ACADEMIA DE CIENCIAS DE MORELOS, A.C.

¿Comentarios y sugerencias?, ¿Preguntas sobre temas científicos? CONTÁCTANOS:
edacmor@ibt.unam.mx

¿Cómo evitar ser incluido en el portal de WikiLeaks? Historia Breve de la Criptografía

Parte I

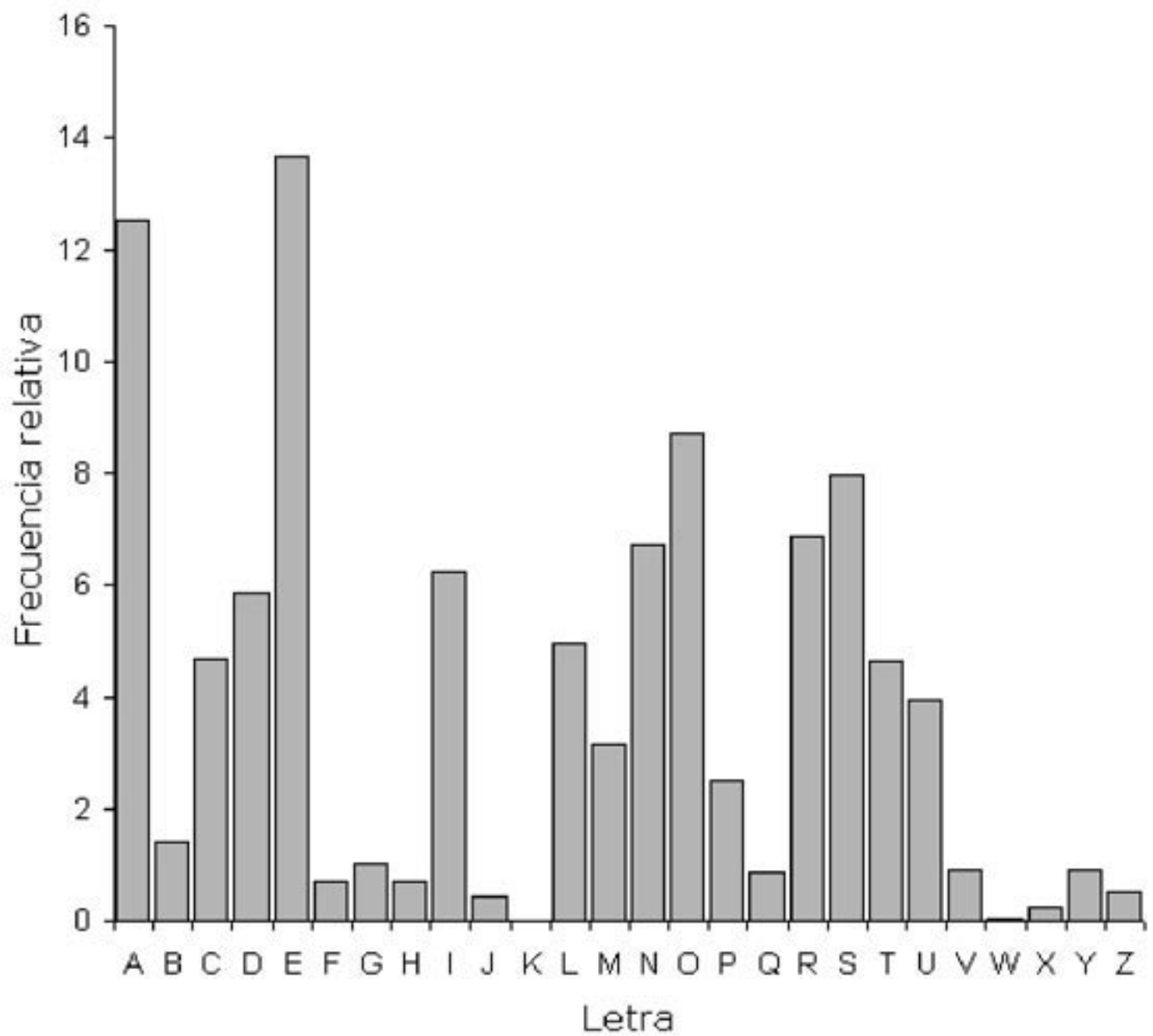
L. Enrique Sucar *(INAOE), Miembro de la Academia de Ciencias de Morelos*
Edgar A. Sucar (estudiante de preparatoria)

Recientemente han salido a la luz pública una serie de comunicaciones, en principio "secretas", a través del célebre portal de *WikiLeaks*. ¿Es posible evitar que la información sea conocida por personas a las que no va dirigida? Desde de la antigüedad ha existido la preocupación de que cierta información delicada no caiga en manos enemigas. En el año 480 AC., Damaratus advirtió a los griegos de una invasión por el ejército Persa, a través de un mensaje en una tabla cubierta con cera, de forma que aparentemente no había nada escrito en la tabla, pudiendo pasar el mensaje inadvertido hasta llegar a su destino. Al remover la cera se reveló el mensaje, lo que permitió a los griegos prepararse; los persas perdieron el elemento sorpresa y fueron derrotados. Damaratus utilizó lo que se conoce como estenografía, escondiendo el contenido del mensaje. Actualmente se usa la *estenografía* para esconder mensajes en imágenes para que, por ejemplo, puedan ser identificadas por el autor.

