Área Académica: Computación

Tema: Seguridad en Redes

Profesor: M. en C. Luis Rodolfo Coello Galindo

Periodo: Julio – Diciembre de 2013

Tema: Network Security

Abstract

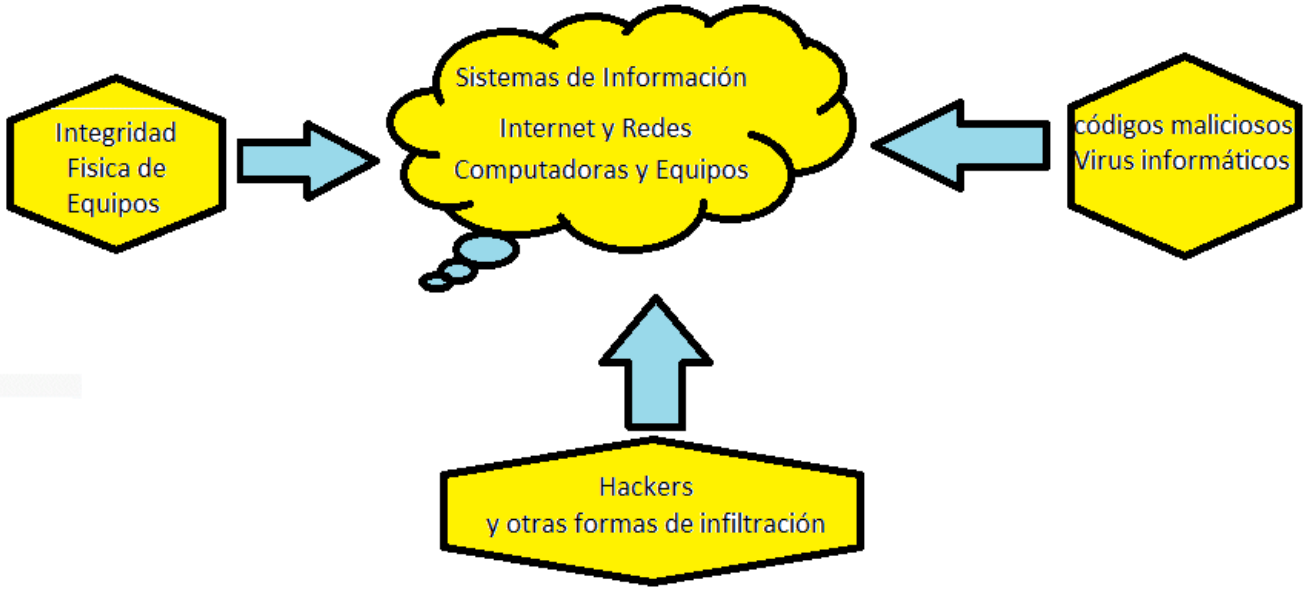
The network security comprises an area of interest in the world of information technology and computing. That´s why it is important to know the functioning of the different methods and algorithms implemented nowadays, for encryption and data coding

Keywords: Algorithms, Data coding.

Escuela Superior de Tizayuca

Introducción

Empresas, organizaciones y cualquier persona que utiliza dispositivos de comunicación de datos, envía y recibe correos electrónicos, comparte información de manera local o a nivel mundial, realiza transacciones, ofrece servicios y encuentra soluciones a sus requerimientos.



Vulnerabilidad en redes

Codificación -Encriptación

- Blindaje (encriptación) Vs. Codificación

- Codificación: es el método que permite convertir un carácter de un lenguaje natural (alfabeto o silabario) en un símbolo de otro sistema de representación (sistema binario).

- Encriptación: método que permite representar un lenguaje natural (alfabeto) en otro distinto sin cambiar su representación.

Escuela Superior de Tizayuca

Finalidad:

- Garantizar el secreto en la comunicación entre dos o más entidades (personas, organizaciones, etc.)
- Asegurar que la información que se envía es autentica en un doble sentido: que el remitente sea realmente quien dice ser.
- Impedir que el contenido del mensaje enviado (criptograma) sea modificado en su tránsito.

Escuela Superior de Tizayuca

- Técnica de encriptación o criptografía de datos.

- Encriptación, del griego *krypto* (oculto) y *graphos* (escribir), es la técnica de alterar la representación lingüística de mensajes, mediante técnicas de cifrado para hacerlos ininteligibles a intrusos que intercepten estos mensajes.

confidencialidad !!!

Escuela Superior de Tizayuca

Escuela Superior de Tizayuca

Seguridad de datos

- Método de sustitución mono-alfabética.
- Método por sustitución poli-alfabética.

