



Julio 2017 - ISSN: 2254-7630

ANÁLISIS DE ALGORITMOS MATEMÁTICOS DE CRIPTOGRAFÍA PÚBLICA PARA MEJORAR EL APRENDIZAJE DE LA MATERIA DE CRIPTOGRAFÍA EN LA CARRERA DE INGENIERÍA EN SISTEMAS INFORMÁTICOS DE LA ESPOCH*

Mario Humberto Paguay Cuvi

Docente de la Facultad de Informática y Electrónica en la Escuela Superior Politécnica de Chimborazo. Doctor en Matemática, Magister en Matemática Básica. mpaguay@esPOCH.edu.ec.

Gloria de Lourdes Arcos Medina

Docente de la Facultad de Informática y Electrónica en la Escuela Superior Politécnica de Chimborazo. Ingeniera de Sistemas en Informática, Master en Informática Aplicada. garcos@esPOCH.edu.ec.

Lourdes del Carmen Zúñiga Lema

Docente de la Facultad de Informática y Electrónica en la Escuela Superior Politécnica de Chimborazo. Doctor en Matemática, Magister en Ciencias de la Educación Aprendizaje de la Matemática. luzuñiga@esPOCH.edu.ec.

Danilo Mauricio Pastor Ramírez

Docente de la Facultad de Informática y Electrónica en la Escuela Superior Politécnica de Chimborazo. Doctor en Matemática, Master en Informática Aplicada. dpastor@esPOCH.edu.ec.

Para citar este artículo puede utilizar el siguiente formato:

Mario Humberto Paguay Cuvi, Gloria de Lourdes Arcos Medina, Lourdes del Carmen Zúñiga Lema y Danilo Mauricio Pastor Ramírez (2017): "Análisis de algoritmos matemáticos de criptografía pública para mejorar el aprendizaje de la materia de criptografía en la carrera de Ingeniería en Sistemas Informáticos de la ESPOCH", Revista Caribeña de Ciencias Sociales (julio 2017). En línea: <http://www.eumed.net/rev/caribe/2017/07/criptografia-esPOCH.html>

RESUMEN

Partiendo del estudio de las teorías matemáticas y definiendo los parámetros para realizar el análisis de los algoritmos de criptografía pública, además de realizar ambientes de aprendizaje para determinar la incidencia de la utilización de los algoritmos matemáticos de criptografía pública en los alumnos de la carrera de Ingeniería en Sistemas Informáticos de la ESPOCH, se ha llegado a seleccionar el algoritmo más adecuado para mejorar el aprendizaje de la materia de criptografía. En este trabajo se ha empleado una investigación cuasi experimental siguiendo el método científico, se han desarrollado ambientes de prueba sobre RSA (Rivest, Shamir y Adleman), Diffie-Hellman, El Rabin y El Gamal, siendo RSA el mejor algoritmo para la enseñanza con un total de 100% en su valoración técnica; mientras que en conceptos matemáticos Diffie-Hellman resulta ser el de mejor comprensión en los estudiantes con un 50,40%. Se ha definido que los conceptos matemáticos fundamentales son la aritmética modular, teoría de números, curvas elípticas, estructuras algebraicas (grupos finitos) y el algoritmo extendido de Euclides; con ello se recomienda analizar de manera profunda la malla curricular de la EIS (Facultad de Informática y Electrónica, 2013), para que estos conceptos sean añadidos a las asignaturas de matemática lo cual beneficiará al estudiante a la mejor comprensión de la asignatura.

Palabras claves: Aprendizaje, Algoritmos, Criptografía, Matemáticas, Sistemas Informáticos.

* Artículo extraído del Proyecto de investigación presentado ante el Instituto de Posgrado y Educación Continua de la ESPOCH, como requisito parcial para la obtención del grado de Magister en "Matemática Básica", disponible de forma completa en <http://dspace.esPOCH.edu.ec/bitstream/123456789/4431/1/20T00643.pdf>

JEL: A30 Generalidades; C00 – Generalidades; I20 Generalidades; I20 Generalidades: I21 Análisis de la Educación

https://es.wikipedia.org/wiki/C%C3%B3digos_de_clasificaci%C3%B3n_JEL

ABSTRACT

Based on the study of mathematical theories and defining the parameters for analysis of public key cryptography algorithms, in addition to implement learning environments to determine the incidence of using mathematical algorithms of public key cryptography in students of Computer Systems Engineering career of ESPOCH, we come to select the most appropriate algorithm to improve the learning of the subject of cryptography. In this paper it has used a quasi-experimental research using the scientific method; it developed test environments about RSA, Diffie-Hellman, Rabin and El Gamal, being RSA the best algorithm for teaching with an effectiveness of 100% on its technical evaluation; while Diffie-Hellman mathematical concepts prove to be the better in students understanding with a 50.40%. It has defined that the fundamental mathematical concepts are modular arithmetic, number theory, elliptic curves, algebraic structures (finite groups) and the extended Euclidean algorithm; it is therefore recommended to analyze in depth the curriculum of the EIS for these concepts to be added to the mathematics courses which will benefit the student to a better understanding of the subject.

