Aprendiendo estadística en una red social a través de la criptografía

Learning Statistics in a Social Network Through Cryptography

Texto recibido: 8 de septiembre de 2017
Texto aprobado: 15 de octubre de 2017

Por: Marco Antonio Olivera Villa

Resumen:
El presente trabajo resulta de la utilización de una red social para experimentar, construir y colaborar a distancia, en una serie de actividades didácticas basadas en la criptografía, pero usando herramientas de estadística. La idea básica fue analizar los posibles procesos de aprendizaje e interacción al interior de dicha comunidad de aprendizaje.

Palabras clave: criptografía, estadística, aprendizaje colaborativo, construccionismo, red social.

Abstract:
In this work, we investigated the use of a social network for experimenting, constructing and collaborating –at a distance— on math activities, based on cryptography, but using statistical tools. The basic idea was to analyze the possible processes of learning and interaction within the learning community.

Keywords: *criptography, statistics, collaborative learning, constructionism, social network.*

Introducción

La criptografía es una rama de la ciencia que se dedica a la codificación y decodificación de mensajes, la idea central es enviar información de manera que no sea entendible por terceras personas que pudieran interceptarla. La historia de la criptografía se remonta a los griegos (Fernández, 2004), donde se implementaron diversas metodologías para enviar mensajes secretos, en la segunda guerra mundial se construyeron máquinas que usaban algoritmos muy sofisticados para encriptar o desencriptar mensajes. En la actualidad, la criptografía se usa, por ejemplo, en las transacciones bancarias o en el envío de correos electrónicos.

En esta investigación se pretendió crear una red social conformada por estudiantes del Colegio de Ciencias y Humanidades, la idea fue que propusieran y analizaran criptosistemas, es decir metodologías matemáticas para encriptar o desencriptar mensajes. En este contexto, tal como se verá en las secciones siguientes, la estadística a través del análisis frecuencial tuvo un papel preponderante en las discusiones llevadas a cabo en la comunidad virtual.

En las siguientes secciones: 1) se mencionarán algunos antecedentes y se describirán las actividades de aprendizaje, así como su encuadre en el plan de estudios del CCH, 2) se expondrá el marco conceptual, 3) se explicará la metodología, así como el análisis de resultados y 4) se harán explícitas las conclusiones.

Antecedentes, diseño didáctico y su encuadre en el plan de estudios del CCH

El principal antecedente de este trabajo es una investigación de Massimo M., Fioretto A., Sgarro A. y Zuccheri L. (2002) en donde plantea que la criptografía es un camino estimulante para introducir ideas estadísticas, computacionales, lingüísticas, etcétera. Asimismo, el análisis criptográfico permite que los estudiantes desarrollen habilidades en la solución de problemas. En su investigación describe experiencias didácticas en donde algunos estudiantes proponen criptosistemas de sustitución y sus compañeros deben descifrar dichos criptosistemas a través del análisis de frecuencias, ya sea de forma manual o con tecnología. El trabajo descrito tiene un cierto paralelismo con nuestra propuesta, la cual abordaremos a continuación, primeramente, explicando su encuadre dentro del plan de estudios del CCH.

Las actividades de aprendizaje fueron planeadas para trabajarse con los estudiantes del Colegio de Ciencias y Humanidades, en el curso de Estadística 1, en la primera unidad correspondiente a estadística descriptiva, en particular para encuadrarse en los siguientes aprendizajes, descritos en su plan de estudios (Escuela Nacional Colegio de Ciencias y Humanidades, 2016): 1) valorar la importancia de la recopilación de datos y 2) construir tablas de frecuencias, así como histogramas, gráficas de barras, etc. para representar el comportamiento de las variables. El logro de estos aprendizajes, se valorarán en la sección de conclusiones.

Respecto al diseño didáctico, hubo tres actividades de aprendizaje montadas en una plataforma que contaba con diversas herramientas de colaboración y discusión: mensajero, red social, foros, y repositorio para almacenar diversos tipos de documentos (ver figura 1).

La primera actividad: mensajes secretos, tenía como propósito hacer reflexionar y generar discusiones entre los estudiantes sobre sus posibles conocimientos y experiencias sobre el envío de mensajes secretos y la criptografía, así como cuestionarlos sobre situaciones cotidianas en las que se usa, tales como transacciones bancarias, correo electrónico, etc.

