Práctica 1: Introducción a la Criptografía

Seguridad de Sistemas Informáticos

Resumen

Esta práctica tienen por objetivo ilustrar la necesidad de algunas cuestiones básicas de la Criptografía. Para ello primero se introducen algunas cuestiones sobre vulnerabilidades actuales. Posteriormente se usan las plataformas `http://www.cryptool-online.org/`,`http://www.cryptoprograms.com`. Concretamente se trabajará con los elementos de Criptografía clásica y el análisis de frecuencias.

0.1. Descripción

El concepto de vulnerabilidad es muy amplio. Para ilustar esta cuestión se presentará una herramienta de búsqueda Google Dorks y algunos repositorios asociados a Certs de seguridad que recopilan y gestionan las vulnerabilidades que se van reportando de acuerdo con las directrices CVE.

CrypTool-Online y cryptoprograms son plataformas de e-learning de herramientas criptográficas, con el objetivo de posibilitar al público en general aplicar y analizar los principales algoritmos criptográficos de manera sencilla. En esta primera práctica se persigue sobre todo la familiarización con la herramientas y la adquisición de conceptos básicos relacionados con la protección de la confidencialidad.

0.2. Desarrollo

0.3. Vulnerabilidades

La técnica de utilizar las búsquedas avanzadas de los buscadores es una herramienta realmente útil a la hora de buscar vulnerabilidades o recursos. Podemos explotar las capacidades de búsqueda que se nos presentan para sacarle el máximo provecho. En esta parte de la práctica vamos a trabajar concretamente con las búsquedas de Google. Para ello se proponen una serie de búsquedas en las que se deben de explicar por un lado los parámetros de la búsqueda y por otro los resultados obtenidos.

- allinurl:"admin.php"
- intext:"please find attached" "login"| password ext:pdf
- intitle:index.of id_rsa-id_rsa.pub
- camera linksys inurl:main.cgi
- En Google Hacking Database puedes encontrar una base de datos con google dorks clasificados por tipos. Accede a su web, mediante el enlace `https://www.exploit-db.com/google-hacking-database/`, revisa la base de datos comentada, selecciona al menos 3 búsquedas y explica sus parámetros y sus resultados. Recuerda añadirlo al entregable.

Incibe incluye un Cert (Computer Emergency REsponse Team) de Seguridad e Industria `https://www.incibe-cert.es/`. Si entras en el apartado de alertas y vulnerabilidades verás los avisos de seguridad ordenados cronológicamente. Realiza una búsqueda de al menos una vulnerabilidad asociada a cifrado, otra a integridad y otra a autenticación.

0.3.1. Criptografía Clásica

1. Conéctate al sitio web `http://www.cryptool-online.org/`.
2. Comenzamos con el Cifrado de César. Consulta su descripción.

3. Sigue los pasos necesarios para cifrar el siguiente texto con el cifrado de César: “Holmes had been seated for some hours in silence with his long, thin back curved over a chemical vessel in which he was brewing a particularly malodorous product. His head was sunk upon his breast, and he looked from my point of view like a strange, lank bird, with dull gray plumage and a black top-knot. ”So, Watson,“ said he, suddenly, ”you do not propose to invest in South African securities” Extracto de The Adventure Of The Dancing Men, Arthur Conan Doyle.

4. Define cuál sería la expresión matemática asociada al Cifrado de César.

5. Los siguientes criptogramas se han obtenido realizando una sustitución monoalfabética en la que el desplazamiento no siempre es el utilizado por el cifrado de César. El texto en claro está escrito en inglés.

   - (a) PBZ CHG REF PNA ORN CNV AVA GUR OEN VA
   - (b) GZZG IQOT ZNKK BKTO TMUX GZJG CT.
   - (c) WKHHP SHURU KDVEH HQDVV DVVLQ DWHG

6. Ve al apartado de cifrados de sustitución monoalfabética en CyptTool Online ¿Es el cifrado de César un cifrado monoalfabético?

7. Pasamos ahora a analizar el cifrado multiplicativo. Ve al apartado correspondiente en el mismo sitio web. Usando el alfabeto que está por defecto intenta descifrar el criptograma: qtFyKycK yc FVm PayFV FVaF hmaJc FQ agVymLmKmnF. NQFVyns gan Dm JQnm oyFVQiF VQtm anJ gQnPyJmngm . Observa cuáles on las las claves que están disponibles para descifrar ¿Qué propiedad cumplen?

8. El cifrado de Vigenere es una sustitución polialfabética periódica. Consulta en CrypTool-Online cómo funciona y obtén el cifrado del texto DESASTRE NUCLEAR EN MURUROA con clave SOS

9. Descifra con Vigenere IIELD QJEIC DUWWO MBURA FWLBU, sabiendo que la clave ha sido WINDOWS.

10. ¿Cuál es la expresión matemática que define el cifrado de Vigenere?

11. Usa el servicio web `cryptoprograms.com` para cifrar usando Playfair LA SOMBRA DEL VIENTO con la clave DANIEL SEMPERE.

12. Descifra usando el servicio web anteriorla siguiente cadena de texto difrada con Playfair FP LV MT SO RH LB VN con la clave EVANESCENCE.

13. Visualiza el vídeo `http://youtu.be/G2_Q9FoD-oQ`. En él encontrarás cómo funciona la máquina de cifrado Enigma. Compara la descripción dada allí con la ofrecida en la web de Cryptool Online.

0.4. Entrega

Debes desarrollar un informe que contenga las respuestas a las cuestiones planteadas en la práctica y generar un archivo pdf que deberás subir a la tarea habilitada en el aula virtual.