Keywords: Learning, Algorithms, Cryptography, Mathematics, Computer Systems

INTRODUCCIÓN

Actualmente las redes de comunicación han tenido un gran crecimiento, tanto así que para los seres humanos es vital mantenerse en contacto con familiares y amigos ya sean por teléfono o a su vez el internet, y no solo la comunicación familiar sino también las noticias y ámbitos militares hoy por hoy pueden generar un volumen de información sumamente grande así como también transmitirlo de forma inmediata. Pero no toda información es pública y desde la antigüedad ha sido así, por ejemplo los mensajes militares en el campo de batalla que se envían de un lugar a otro deben ser privados y deben poder conocerse solo entre los miembros de una unidad, nación o país, como es el caso de la comunicación realizada mediante la máquina ENIGMA empleada por el ejército alemán durante la segunda guerra mundial.

Por esta necesidad se han creado distintos métodos de cifrado de información el cual permite comunicarse entre dos puntos de forma segura, esto evitaría que una persona no deseada o un enemigo capturen estas comunicaciones y tomen ventaja, otro ejemplo de mensajes que deben ser cifrados son por ejemplo las conexiones que se realicen a través de internet como transacciones bancarias, es por ello que las entidades financieras emplean mecanismos como cifrados SSL (Secure Socket Layer) en sus sitios web, esto permite aumentar la seguridad de los datos que viajan desde el ordenador hasta su sitio. (Banco de Guayaquil, Consejos de Seguridad, 2017).

Dado también que los sistemas informáticos son la mejor forma de gestionar la información actualmente, se imparte en la Escuela Superior Politécnica de Chimborazo la asignatura de criptografía a los sextos semestres de la carrera de Ingeniería en Sistemas (Facultad de Informática y Electrónica, 2013), se pretende ayudar a la asignatura al proporcionar un análisis de los algoritmos de criptografía pública con la finalidad de encontrar el algoritmo más adecuado para la mejor comprensión de la materia realizando un estudio comparativo entre RSA, Diffie-Hellman, Rabin and El Gamal, con la finalidad de optimizar la asimilación de estos conceptos en los estudiantes. Teniendo

como objetivo Analizar los algoritmos matemáticos de criptografía pública para mejorar el aprendizaje de la materia de criptografía en la carrera de Ingeniería en Sistemas de la ESPOCH.

Para esto se planteó como hipótesis: “El algoritmo RSA es el más adecuado para el aprendizaje de la criptografía pública en los alumnos de la Facultad de Informática y Electrónica de la ESPOCH en relación de los algoritmos Diffie-Hellman, El Gamal y El Rabin”. Qué problemas se han investigado con respecto a conocer si determinado algoritmo de criptografía publica es el más adecuado en la enseñanza de la criptografía, como habían definidos esos problemas, qué evidencias empíricas y metodológicas se habían utilizado ,cual es el producto de las investigaciones, al respecto se ha podido indagar los siguientes publicaciones :

En el estudio de La Enseñanza de la Criptografía en los Cursos de Educación Media “El problema que se aborda en esta investigación se centra en un aspecto específico de la formación matemática de los maestros.” (Ibáñez, 2012). El “Análisis De Algoritmos De Cifrado De Llave Secreta Y Su Uso Dentro De Una Organización Pública” (Morales, 2009). Estudio comparativo es “Análisis de Algoritmos Criptográficos y su aplicación al Cifrado de Archivos” (Blanco, 2010). Estudios comparativos sobre estos algoritmos de cifrado existen pero no poseen fines educativos, luego de realizar este estudio se evidencia que no existen estudios similares o relacionados directamente con lo cual se fortifica la necesidad de buscar el mejor algoritmo criptográfico para la enseñanza de la asignatura de criptografía.

REVISIÓN DE LA LITERATURA

Dentro de los principales algoritmos de estudio se encuentran RSA, Diffie-Hellman, El Gamal, El Rabin que son algoritmos de clave pública, dichos algoritmos no se generan de la misma forma y cada uno posee un nivel de complejidad de aprendizaje que varía a los conceptos informáticos y matemáticos.

Algoritmo RSA

Algoritmo de cifrado de información y de firmas digitales publicado a partir de 1977, creado por Ron Rivest, Adi Shamir y Leonard Adleman, característico de poseer un par de claves, una pública y una privada con las cuales se puede cifrar y leer los mensajes en claro. Este método de cifrado usa una de las claves a la vez es decir se cifra con una clave pública que lo puede tener cualquier persona y se utiliza la otra llave (privada) para leer el mensaje que se nos ha enviado. Esta fortaleza se debe a la imposibilidad de factorar números primos extremadamente grandes por lo que se usan generalmente números de más de 1000 bits de forma similar las firmas digitales son firmadas y verificadas por los usuarios de documentos para verificar la autenticidad del emisor. (Lucena, 2009) Del total de conceptos matemáticos se han distinguido 3 necesarios para la comprensión del algoritmo RSA los cuales son Aritmética Modular, Estructuras Algebraicas y el Algoritmo Extendido de Euclides

Algoritmo Diffie-Hellman

Publicado en 1976 por Whitfield Diffie y Martín Hellman es un algoritmo para realizar un intercambio de claves por un medio no seguro, si bien es cierto se hace público en 1976 se ha conocido ya que la agencia de inteligencia británica ya hacía uso de métodos similares en sus comunicaciones. Si bien es cierto se usa para el envío de claves por lo general para luego usar sistemas de clave pública como el RSA no se puede usar en dos personas sino quizás más personas puedan distribuirse claves mediante este mecanismo. Es considerado por muchos como el primer algoritmo seguro de intercambio de claves anónimas.