La segunda actividad: ¿Cómo mandarías mensajes secretos? tenía como objetivo dar un impulso inicial a los estudiantes para que comenzaran a crear e intercambiar criptosistemas, a partir de la inventiva propia, pero teniendo a su disposición una serie de recursos proporcionados por el profesor, tales como lecturas, videos y páginas web de diversos criptosistemas sencillos basados en técnicas estadísticas. En específico, el profesor introdujo el criptosistema de sustitución, en el cual cada letra del mensaje original se sustituye por otro carácter. Para este criptosistema, se hace una correspondencia entre la frecuencia ya conocida de las letras en la Lengua Española, y la frecuencia de letras en un mensaje codificado. Por ejemplo, si en la Lengua Española las letras que aparecen con mayor frecuencia son la a, e, i y en un mensaje codificado por sustitución, las letras con mayor frecuencia son l, p, k, se puede establecer una correspondencia, de manera que la letra l es en realidad la letra a, la letra p es en realidad la letra e y la letra k es la letra i. Por lo tanto, este tipo de criptograma requiere un análisis de frecuencias para descifrarlo.

La tercera actividad: encriptando/desencriptando, en esta actividad los estudiantes proponían retos a sus compañeros, dándoles mensajes encriptados y pidiéndoles que los desencriptaran. Se trabajó con el criptosistema de sustitución, descrito en la actividad 2.

Figura 1: Plataforma educativa en donde se montaron las actividades

Resulta básico mencionar que en la plataforma había actividades iniciales propuestas por el profesor y algunas otras, que los mismos estudiantes propusieron; la idea central en el diseño didáctico fue que se creara una comunidad de aprendizaje autosostenible, en el sentido de que fueran los propios alumnos quienes plantearan problemas o retos a sus compañeros, de manera que la comunidad en su conjunto pudiera avanzar en el conocimiento.

Marco conceptual, construccionismo, aprendizaje colaborativo y uso de tecnología

Los pilares pedagógicos bajo los cuales se encuentra esta investigación son los siguientes: el construccionismo, el aprendizaje colaborativo y el papel de la tecnología en el aprendizaje. A continuación, abordaremos cada uno de estos puntos.

La idea central de la red social a la que hemos hecho mención fue que los estudiantes, usando herramientas tecnológicas, pudieran intercambiar ideas matemáticas. En este sentido, nos parece importante revisar la filosofía construccionista de Papert (1981), quien considera que el conocimiento no es algo que se adquiere, sino que se construye. Un aspecto particularmente importante en la obra de Papert (1981) y que está muy ligado a esta investigación, es considerar a la computadora como un laboratorio de investigación donde los estudiantes pueden aprender.

Otros aspectos relevantes fueron las formas de interacción y comunicación que ocurrieron al interior de la comunidad. Por lo tanto, se revisó la idea de aprendizaje colaborativo: un sistema de interacciones que permiten organizar e inducir la influencia recíproca entre los integrantes de un equipo (Johnson & Johnson, 1997). En este paradigma, el aprendizaje se desarrolla a través de un proceso gradual en el que cada miembro y todos se sienten mutuamente comprometidos con el aprendizaje de los demás, generando una interdependencia positiva que no implica competencia.

Es precisamente debido a este papel activo, que el aprendizaje se puede ver como una construcción a través de un entretejido de ideas, tanto a nivel individual como colectivo y en este entretejido, las redes sociales, son una herramienta útil. Bajo esta perspectiva Hargadon (2009) considera una red social como la creación de herramientas web para la construcción de una comunidad y un contenido.

Finalmente, un elemento central que envolvió el proyecto de investigación fue la tecnología desde dos perspectivas: primero, como proveedora de infraestructuras de comunicación y difusión para facilitar la exploración de ideas matemáticas y segundo, como un medio de construcción por sí misma. Desde la primera perspectiva, la red social, en el sentido de Hargadon (2009), -quien la considera como la creación de herramientas web para la construcción de una comunidad y un contenido-, tuvo un papel fundamental al ser el medio que permitió un entretejido de ideas, tanto a nivel individual como colectivo. En cuanto a la segunda perspectiva, la computadora sirvió como un instrumento de mediación (ver Bentonilla y Clavijo, 2001), es decir, como un medio para hacer más accesible el conocimiento. A continuación, se describen las actividades didácticas y la metodología de análisis.