Método de transposición mono alfabética

- Este sistema se basa en el método de sustitución mono alfabética, es decir, el proceso de sustitución se lleva a cabo en cada uno de los elementos del texto.

- Funcionamiento: a cada letra le corresponde la que está 3 posiciones por delante en un proceso circular que recorre todo el alfabeto.

Escuela Superior de Tizayuca

Método de transposición mono- alfabética

Paso #1: definir la longitud de nuestro alfabeto

{a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v, w, x, y, z} = 26 caracteres.

Paso #2: generación del mensaje(*M*): {hola}

Paso #3: implementar la regla de cesar: corrimiento de 3 posiciones por delante de todo el alfabeto en un proceso cíclico.

Paso #4: obtención del mensaje encriptado (ME): {krod}

Escuela Superior de Tizayuca

Método por sustitución poli-alfabética.

- Variante del método simple o mono-alfabético.
- Implementa el principio de corrimiento pero en orden diferente.
- Implementa la creación de tramas o paquetes de información.

Escuela Superior de Tizayuca

Método por sustitución poli-alfabética.

Paso #1: definir la longitud de nuestro alfabeto

{a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v, w, x, y, z} = 26 caracteres.

Paso #2: generación del mensaje a enviar (M):{polialfabetica}.

Paso #3: generación de trama sobre (M): 8 caracteres.

Trama #1:{polialfa}; Trama #2:{betica}

Paso#4: asignación de corrimientos cíclico sobre cada carácter de cada una de las tramas asignadas.

Trama #1:

p	1 (Izq o der)
o	2 (Izq o der)
l	3 (Izq o der)
i	4 (Izq o der)
a	5 (Izq o der)
l	6 (Izq o der)
f	7 (Izq o der)
a	8 (Izq o der)

Escuela Superior de Tizayuca

Método por sustitución poli-alfabética.

Trama #2

b	1 (Izq o der)
e	2 (Izq o der)
t	3 (Izq o der)
i	4 (Izq o der)
c	5 (Izq o der)
a	6 (Izq o der)

----------	

paso #4: realizar el corrimiento asignado para cada trama sobre el alfabeto.

Paso #5:obtención del mensaje encriptado (*ME*)

Escuela Superior de Tizayuca

Codificación

- Es el proceso por el cual la información de una fuente es convertida en símbolos para ser transmitida a través de un canal de comunicación de datos.
- En sistemas de comunicación de datos digitales, se implementa el código binario (0,1)
- Existen muchas técnicas o métodos para codificación de datos → código Huffman

Escuela Superior de Tizayuca

Código Huffman

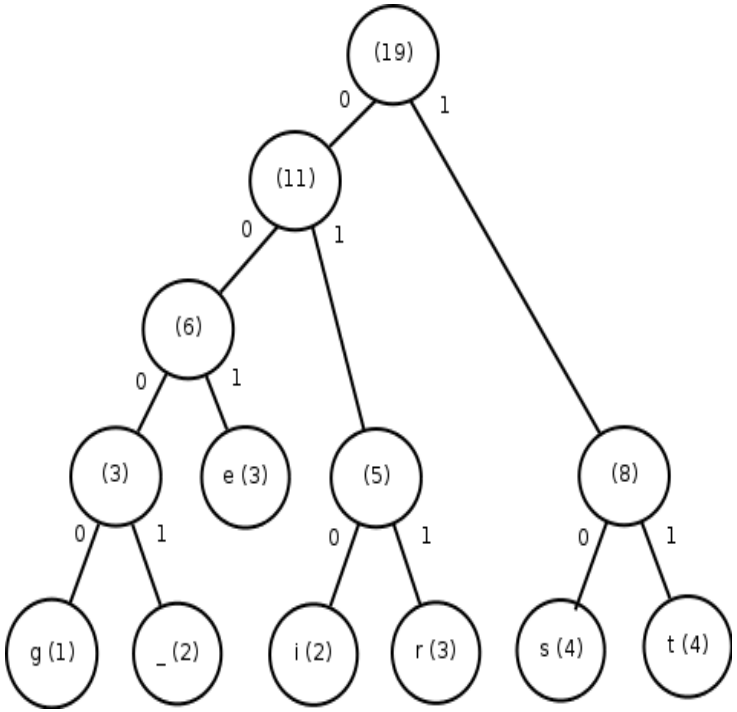
- Es un método usado para compresión de datos. El término se refiere al uso de una tabla de códigos de longitud variable para codificar un determinado símbolo (como puede ser un carácter en un archivo), donde la tabla ha sido rellenada de una manera específica basándose en la probabilidad estimada de aparición de cada posible valor de dicho símbolo.