Aun así, siendo seguro como es, se puede vulnerar mediante el ataque hombre en el medio por lo que es necesario verificar de alguna forma la autenticidad del usuario remitente o receptor, este

algoritmo también usa el principio del logaritmo discreto. (Lucena, 2009). Para la comprensión del algoritmo Diffie-Hellman se han determinado los siguientes conceptos matemáticos Aritmética Modular, Estructuras Algebraicas y Grupos Finitos

Algoritmo El Gamal

Fue desarrollado por Taher Elgamal en 1984 es un algoritmo de cifrado y firmado asimétrico no posee ningún tipo de licencia y se usa en proyectos GNU, este algoritmo de cifrado consta de 3 partes el generador de claves y los métodos de cifrado y descifrado. Este método sirve de algoritmo base para la generación de cifrados como DSS y NIST la única dificultad de este algoritmo radica en que las cadenas de cifrado son mucho más largas así como el recurso computacional más elevado, en comparación con el método RSA, ElGamal es mucho menos eficiente.(Departamento de Sistemas Informáticos y Computación). Para la comprensión del algoritmo El Gamal se necesitan los siguientes conceptos matemáticos: son Aritmética Modular, El Algoritmo Extendido de Euclides, El Teorema Chino del Resto, Grupos Finitos

Algoritmo El Rabin

Publicado en 1979 fue el único algoritmo que permitía descifrar un mensaje completo a partir del texto cifrado, desarrollado por Michael Rabin, usa métodos como el teorema chino del resto y la exponenciación modular, considerado como más seguro que RSA u debilidad está en lo métodos de factorización de las raíces cuadradas que se utilizan para generar las claves. (Departamento de Sistemas Informáticos y Computación). Del total de conceptos matemáticos se han distinguido 6 necesarios para la comprensión del algoritmo El Rabin los cuales es Aritmética Modular, Estructuras Algebraicas, El Algoritmo Extendido de Euclides, El Teorema Chino del Resto, Logaritmos y la Obtención de Raíces Cuadradas

MATERIALES Y MÉTODOS

Tipo de Investigación

El tipo de investigación fue descriptiva debido a que se estudió cada uno de los algoritmos matemáticos de criptografía pública con la finalidad de determinar el algoritmo óptimo para la enseñanza de la asignatura y aplicativa porque se realizaron ambientes de prueba impartiendo por cátedras al mismo grupo de estudiantes los algoritmos de criptografía pública, además se empleó el método científico para la comprobación de la hipótesis.

Población y Muestra

Para llevar a cabo el estudio se ha tomado como población todos los estudiantes del séptimo semestre de la Escuela de Ingeniería en Sistemas de la Facultad de Informática y Electrónica, dado que la asignatura de criptografía se encuentra dentro de las materias optativas de la carrera, se busca generar un estudio con una muestra intencional toda la población en sí de 23 estudiantes de séptimo semestre dado que los estudiantes ya pueden por sus créditos recibir esta cátedra, a más de ello se considera que los estudiantes en este semestre ya poseen varios conocimientos matemáticos y nociones criptográficas necesarios para la comprensión de los algoritmos criptográficos de llave pública.

Diseño de la Investigación

Para la siguiente trabajo, se determinará el diseño de la investigación en donde se busca determinar cuál es el algoritmo óptimo para la enseñanza de la criptografía en la EIS - ESPOCH, tomando como

punto de partida su diseño, la población y muestra a la que se aplicará, la operacionalización de las variables así como las técnicas e instrumentos que permitirán la recolección de los datos, se diseñarán los entornos de prueba que se realizarán a los estudiantes para su posterior análisis en donde obtendremos los resultados generales de la investigación.

Para la investigación se ha determinado un diseño cuasi-experimental dado que se busca manipular la variable independiente (los algoritmos de criptografía pública) y obtener resultados en la variable dependiente (el nivel de enseñanza en la asignatura de criptografía) es decir un principio de causa-efecto, con un grupo ya conformado de estudiantes los mismos que fueron seleccionados dentro de la Escuela de Ingeniería en Sistemas en la ESPOCH y además han cursado la asignatura de criptografía (séptimo semestre).

Métodos, Técnicas e Instrumentos

Una vez definida la población y seleccionada la muestra, para el proyecto se utiliza el método científico. Este modelo de investigación es un modelo genérico que ha sido aceptado y difundido por la comunidad de científicos a nivel mundial a más de ellos para los escenarios se emplea el método inductivo puesto que de las cátedras de los algoritmos se busca mejorar la cátedra de la asignatura de criptografía en la Escuela de Ingeniería en Sistemas.

Para la recolección de la información del proyecto se planteó el método científico y como técnica principal la encuesta a modo de cuestionario puesto que se dictó cátedras de criptografía sobre los algoritmos de llave pública, empleando los algoritmos matemáticos a los estudiantes de séptimo semestre de la carrera, las preguntas que se realizaron en esta técnica son de tipo cerradas con ello se facilitó la interpretación de sus resultados, la encuesta se aplicó al finalizar cada cátedra y se los hizo mediante las herramientas de formularios de Google ya que las encuestas pueden ser procesadas de inmediato e interpretar sus datos para el estudio de una forma más eficaz.