Otra manera de ocultar un mensaje es haciendo inaccesible su significado, mediante lo que se conoce como *criptografía*. Ésta consiste básicamente cambiar los caracteres del mensaje por otros con base en cierto protocolo, acordado de antemano entre el autor y el destinatario. De esta forma, aunque todos pueden "leer" el mensaje, sólo los que conocen el protocolo pueden entenderlo. Así puedo incluir un mensaje secreto en este artículo: "UIUOPYTU OP ITPZITUE OP YADPXAE", utilizando *cifrado por sustitución*.

El *cifrado por sustitución* consiste en reemplazar cada letra en el mensaje por otra, de acuerdo a cierta clave en la que se indica la correspondencia entre cada letra en el mensaje original, con otra letra en el mensaje cifrado. Por ejemplo: a—X, b—L, c—R, d—P, ..., i—Q, ..., o—A, ..., s—M, ..., z—T (en minúsculas las letras originales y en mayúsculas las del código). De acuerdo a este código, la palabra "XPQAM" quiere decir "adiós". Para poder interpretar el mensaje, el destinatario debe conocer la secuencia de letras del código que corresponde al alfabeto, lo que se conoce como *la llave*. Una persona que intercepte nuestro mensaje podría intentar descifrarlo probando con todas las posibles *llaves*, que son del orden de 400,000,000,000,000,000,000,000,000 (considerando un alfabeto de 26 caracteres). Si le tomara un segundo probar cada posible *llave*, ¡le tomaría mil millones de veces el tiempo estimado de vida del universo descifrar el mensaje! El cifrado por sustitución fue utilizado por el emperador romano Julio César, siendo un medio confiable para codificar mensajes por cerca de mil años.

Mientras un grupo de personas diseñan métodos para cifrar los mensajes, otro grupo busca como descifrarlos, lo que se conoce como *criptoanálisis*. La historia de la criptografía es básicamente una competencia entre los que diseñan los códigos y los que intentan descifrarlos, con periodos en que dominan unos u otros. Después de un largo periodo en que el *cifrado por sustitución* era aparentemente infalible, los árabes lograron romper el código mediante una brillante combinación de estadística y lingüística. En vez de probar todas las posibles *llaves*, la clave del método para descifrarlos se basa en la observación de que en cada lenguaje ciertas letras tienden a ser más frecuentes que otras. Con base en el análisis de muchos textos en español, podemos estimar la frecuencia de cada letra del alfabeto, *ver Figura*. Al comparar las frecuencias de las letras en el código con las del alfabeto, se pueden identificar algunas letras; éstas se reemplazan en el mensaje en lo que se logran identificar otras, hasta llegar a descifrar el mensaje (trata de descifrar el mensaje secreto). Un caso famoso del uso del criptoanálisis es el de "Mary, Queen of Scots", quien fue condenada a muerte en 1570, al ser descifradas las comunicaciones secretas que mantenía con un grupo de



Frecuencia relativa de las diferentes letras en textos en español.

¿Comentarios y sugerencias?, ¿Preguntas sobre temas científicos? CONTÁCTANOS:
edacmor@ibt.unam.mx

conspiradores católicos, que planeaban el asesinato de la reina Isabel de Inglaterra.

Una vez roto el método anterior, se creó un método más seguro basado en el mismo, pero utilizando más de un alfabeto. Por ejemplo, si se tienen dos alfabetos (A, B), la primera letra del mensaje se codifica con el alfabeto A, la segunda con el B, la tercera con el A, y así sucesivamente. Con esto, cada letra puede tener diferentes códigos y ya no es posible usar las frecuencias para descifrar el mensaje. Esta idea fue perfeccionada en Francia por Vigenere, mediante un sistema de 26 alfabetos con 26 letras cada uno, donde cada alfabeto es igual al anterior desplazado por una letra. El mensaje se codifica con una combinación de varios alfabetos que se seleccionan con una palabra *llave*, que indica la primera letra de cada alfabeto seleccionado. El *cifrado indescifrable* de Vigenere permaneció inaccesible por 200 años, y se volvió muy importante al surgir las comunicaciones electrónicas como el telégrafo y la radio, donde la necesidad de mantener la seguridad se hizo más evidente. Eventualmente, a finales del siglo XIX, fue descifrado por el inventor inglés Charles Babagge. La clave para romper el código es buscar palabras cortas frecuentes, como "de", que dada la naturaleza cíclica del código, aparecen codificadas de la misma manera dentro del texto: con esto es posible encontrar la llave y así descifrar el mensaje. Así es como los ingleses lograron descifrar un telegrama alemán dirigido al Presidente de México durante la Primera Guerra Mundial, en que lo invitaba a aliarse contra EUA: esto aceleró el que los Estados Unidos intervinieran en la guerra en Europa y la eventual derrota de Alemania.