Escuela Superior de Tizayuca

Código huffman

Descripción del algoritmo:

El algoritmo consiste en la creación de un árbol binario que tiene cada uno de los símbolos por hoja, y construido de tal forma que siguiéndolo desde la raíz a cada una de sus hojas se obtiene el código Huffman asociado.



Escuela Superior de Tizayuca

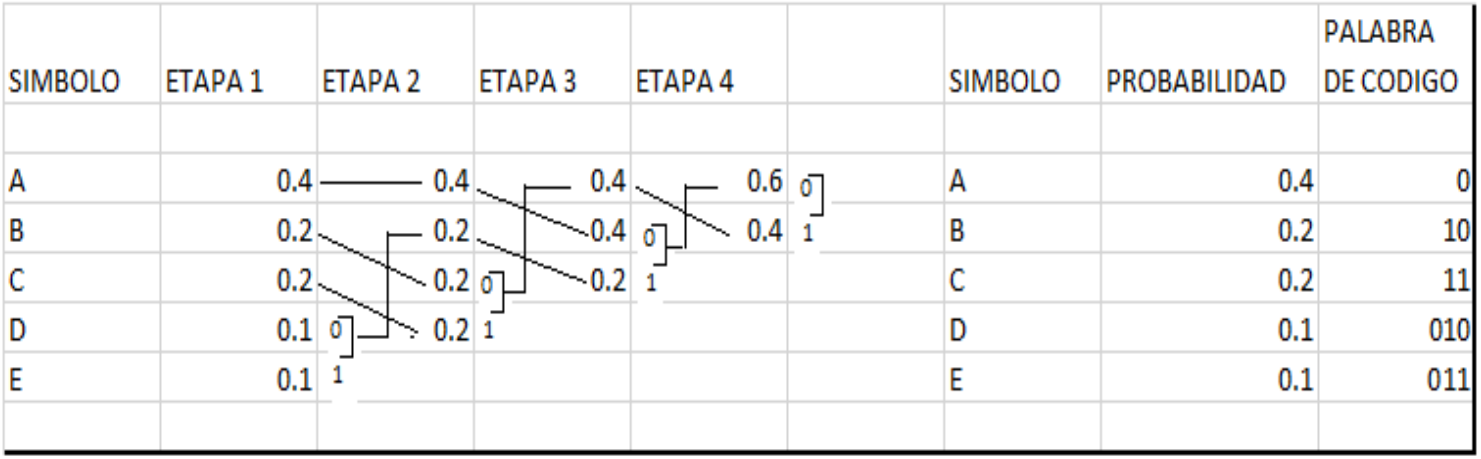
Funcionamiento:

- Los símbolos de la fuente se listan en orden de probabilidades decrecientes. A los dos símbolos de probabilidad más baja (penúltimo y ultimo) se le asignan un 0 y un 1, respectivamente.
- Estos dos símbolos se consideran como si se combinaran en un nuevo símbolo de fuente con probabilidad igual a la suma de las dos probabilidades originales. La probabilidad obtenida se pone en la lista de acuerdo con su valor.
- El procedimiento se repite hasta que nos quedamos con la lista final de las únicos símbolos, a los cuales se les asignarán un 0 y un 1.
- El código para cada símbolo se determina procediendo hacia atrás y siguiendo la frecuencia de ceros y unos asignados a cada símbolo.

Escuela Superior de Tizayuca

Ejemplo árbol de Huffman

- Se consideran cinco símbolos del alfabeto de una fuente discreta sin memoria, cuyas probabilidades se enlistan a continuación, obtener la codificación de cada símbolo, la longitud promedio y la entropía.



SIMBOLO	ETAPA 1	ETAPA 2	ETAPA 3	ETAPA 4		SIMBOLO	PROBABILIDAD	PALABRA DE CODIGO
A	0.4	0.4	0.4	0.6	0	A	0.4	0
B	0.2	0.2	0.4	0.4	1	B	0.2	10
C	0.2	0.2	0.2			C	0.2	11
D	0.1	0.2				D	0.1	010
E	0.1					E	0.1	011

Escuela Superior de Tizayuca

Bibliografía

Herrera E. y Herrera Pérez E. (2003). Tecnologías y redes de transmisión de datos. México, DF: Editorial Limusa.

Stallings, William. (2000).Comunicaciones y Redes de computadoras. Madrid, España: Editorial Prentice Hall.

Salomon, D. (2004). Data Compression, 3rd Edition. United States: Editorial Springer.

Tanenbaum, A. S. (2003). Redes de Computadoras 4ª edición. México, DF: Editorial Pearson Educación.

Escuela Superior de Tizayuca