Los instrumentos utilizados en la investigación se citan a continuación:

- Comparación Directa – Revisión de Literatura, Fuentes, Bibliografías
- Encuestas - Cuestionario
- Ambientes de Prueba

A los estudiantes de séptimo semestre que fueron sometidos a la encuesta se les impartió 4 ponencias que ha preparado el tesista en las cuales se impartió un algoritmo de criptografía pública (RSA, El Gamal, Diffie-Hellman, El Rabin) con el siguiente detalle por escenario:

- Breve introducción al algoritmo de cifrado.
- Tipos de conceptos matemáticos a emplearse en el algoritmo.
- Problema práctico.
- Descripción de los datos de entrada del algoritmo de cifrado.
- Ejecución del algoritmo de cifrado.
- Ejecución del algoritmo de des cifrado.

Este distributivo tuvo como fundamentación teórica los análisis de los diferentes métodos de cifrado, toda la cátedra no fue más allá de 60 minutos con lo que se necesitaron 2 horas clase formal para

completar los contenidos, se ha dispuesto los contenidos así con la finalidad de que los estudiantes comprendan la idea global de criptografía.

Para los 4 ambientes (RSA, El Gamal, Diffie-Hellman, El Rabin), se realizaron las siguientes preguntas:

- Entendimiento del algoritmo matemático.
- Comprensión y dominio en la obtención de los datos de entrada.
- Conceptualización del algoritmo de cifrado.
- Conceptualización del algoritmo de descifrado.
- El estudiante es capaz de implementar al menos un algoritmo criptográfico.
- El estudiante es capaz de crear un algoritmo criptográfico personalizado.
- El estudiante puede descifrar un texto encriptado.
- Conocimiento sobre aritmética modular.
- Conocimiento sobre estructuras algebraicas.
- Conocimiento sobre logaritmos.
- Conocimiento sobre la obtención de raíces cuadradas.
- Conocimiento sobre el Teorema chino del resto.
- Conocimiento sobre el algoritmo Extendido de Euclides.
- Conocimiento sobre Curvas Elípticas.
- Conocimiento sobre Grupos Finitos

RESULTADOS Y DISCUSIÓN

Para el desarrollo de los Resultados y Discusión de la investigación se toman los indicadores e índices de las siguientes tablas:

Tabla 1: Operacionalización Metodológica Variable

INDICADORES	ÍNDICES
Datos de Entrada.	Número de los datos de entrada.
	Dificultad para la preparación de los datos.
Algoritmo de Cifrado.	Número de pasos.
	Dificultad de los pasos.
	Orden de complejidad.
Algoritmo de Descifrado.	Número de pasos.
	Dificultad de los pasos.
	Orden de complejidad.
Conceptos Matemáticos.	Cantidad de definiciones matemáticas empleadas.
	Importancia de los conceptos matemáticos.

Independiente

Fuente: Autores
Año: 2015

Tabla 2: Operacionalización Metodológica Variable

INDICADORES	ÍNDICES
Nivel de comprensión.	Entendimiento del algoritmo matemático.
	Comprensión y dominio en la obtención de los datos de entrada.
	Conceptualización del algoritmo de cifrado.
	Conceptualización del algoritmo de descifrado.
Nivel de aplicación de conocimientos.	El estudiante es capaz de implementar al menos un algoritmo criptográfico.
	El estudiante es capaz de crear un algoritmo criptográfico personalizado.
	El estudiante puede descifrar un texto encriptado.
Conceptos Matemáticos.	Conocimiento sobre aritmética modular.
	Conocimiento sobre estructuras algebraicas.
	Conocimiento sobre logaritmos.
	Conocimiento sobre la obtención de raíces
	Conocimiento sobre el Teorema chino del resto.
	Conocimiento sobre el algoritmo Extendido de
	Conocimiento sobre Curvas Elípticas.
	Conocimiento sobre Grupos Finitos

Dependiente

Fuente: Autores
Año: 2015

Como se puede apreciar en las Tablas 1 y 2, tanto los indicadores e índices evidencian la operacionalización metodológica de las variables, se analizará uno por uno los indicadores y se empleará la escala de Likert para sus valoraciones, se hará una tabla de resumen para interpretar posteriormente cada indicador, analizar sus valoraciones y ver los estados de las variables para posteriormente realizar la prueba de la hipótesis planteada en el estudio con la finalidad de emitir las conclusiones y recomendaciones pertinentes, se inicia con el análisis de los indicadores de la variable independiente y posteriormente la variable dependiente.

Variable Independiente

A Continuación se realiza el análisis de los indicadores de la variable independiente de la siguiente manera:

Indicador 1- Datos de entrada

Los algoritmos criptográficos por lo general necesitan de ciertos datos para su funcionamiento, estos datos pueden ser por ejemplo en el proceso de cifrado, un texto para ser cifrado necesita de la clave pública del usuario destinatario más la clave privada del usuario emisor y el texto a cifrar con esto ejecutado el algoritmo ya obtendremos un texto que sólo los dos usuarios comprenderán, para determinar este indicador se analizarán los siguientes índices:

Índice 1 – Número de Datos de Entrada.- Se realiza el análisis comparativo entre los algoritmos RSA, Diffie-Hellman, El Rabin y El Gamal de los datos de entrada que requiere cada algoritmo para su funcionamiento.