Metodología y análisis de resultados

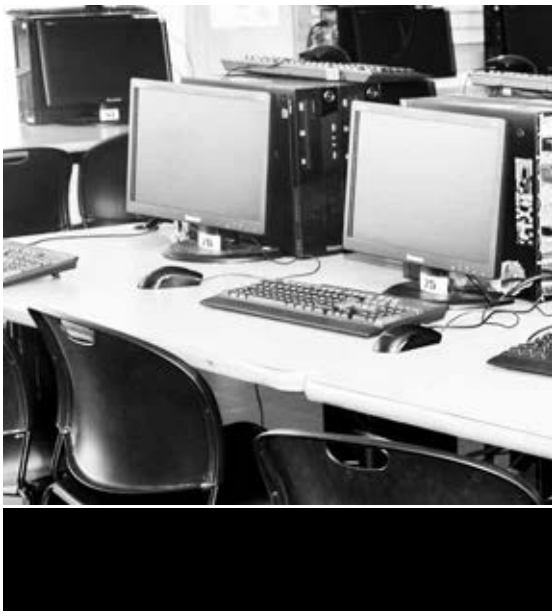
Los objetivos de la investigación fueron:1) analizar la interacción y reflexión en la red social y 2) averiguar si se promovió el aprendizaje. La implementación de las actividades se llevó a cabo con un grupo de 15 estudiantes del Colegio de Ciencias y Humanidades de la UNAM -12 de ellos con edades alrededor de17 años y 3 estudiantes con una edad de 18 años-quienes entraron a la plataforma de aprendizaje en promedio dos veces por semana durante dos meses.

El análisis de resultados se dio a través de analizar las diversas intervenciones que tuvieron los estudiantes en la plataforma: comentarios y criticas acerca de las ideas de los compañeros; formulación de nuevos retos de encriptación; así como asesoría en el uso de las herramientas informáticas. En la actividad 1, sobre mensajes secretos, los estudiantes pusieron en marcha sus conocimientos previos, los cuales evidenciaron que tenían cierta idea acerca del envío de mensajes codificados, mencionaron, por ejemplo, el envío de información en bytes.

Fotografía: Archivo fotográfico de la DGECCH, SC 2017

En la actividad 2, ¿Cómo mandarías mensajes secretos?, se planteó este problema y se tuvieron varias propuestas: una fue escribir las letras al revés y otra fue sustituir cada letra por un número, en esta actividad, se le recuerda al lector, que el profesor introdujo el criptosistema de sustitución, el cual se trabajaría en la siguiente actividad.

La actividad 3, encriptando/desencriptando fue la parte medular del trabajo, en esta etapa algunos estudiantes propusieron textos y se analizaron la distribución de las frecuencias de las letras del alfabeto usando tablas y gráficas mediante la hoja de cálculo (ver figura 2), con el objetivo de encontrar patrones de repetición, o dicho estadísticamente, buscar patrones de regularidad estadística en la frecuencia de cada letra. En esta actividad los estudiantes retaron a sus compañeros con mensajes encriptados, los cuales debían descifrar usando un análisis de frecuencias; la respuesta de los participantes fue positiva en el sentido de involucrarse en un proceso de colaboración para lograr el objetivo.



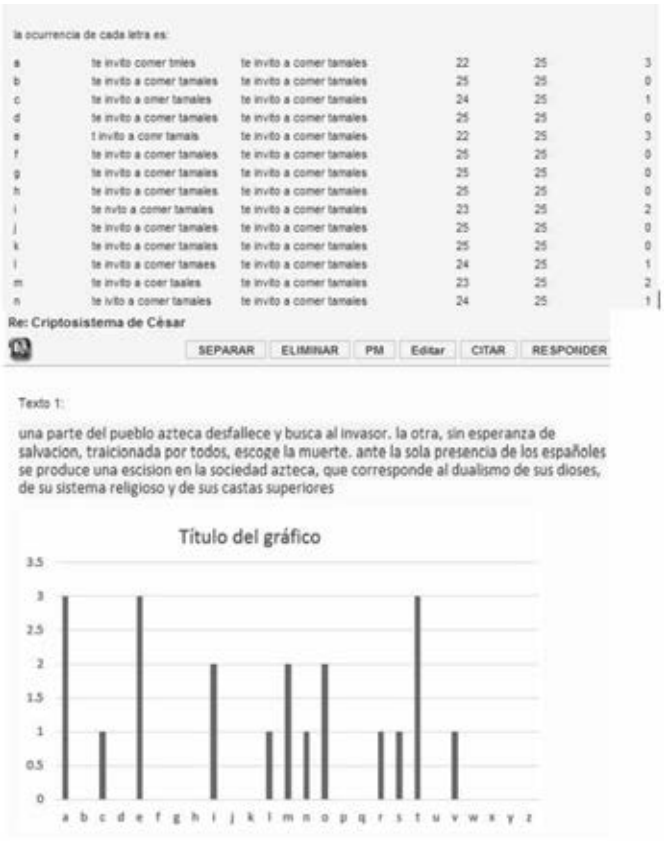


Figura 2: Implementación en Excel de las frecuencias de aparición e cada letra en un texto y un gráfico que muestra la frecuencia de aparición de un conjunto de letras.

