Identificación de texto: la identificación de un fichero como tipo texto y la subclasificación del mismo en base a diferentes criterios.

Segurmática Antivirus: software antivirus desarrollado por la Empresa de Consultoría y Seguridad Informática Segurmática.

Regla: criterio de búsqueda empleado para subclasificar los ficheros de texto de forma rápida o más certera.

Identificación de patrones: la detección de cierta regla en el contenido de los ficheros.

Formatos contenedores: Son formatos que permiten almacenar contenidos en el mismo, por ejemplo los ficheros .RAR permiten almacenar ficheros y carpetas, los instaladores (ej: .MSI) también, ficheros .DOC también permiten almacenar contenido (ej: Macros, Binarios, etc…).

Formatos empaquetados: Son formatos cuyo contenido original se encuentra protegido, ya sea compactado, encriptado u ofuscado, ejemplo UPX, AS-PACK.

ROP (Return Oriented Programming): Técnica que utiliza la pila de llamada de ensamblador para ejecutar código antes de retornar de un llamado.

Fichero PE y ELF: Formatos de ficheros binarios de Windows y Linux respectivamente. Algunos ejemplos de extensiones que utilizan en Windows: .exe, .dll, .sys, .scr, en Linux: .a, .o, sin extensión.

Antivirus: Aplicación o grupo de aplicaciones dedicadas a la prevención, búsqueda, detección y eliminación de programas malignos en sistemas informáticos.

Programas malignos: Cualquier programa que tiene un objetivo poco ético o ilegal, como virus, troyanos, espías, etc.

Firma digital: La firma digital es el equivalente electrónico de la firma manuscrita. Se trata de un modelo estructurado que permite autenticar el origen y el contenido de un mensaje (validando su integridad), de forma tal que pueden ser comprobados por un tercero. Puede ser vista como una secuencia de bits asociada indisolublemente a un mensaje, y que sólo puede ser generada por el titular legítimo.

FPGA: Son las siglas de Field Programmable Gates Array (Arreglo de Compuertas Programables "en el Campo de aplicación"). Se trata de una tecnología de dispositivos de hardware que permite a los desarrolladores reprogramar las aplicaciones después de su fabricación cada vez que sea necesario (siendo esta una gran ventaja y la característica más distintiva), y además se pueden utilizar para diseñar la mayoría de los tipos de circuitos de aplicación específica en un corto tiempo de desarrollo.

Microblaze: Este es un microprocesador de propósito general de tipo RISC (Reduced Instruction Set Computer) optimizado para las FPGA de la compañía Xilinx. Este procesador es de tipo softcore, puede ser reprogramado, y brinda la posibilidad de configurar recursos como

multiplicadores, desplazadores y conexiones a diferentes buses en dependencia de los requerimientos del trabajo realizado.

La **criptografía simétrica** es un método criptográfico en el cual se usa una misma clave para cifrar y descifrar mensajes. Las dos partes que se comunican han de ponerse de acuerdo de antemano sobre la clave a usar. Una vez ambas tienen acceso a esta clave, el remitente cifra un mensaje usándola, lo envía al destinatario, y éste lo descifra con la misma.

Advanced Encryption Standard (**AES**), también conocido como **Rijndael** (pronunciado "Rain Doll" en inglés), es un esquema de cifrado por bloques adoptado como un estándar de cifrado por el gobierno de los Estados Unidos. El AES fue anunciado por el Instituto Nacional de Estándares y Tecnología (NIST) como FIPS PUB 197 de los Estados Unidos (FIPS 197) el 26 de noviembre de 2001 después de un proceso de estandarización que duró 5 años. Se transformó en un estándar efectivo el 26 de mayo de 2002. Desde 2006, el AES es uno de los algoritmos más populares usados en criptografía simétrica. El cifrado fue desarrollado por dos criptólogos belgas, Joan Daemen y Vincent Rijmen, ambos estudiantes de la *Katholieke Universiteit Leuven*, y enviado al proceso de selección AES bajo el nombre "Rijndael".

En el artículo se refiere a **GOT-28147**, El algoritmo de cifrado simétrico GOST, fue publicado en 1990 como el EstándarSoviético (GOST 28147-89). El algoritmo provee un nivel de seguridad de la información flexible, que le permite ser utilizado para proteger información en sistemas de computadoras y redes de computadoras. Además este algoritmo puede ser implementado tanto en software como en hardware.

software libre: es la denominación del software que respeta la libertad de todos los usuarios que adquirieron el producto y, por tanto, una vez obtenido el mismo puede ser usado, copiado, estudiado, modificado, y redistribuido libremente de varias formas.

Nova Distribución Cubana de GNU/Linux es una distribución de GNU/Linux desarrollada en la Universidad de las Ciencias Informáticas con razón de apoyar la migración del país a tecnologías de Software Libre y Código Abierto.

El **código fuente** de un programa informático (o software) es un conjunto de líneas de texto que son las instrucciones que debe seguir la computadora para ejecutar dicho programa. Por tanto, en el código fuente de un programa está escrito por completo su funcionamiento.

Autor: MsC Julio César Jerez Camps.