La comparación de los 4 algoritmos se ha determinado que los 5 datos de entrada del algoritmo RSA permiten al usuario tener los requerimientos completos para cifrar el mensaje por lo que se le ha dado una valoración de 100%, haciendo referencia cada dato de entrada tendría una valoración de 20% con lo que los 3 datos de El Gamal, los 4 datos de Diffie-Hellman y El Rabin corresponden a un 60% y 0% respectivamente.

La escala Likert se ha definido de la siguiente forma: 5 puntos al algoritmo más óptimo y 1 punto al algoritmo que no es óptimo, cada punto Likert equivale al 20% del total de pasos del algoritmo, como se evidencia en el Gráfico N° 1.

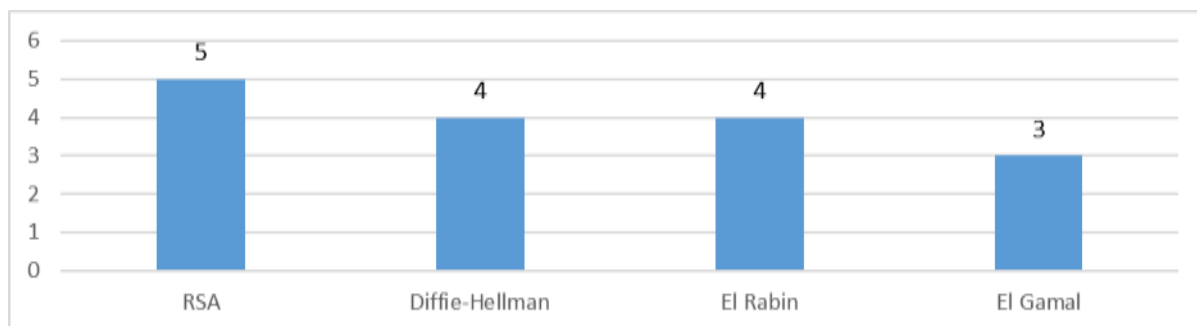


Gráfico N°1: Resumen Índice 1

Fuente: Autores

Elaboración: Autores

Índice 2 – Dificultad para la preparación Datos de Entrada.- Si el algoritmo lo requiere los datos de entrada deben someterse a un proceso para que sean útiles realmente, este indicador es analizado debido a que los procesos de preparación emplean conceptos y definiciones matemáticas que deben ser entendidas por los estudiantes.

Se da un valor alto a los procesos que poseen una dificultad baja por lo que los puntos de referencia serían 1 – a las operaciones matemáticas de baja dificultad, 3 operaciones de mediana dificultad y 5 – a las operaciones que implican una alta dificultad y se resume en el Gráfico N°2.

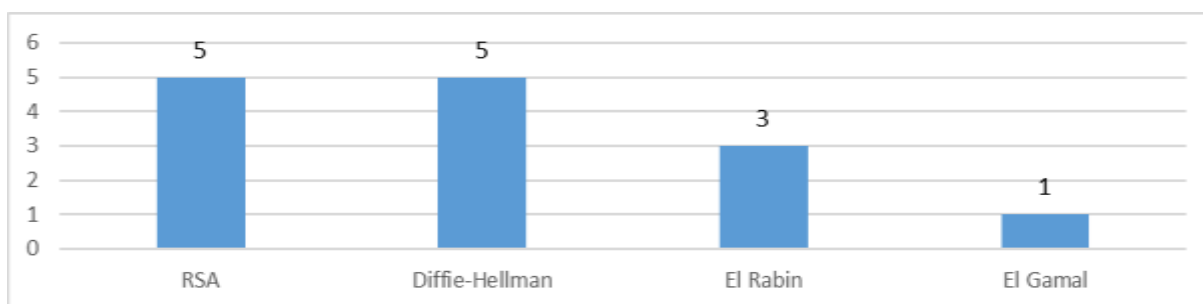


Gráfico N°2: Resumen Índice 2

Fuente: Autores
Elaboración: Autores

Se le ha dado el valor de 5 puntos al algoritmo RSA debido a que las operaciones multiplicación y módulo son sencillas, así como la potenciación en Diffie-Hellman el caso opuesto es El Gamal en donde el estudiante debe comprender que es un grupo finito de números y lograr realizar la discriminación de los datos de entrada necesarios por lo que se le ha dado una valoración de 1.

Indicador 2 - Algoritmo de Cifrado

Este algoritmo es de suma importancia puesto que se ve la mitad de la conceptualización de la criptografía en sí, es decir, el cifrado de la información.

Índice 3 – Número de Pasos del Algoritmo de Cifrado.- Para obtener el cifrado se sigue una cantidad de pasos que han sido contabilizados en el análisis de los algoritmos, de esta manera se evidencia que el algoritmo RSA posee un solo paso de cifrado y El Gamal 5 por lo que se considera a los pasos de El Gamal el 100 de pasos para realizar un algoritmo de los cuales se le da la valoración de 100% que es el algoritmo que posee mayor número de pasos es más complejo de comprender.

La valoración de cada punto corresponde al 20% del total de pasos. Para realizar el algoritmo de cifrado de los mismos que se ha dado la valoración de 5 puntos al algoritmo RSA porque posee un sólo paso para cifrar la información por lo que el estudiante no tendrá mucha dificultad y obtendrá un mensaje cifrado en corto tiempo, el algoritmo Diffie-Hellman no aporta a este índice puesto que en su algoritmo de cifrado es otro algoritmo como RSA, Diffie-Hellman permite el intercambio seguro de claves por lo que se le asigna la valoración de 0, los datos se resumen en el Gráfico N° 3.