El desarrollo de la tecnología en el siglo XX llevó a la automatización de la criptografía, siendo la *Enigma* la máquina criptográfica más celebre, utilizada por los alemanes durante la segunda guerra mundial. La *Enigma* es como una máquina de escribir donde se escribe el mensaje, que luego pasa por un disco que conecta las letras de la entrada con otras en la salida, que se muestran iluminando la letra correspondiente. Para hacer más difícil descifrar el mensaje se utilizan tres discos, y además las posiciones de cada uno van cambiando, rotando después de que cada letra es tecleada. La *llave* en este caso da la posición inicial de los discos, los cuales son móviles, de forma que aunque se tenga la máquina no se puede descifrar el mensaje si no se conoce la *llave*. Mediante un esquema de reflexión, la misma máquina puede ser utilizada para cifrar y descifrar los mensajes; y fue utilizada con éxito por los alemanes en la primera parte de la guerra. Dada la importancia de poder descifrar los mensajes del enemigo, los ingleses juntaron un grupo de destacados científicos, liderados por Alan Turing, quienes lograron eventualmente romper la *Enigma*, lo que contribuyó a la victoria aliada en la Segunda Guerra Mundial; y además al desarrollo de las computadoras.

La principal limitación de todos los métodos anteriores es que se requiere de una *llave privada*: si el enemigo llega a conocer esta llave se pierde el secreto. El avance más importante en la historia de la criptografía es la llave pública, con lo que incluso si se conoce la llave es prácticamente imposible descifrar el mensaje. Si quieres conocer el significado del mensaje secreto y cómo funciona la llave pública, no te pierdas la segunda parte de la historia de la criptografía en esta misma columna.

Para actividades recientes de la Academia y artículos anteriores puede consultar: www.acmor.org.mx

Universidad Autónoma del Estado de Morelos

Facultad de Ciencias

La Secretaría Académica
La Facultad de Ciencias,
Facultad de Ciencias Químicas e Ingeniería (FCQel), y
La Dirección de Educación Superior
de la UAEM

CONVOCAN

A LOS ESTUDIANTES DE NIVEL MEDIO SUPERIOR (Bachillerato, Preparatoria), A PARTICIPAR EN LA

XIX Olimpiada Estatal de Física 2011

Que se celebrará el SÁBADO 21 de mayo a las 10:00 horas en 3 sedes:

Requisitos:
Los estudiantes a concursar deberán estar inscritos a lo más en el cuarto semestre de nivel medio superior y haber nacido después del 1 de julio de 1992. Máximo 10 estudiantes por escuela.
Fecha límite para inscripción: siete días antes del concurso

Sede Región Norte: ***Grupo Educativo Cristóbal Colón*** Av. Morelos 345, Col. Centro Cuernavaca, Morelos *www.cristobalcolon.edu.mx* Tel. (777)318 57 07 ext. 110 y 127	Director de Preparatoria: MA Javier Vázquez López *dirtec-prepa@cristobalcolon.edu.mx* Coordinadora Regional: IQ Fabiola Brito Paulino *fabibp11@hotmail.com*
Sede Región Oriente: ***Escuela "El Peñón"*** Ex-hacienda Montefalco s/n, Col. Santa Clara Jonacatepec, Morelos *www.elpenon.org.mx* Tel. (735)355 03 43 ext. 113	Director: MC José Emmanuel Hernández Guzmán *joseemmhdz@yahoo.com.mx* Coordinador Regional: Ing. Erasmo Arrenchú Paredes *erasrench@yahoo.com.mx*
Sede Región Sur: ***Colegio de Bachilleres del Estado de Morelos Plantel 08, Tehuixtla (CoBaEM 08)*** Av. Adolfo López Mateos s/n, Col. La Azuchilera, Tehuixtla Jojutla, Morelos *www.cobaem.edu.mx* Tel. (734)341 02 24	Directora: Biol. Ma. Estela Aranda Figueroa *earanda@cobaem.edu.mx* Coordinador Regional: Ing. Mauricio Mejía Ramírez *mauromejia5@hotmail.com*

Temario del Examen:

- Vectores, Operaciones geométricas y analíticas
- Cinemática
- Movimiento rectilíneo uniforme y uniformemente acelerado
- Movimiento circular uniforme
- Dinámica. Leyes de Newton
- Trabajo, energía y potencia

Los resultados serán publicados A MÁS TARDAR 10 días hábiles después del concurso en el portal de olimpiadas:
www.uaem.mx/olimpiadas
Premiación a los primeros lugares el día 14 de junio a las 10:00 horas en el Auditorio "Emiliano Zapata" de la UAEM
Los ganadores podrán asistir a un curso de entrenamiento por catedráticos de la Facultad de Ciencias, al final del cual se elegirá a la delegación que representará a Morelos en la XXII Olimpiada Nacional de Física a celebrarse en Guadalajara, Jalisco en noviembre próximo.

Inscripciones en **www.uaem.mx/olimpiadas**
Informes en el portal, con los Coordinadores Regionales o al correo: aquino@uaem.mx

No hay costo de Inscripción

Academia de Ciencias de Morelos A.C.

AGEFIS

SMF