Universidad del País Vasco Euskal Herriko Unibertsitatea | BILBOKO INGENIARITZA ESKOLA ESCUELA DE INGENIERÍA DE BILBAO

Sistemas de Gestión de Seguridad de la Información 2023/2024

Laboratorio 1 – Cifrado I

Objetivos:

1. Aprender a manejar algunas técnicas básicas de cifrado y ocultación de la información.
2. Aprender algunas de las técnicas de criptoanálisis existentes.
3. Comprender algunas de las utilidades de las funciones de resumen criptográfico.

Recursos necesarios:

- Ubuntu (Usuario/password: lsi/lsi).
- Archivos en eGela, en la carpeta “Laboratorio 1 – Cifrado I”.

Índice:

1.- Criptoanálisis mediante análisis de frecuencias

Crea un programa que descifre el siguiente mensaje mediante análisis de frecuencias (El mensaje original está en castellano):

RIJ AZKKZHC PIKCE XT ACKCUXJHX SZX, E NZ PEJXKE, PXGIK XFDKXNEQE RIPI RIPQEHCK ET OENRCNPI AXNAX ZJ RKCHXKCI AX CJAXDXJAXJRCE AX RTENX, E ACOXKXJRCE AXT RITEQIKERCIJCNPI OKXJHXDIDZTCNHE AX TE ACKXRRCIJ EJEKSZCNHE.

AZKKZHC OZX ZJ OERHIK AX DKCPXK IKAXJ XJ XT DEDXT AX TE RTENX IQKXKE XJ REHETZJVE XJ GZTCI AX 1936. DXKI AZKKZHC, RIPI IRZKKX RIJ TEN DXKNIJETCAEAXN XJ TE MCNHIKCE, JI REVI AXT RCXTI. DXKNIJCOCREQE TE HKEACRCIJ KXvITZRCIJEKCE AX TE RTENX IQKXKE. NZ XJIKPX DIDZTEKCAEA XJHKX TE RTENX HKEQEGEAIKE, KXOTXGEAE XJ XT XJHCXKKI PZTHCHZACJEKCI XJ QEKRXTIJE XT 22 AX JIvCXPQKX AX 1936, PZXNHKE XNE CAXJHCOCRERCIJ. NZ PZXKHX OZX NCJ AZAE ZJ UITDX IQGXHCvI ET DKIRXNI KXvITZRCIJEKCI XJ PEKRME. NCJ AZKKZHC SZXAI PEN TCQKX XT REPCJI DEKE SZX XT XNHETCJCNPI, RIJ TE RIPDTCRCAEA AXT UIQCXKJI AXT OKXJHX DIDZTEK V AX TE ACKXRRCIJ EJEKSZCNHE, HXKPCJEKE XJ PEVI AX 1937 TE HEKXE AX TCSZCAEK TE KXvITZRCIJ, AXNPIKETCLEJAI E TE RTENX IQKXKE V OERCTCHEJAI RIJ XTTI XT DINHXKCIK HKCZJOI OKEJSZCNHE.

PISTA: Diapositiva 23 de tema “Cifrado simétrico”

2.- Esteganografía y algoritmos resumen

Hay un mensaje importante de Buenaventura Durruti para vosotros en una de las imagenes del directorio **imagenes.zip** disponible en eGela. El mensaje ha sido introducido mediante el programa Stegosuite de Ubuntu, sin contraseña. La imagen que contiene el mensaje se corresponde con el Hash (MD5) **e5ed313192776744b9b93b1320b5e268**. ¿Qué archivo es? ¿Qué dice la frase?

Sistemas de Gestión de Seguridad de la Información 2023/2024

Si quieres escribir un mensaje secreto en una imagen, y garantizar al destinatario que nadie lo ha modificado, ¿Qué pasos seguirías?

¿Sería posible incorporar en el contenido de un fichero su propio resumen criptográfico? Esto es, ¿Podría ponerse en el texto de este enunciado el resumen criptográfico que le corresponda al propio enunciado para que pudiérais comprobar su autenticidad?