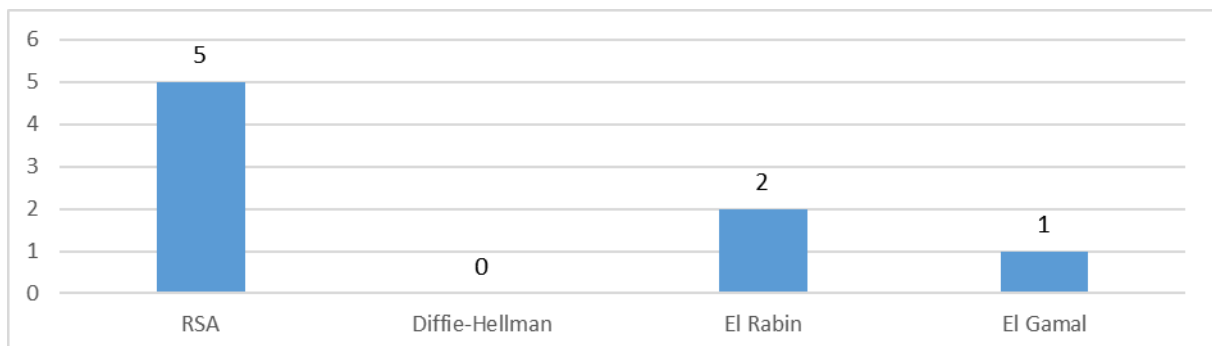


Gráfico N° 3: Resumen Índice 3

Fuente: Autores
Elaboración: Autores

Índice 4 – Dificultad de los Pasos del Algoritmo de Cifrado.- De forma análoga a los algoritmos para la preparación de los datos de entrada aquí se analizan las posibles complicaciones matemáticas de los pasos del algoritmo de cifrado. Se lo excluye al algoritmo Diffie-Hellman puesto que no se puede realizar una continuidad de análisis con el índice anterior.

Se ha asignado en su valor más alto al valor cualitativo más bajo siguiente el criterio de las operaciones matemáticas en lo que destacan los algoritmos RSA y El Rabin cuyas operaciones no representan complejidad en relación a las operaciones de El Gamal en donde hay que transformar el texto en claro a bits para posteriormente cifrarlos, estos datos se resumen en el Gráfico N° 4.

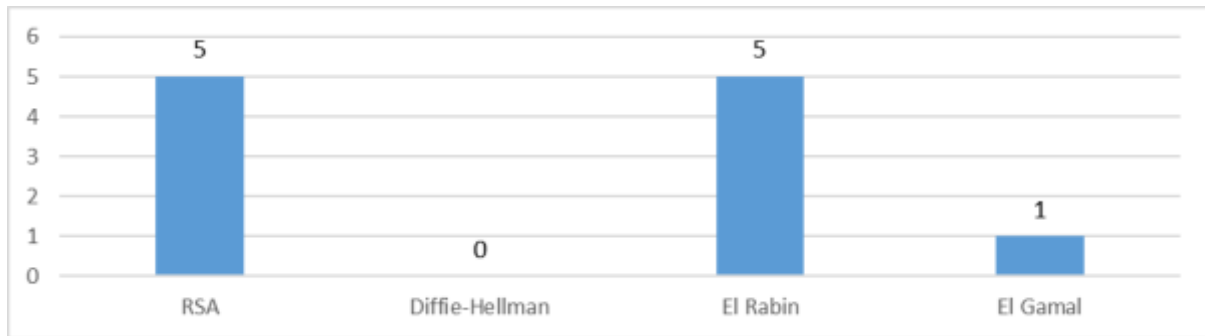


Gráfico N°4: Resumen Índice 4

Fuente: Autores

Elaboración: Autores

Índice 5 – Orden de Complejidad

El orden de complejidad del algoritmo se define por la cantidad de estructuras de decisión (si - entonces, estructuras anidadas, estructuras multi condicional, estructuras switch), bucles de repetición (estructuras while, estructuras do while, estructuras for). Con este orden de complejidad se le ha asignado en la escala de Likert 5 a los algoritmos con orden de complejidad bajo (nulo), 3 a los algoritmos de complejidad medio y 1 a los algoritmos de alta complejidad como se muestra en el Gráfico N° 5:

