones de los caracteres del texto plano van cambiando, resultando en una operación compleja.

4. **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.**

   La máquina Enigma fue un dispositivo electromecánico, inventada por un ingeniero alemán, Arthur Scherbius, un experto en electromecánica que quiso introducir la tecnología tras la Primera Guerra Mundial, con el fin de mejorar los sistemas de criptografía de los ejércitos. La máquina Enigma usaba una combinación de partes mecánicas y eléctricas. El mecanismo estaba compuesto fundamentalmente por un teclado parecido al de las máquinas de escribir cuyas teclas eran interruptores eléctricos, un engranaje mecánico y un panel de luces con las letras del alfabeto. En la maquina Enigma se aplicaba un algoritmo de sustitución de letras(Cifrado de Vigenère).[14]

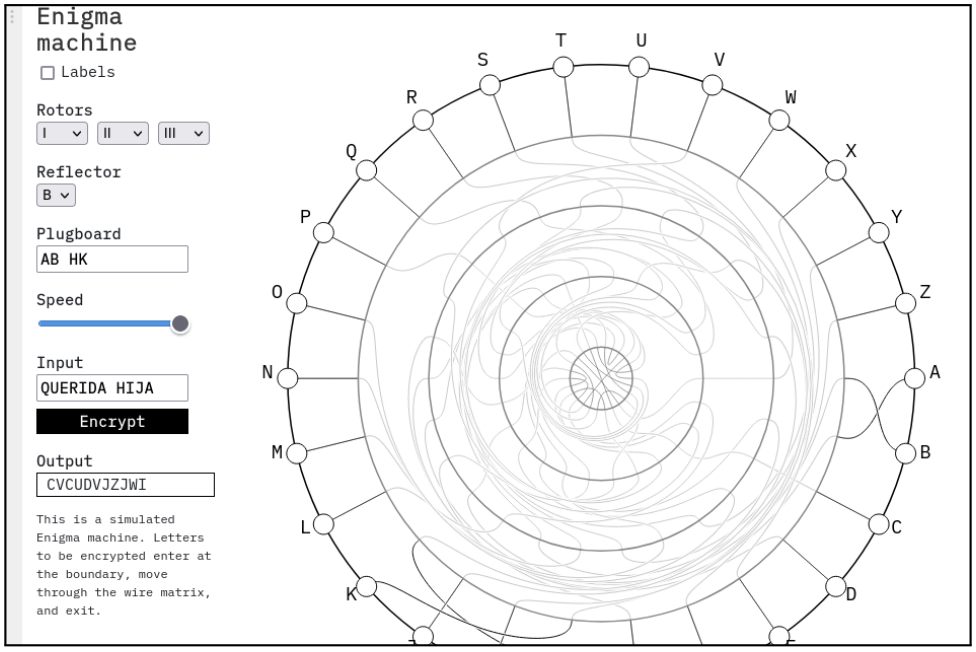

Figura 7: Simulador de la Máquina Enigma

5. **Describa la aplicación de Unicode-8.**

   Unicode es la codificación de caracteres universal, representa el estándar que hace posible la comunicación entre todo el mundo, este estándar de codificación brinda la base para el almacenamiento, procesamiento e intercambio de datos de texto en cualquier idioma.[15]

Referencias

[1] B. Posey, "¿qué es privacidad de datos, seguridad de datos y protección de datos?."

[2] M. Barakat, C. Eder, and T. Hanke, "An introduction to cryptography," *Timo Hanke at RWTH Aachen University*, pp. 1–145, 2018.

[3] W. Stallings, "Cryptography and network security: Principles and practice 0133354695, 9780133354690,"

[4] B. Thuraisingham, *Database and applications security: Integrating information security and data management*. CRC Press, 2005.

[5] S. Aravindan, "What is security management? - systems and applications," Apr 2020.

[6] J. Pande and A. Prasad, "Digital forensics," *Uttrakhand Open University*, 2016.

[7] J. Kremling and A. M. S. Parker, *Cyberspace, cybersecurity, and cybercrime*. SAGE Publications, 2017.

[8] Á. G. Vieites, *Auditoria de seguridad informática (MF0487_3)*. Grupo Editorial RA-MA, 2011.

[9] M. P. Kailay and P. Jarratt, "Ramex: a prototype expert system for computer security risk analysis and management," *Computers & Security*, vol. 14, no. 5, pp. 449–463, 1995.

[10] E. Sullivan, "Continuidad de negocios, business continuity, bcp."

[11] G. B. Urbina, *Introducción a la seguridad informática*. Grupo editorial PATRIA, 2016.

[12] H. T. Álvarez, *El sistema de seguridad jurídica en el comercio electrónico*. Fondo Editorial PUCP, 2005.

[13] C. de Pablos Heredero, J. J. L. H. Agius, S. M.-R. Romero, and S. M. Salgado, *Organización y transformación de los sistemas de información en la empresa*. Esic, 2019.

[14] P. Cipher, B. Park, and P. Bruno, "Enigma machine,"

[15] K. Whistler, M. Davis, and A. Freytag, "The unicode character encoding model," *The Unicode Consortium, Tech. Rep*, vol. 17, 2008.