A continuación, mostramos un episodio de la encriptación por sustitución, en el que es posible apreciar una serie de discusiones en donde se comparan la distribución de frecuencias de las letras en el mensaje encriptado con las frecuencias de un texto de referencia, se aprecia un cierto trabajo colaborativo.

Estudiante 1: propone que descifren el mensaje "fm hbup ujfof ibncsf".

Estudiante 2: propone encontrar las frecuencias de aparición de las letras en un texto de referencia y comparar dichas frecuencias con las del texto encriptado.

Estudiante 3: con base a la obtención de frecuencias del Estudiante 2, afirma que en el mensaje codificado las letras que más se repiten son b, f, u, mientras que en el texto cualquiera las letras que más se repiten son a, e, t.

Estudiante 4: construye las gráficas de las frecuencias del texto encriptado y del texto de referencia.

Estudiante 2: afirma que hay varias posibilidades respecto al verdadero valor de cada letra en el texto encriptado; entre ellas que: la "f" en el texto encriptado sea en realidad la "a", que la "b" sea la "a", etcétera, siguiendo con su análisis también considera que la "f" podría ser la "e". En estos términos afirma que en el texto encriptado, el verdadero valor de la letra es "una antes", de forma que el texto encriptado: "fm hbup ujfof ibncsf", es "el gato tiene hambre".

Fotografía: Archivo fotográfico de la DGECCH, 2017

Conclusiones

En relación con los objetivos de la investigación planteados: 1) analizar la interacción y reflexión en la red social y 2) averiguar si se promovió el aprendizaje, se tiene lo siguiente:

Respecto al primer objetivo, es posible afirmar que la red social que se logró conformar permitió que los estudiantes pudieran expresar sus ideas, así como recibir críticas o retroalimentación de sus compañeros y también explorar de forma colaborativa diversos procesos de encriptación/desencriptación, lo anterior en un ambiente mediado por tecnología.

En cuanto al segundo objetivo de investigación, en el proceso de descifrar los criptosistemas, los estudiantes tuvieron que recopilar datos -al obtener la frecuencia de las letras-, así como construir tablas de frecuencias e histogramas, de acuerdo con lo indicado en el programa de Estadística I (ver Escuela Nacional Colegio de Ciencias y Humanidades, 2016).

Finalmente, consideramos importante contrastar nuestra investigación contra la de Massimo M., Fioretto A., Sgarro A. y Zuccheri L. (2002), en este sentido, coincidimos con los autores, en el hecho de que la criptografía fue un camino estimulante para introducir las ideas estadísticas y también con el hecho de que el análisis criptográfico, permitió, al menos en términos elementales, que los estudiantes se involucraran en la solución de problemas, en este caso: descrifrar criptosistemas.

Referencias

Bentolilla, S., y Clavijo, P. M. (2001). La computadora como mediador simbólico de aprendizajes escolares: análisis y reflexiones desde una lectura vigotskiana del problema. *Fundamentos en humanidades, 2* (3) 1, 77-101.

Borelli M., Fioretto A., Sgarro A. &Zuccheri L. (2002). Cryptography and Statistics: A Didactical Project. En I. Vakalis (ed.). *2nd International Conference on the Teaching of Mathematics at the Undergraduate Level. Conference Proceedings (pp. 265-271)*. Creta, Grecia. Recuperado de <http://users.math.uoc.gr/~ictm2/>.

Escuela Nacional Colegio de Ciencias y Humanidades (2016). *Programas de Estudio. Área de Matemáticas. Programas de estudio de Estadística y Probabilidad I-II*. México: Autor.

Fernández, S. F. (2004). La criptografía clásica. *Sigma*, (24), 119-142.

Hargadon, S. (2009). *White Paper on Educational Networking: The important role Web 2.0 will play in education*. Recuperado de <http://www.elluminate.com/downloads/whitepapers/SocialNetworkingWhitepaper.pdf>.

Johnson, D. W., & Johnson, F. P. (1997). *Joining together: group theory and group skills.* Boston: Allyn & Bacon.

Papert, S. (1981). *Desafío a la mente*. Buenos Aires: Galápago.