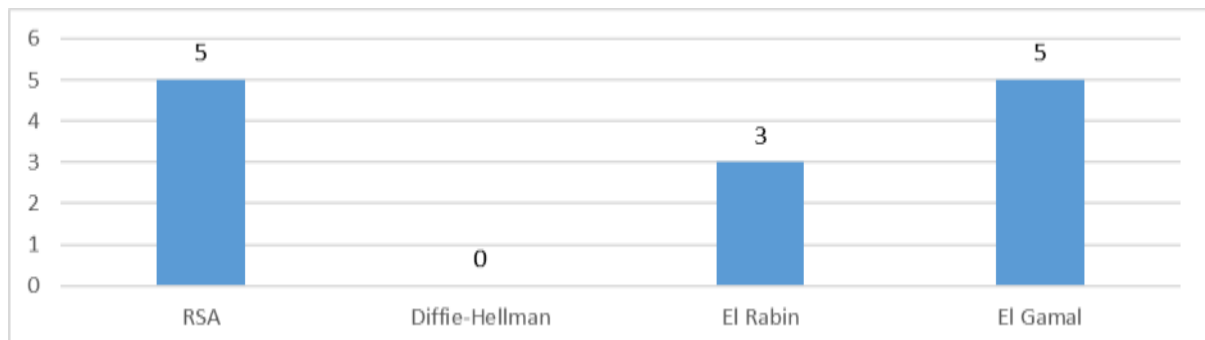


Gráfico N°5: Resumen Índice 5

Fuente: Autores

Elaboración: Autores

Indicador 3 - Algoritmo de Descifrado

Este algoritmo es la parte complementaria de la criptografía y se aplica cuando el receptor ha recibido el mensaje codificado y pretende devolverle a texto en claro.

Índice 6 – Número de Pasos del Algoritmo de Descifrado.- Para obtener el texto en claro se deben seguir de forma rigurosa los pasos que propone el algoritmo criptográfico.

El número de pasos del algoritmo El Gamal suma 3 pasos que se considera el 33,33% y los algoritmos Diffie-Hellman corresponden al 66,67% respectivamente, finalmente a el algoritmo RSA le corresponde el 100% dado que el algoritmo RSA se considera óptimo para la enseñanza puesto que es más fácil asimilar 1 paso frente a 3 pasos de El Gamal, al asignar los valores con la escala se asigna el valor de 5 al algoritmo con menor número de pasos y 1 con el mayor número de pasos

asumiendo que el mayor número de pasos dificulta la comprensión y la ejecución del algoritmo, su valoración se muestra en el Gráfico N° 6.

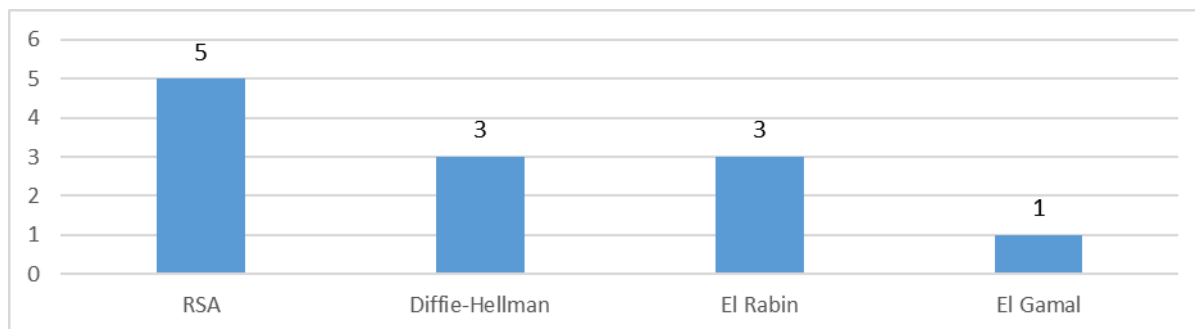


Gráfico N°6: Resumen Índice 6

Fuente: Autores

Elaboración: Autores

Índice 7 – Dificultad de los Pasos del Algoritmo de Descifrado.- Esta sección es muy importante puesto que de estos conceptos matemáticos los intrusos podrán o no vulnerar la información.

La multiplicación, módulo y potenciación son considerados como dificultad baja, las operaciones con logaritmos son consideradas como operaciones de dificultad media y el teorema chino del resto como una dificultad alta estos son los conceptos que manejan los algoritmos, el teorema chino del resto ha sido considerado de una gran dificultad puesto que se requieren conocimientos profundos de matemática para realizar la inversión de las raíces y discriminar aquellas que son útiles, para lo cual se han designado valores de 5 a los de menor dificultad, 3 dificultad media y 1 a la dificultad alta como se detalla en el Gráfico N° 7:

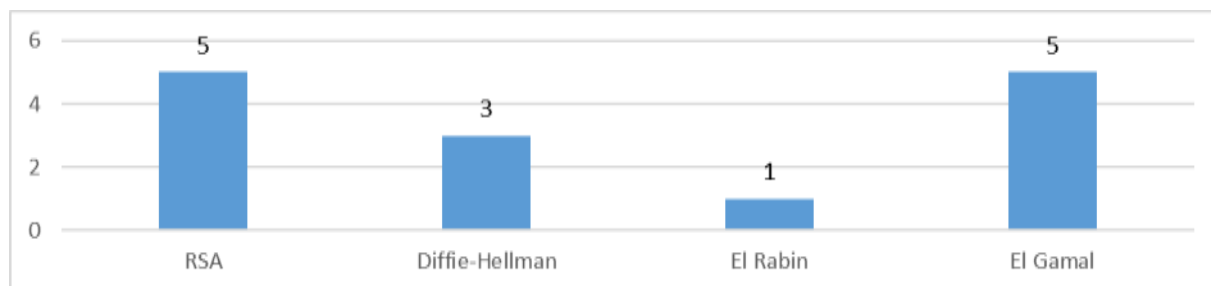


Gráfico N°7: Resumen Índice 7

Fuente: Autores

Elaboración: Autores

Índice 8 – Orden de Complejidad.- El orden de complejidad del algoritmo se define por la cantidad de estructuras de decisión y bucles de repetición.

