## LABORATORIO 01

# Seguridad en Computación

## Erick Gutierrez Enriquez

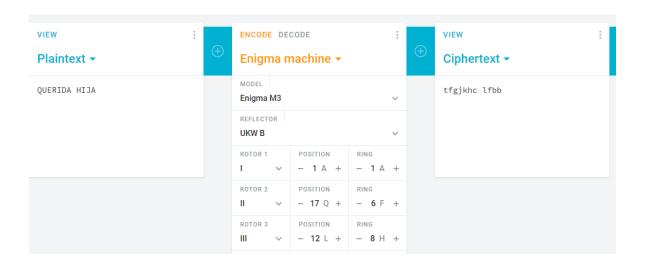
#### **Conclusiones**

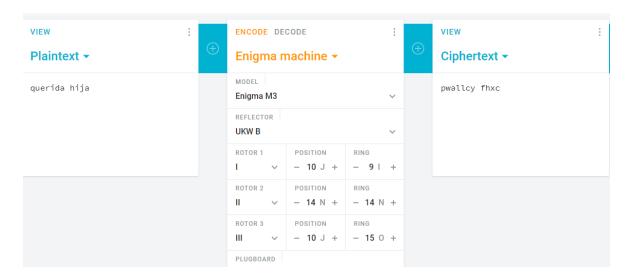
- Preprocesar un texto hace más difícil la obtención del texto original.
- La dificultad de obtener el texto original dependerá de las funciones de preprocesamiento aplicadas.
- Algunos cifrados básicos son sencillos de romper.
- El método kasiski es muy útil para romper el cifrado de Vigenère
- Analizando el texto cifrado podemos ver cuáles caracteres más se repiten y obtener así pistas de cómo descifrarlo.
- UNICODE-8 puede servir para cifrar aún más el mensaje y si se desconoce su tabla puede ser muy difícil de descifrar.
- Agregar palabras en el texto preprocesado puede ayudar a que sea más difícil obtener el texto original
- Se debe escoger una buena palabra a agregar ya que puede que se elimine varias veces en el texto al momento de descifrar.

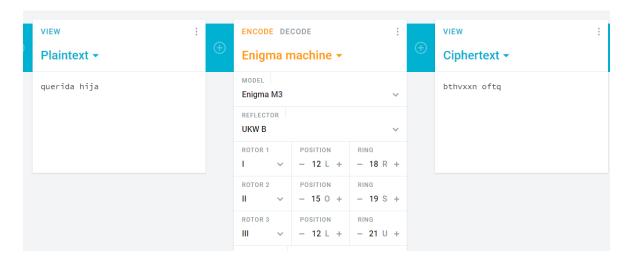
#### Cuestionario

- 1. Describa los siguientes términos (áreas de la seguridad informática).
  - Protección y seguridad de los datos: Consiste en mantener a salvo los datos que un sistemas usa y que pueden ser privados de los usuarios o empresas.
  - Criptografía: Es un método para agregar seguridad a los datos ya que este lo vuelve ilegibles para las personas y se necesita una clave para poder descifrarlos y entenderlos.
  - Seguridad y fortificación de redes: Está en mantener a salvo una red ya que es un tipo muy común de ataque.
  - Seguridad en aplicaciones informáticas,programas y bases de datos:
     Esta área está enfocada en que los programas informáticos y donde se almacenen sus datos sean resistentes ante ataque intencionados o no intencionados.
  - Gestión de seguridad en equipos y sistemas informáticos: Esta se encarga más del nivel de hardware y vulnerabilidades que se pueden encontrar en estos.
  - **Informática forense:** Es una área más especializada en la investigación, suele usarse herramientas más profesionales.

- **Ciberdelito, ciberseguridad:** Es una área más enfocada en la manera en cómo se realizan los ataques cibernéticos y cómo pueden evitarse.
- 2. Describa los siguientes términos (áreas de la seguridad de la información).
  - Gestión de la seguridad de la información: Esta área suele estar destinada a una empresa ya que se encarga de mantener seguridad y administrar los datos que está almacena.
  - Asesoría y auditoría de la seguridad: Suelen ser personas especializadas en ataques y verifican el nivel de seguridad de una empresa o sistema.
  - Análisis y gestión de riesgos: Se encarga de gestionar los riesgos que pueden producir posibles fallos en el sistemas y cómo controlarlos o priorizarlos.
  - **Continuidad de negocio:** Se trata de anticipar problemas informáticos que puedan afectar la entrega de productos y servicios de una empresa o negocio.
  - **Buen gobierno:** Se encargan de mantener seguros datos del gobierno o estado a nivel militar.
  - Comercio electrónico: Son los encargados de mantener seguras las cuentas bancarias y transacciones que se realizan en algún sistema económico.
  - Legislación relacionada con seguridad:
- 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 función de procesamiento que se puede aplicar es usar un caracter en lugar del espacio como una "x" o otra que confunda mas el mensaje, debido a que fue cambiado para ser más ilegible es más complicado volver a obtener el texto original.
- 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 está compuesta por 3 ruedas que se encargan de cifrar el mensaje, para poder empezar a cifrar el mensaje se debe tener un clave que indica la posición inicial de las 3 ruedas así como el orden indicado en números romanos. Cada vez que se registra una tecla esta pasa por la primera rueda que realizará el cambio ajustado y rotan una posición, luego lo pasará a la siguiente rueda, en dicha rueda se realizará su cambio ajustado y se rotará una posición si la primera rueda ya dio una vuelta, luego lo pasa a la tercera está realizara su cambio y rotará si la segunda rueda ya dio un vuelta, por ultimo la ultima rueda pasa el valor al reflector que se encargará mostrar el cifrado final.







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

UNICODE-8 sirve para que los caracteres como 'ABCDE' puedan ser entendidos por la computadora que solo entiende números, para ser exactos solo 1s y 0s pero los números pueden ser representados en números binarios. Entonces lo que hace UNICODE-8 es asignarle un número específico a cada carácter para que pueda ser entendido por la máquina, antes de UNICODE-8 se usaban distintos números para representar los caracteres y era complicado pasar mensajes en computadoras con diferentes configuraciones.