Se determinó que los algoritmos RSA, El Gamal, Diffie-Hellman no poseen estructuras de decisión ni estructuras de repetición por lo que se le asigna una valoración de bajo, el algoritmo El Rabin posee estructuras condicionales para determinar las raíces que son válidas para la factorización de los mensajes se le ha signado un valor de alto ya que los conceptos del teorema chino del resto requieren de 4 raíces las cuales serán discriminadas quedando los algoritmos de complejidad baja con valoración de 5 puntos y el de complejidad alta valoración de 1 punto, como se puede apreciar en el Gráfico N° 8.

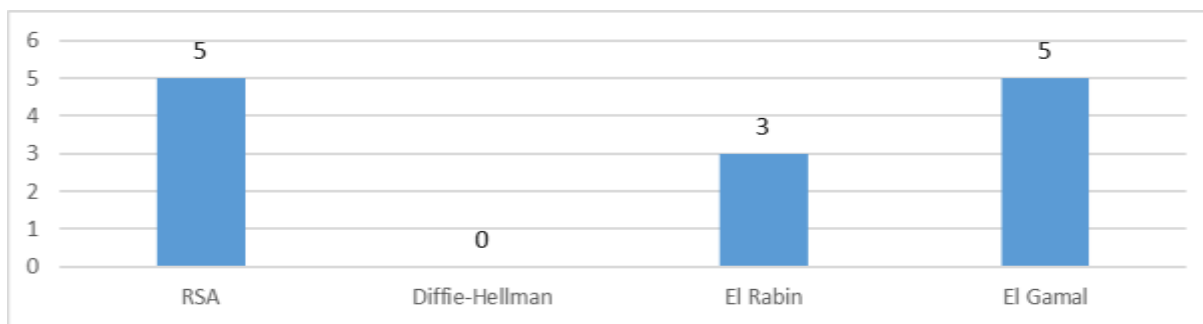


Gráfico N°8: Resumen Índice 8

Fuente: Autores

Elaboración: Autores

Indicador 4 - Conceptos Matemáticos

El indicador conceptos matemáticos genera evidencia de la matemática que se emplea en cada algoritmo es decir las definiciones que sirven para cifra y des cifrar la información, la construcción del algoritmo, el origen de los datos de entrada y cómo influyen estos en el criptosistema por lo que se detallan los índices 9 cantidad de definiciones matemáticas empleadas, 10 la importancia de las definiciones y 11 el orden de complejidad de las mismas.

Índice 9 – Cantidad de Definiciones Matemáticas.- En los algoritmos de encriptación es importante conocer cada una de sus características, por esto se cuantificarán la cantidad de conceptos matemáticos que necesita cada algoritmo criptográfico.

Las definiciones que se emplean en todo el ciclo de vida del algoritmo de criptografía en donde la máxima suma de los valores es 5 que ello significa para el estudiante conocer más a profundidad sobre estos temas, por lo que a los algoritmos de menor cantidad de definiciones posee una valoración de 5 y el que más definiciones posea será el mayor grado de dificultad 1 en Likert, cada punto de la escala equivale al 20% del total del mayor número de conceptos.

Definimos que el algoritmo RSA y Diffie-Hellman son los algoritmos con menos definiciones matemáticas mientras El Rabin y el Gamal poseen la mayor cantidad por lo que RSA y Diffie-Hellman requieren menos nociones previas con ello los estudiantes podrán comprender de mejor manera el algoritmo, los datos se resumen según en Gráfico N° 9.

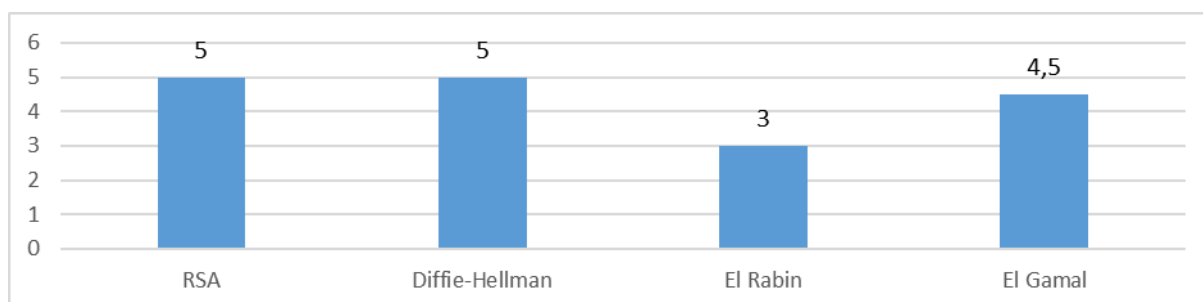


Gráfico N°9: Resumen Índice 9

Fuente: Autores

Elaboración: Autores

Índice 10 – Importancia de las Definiciones Matemáticas.- Se han determinado los conceptos matemáticos y su impacto en los algoritmos de cifrado por lo que se ha considerado que los conceptos de aritmética modular, números primos, inversión modular y algoritmos tienen un impacto bajo puesto que son conceptos que son fáciles de asimilar por los estudiantes , en cambio los

conceptos de teorema chino del resto, grupos finitos de número, algoritmo extendido de Euclides y la teoría de números son mucho más complejos de asimilar por lo que han sido considerados como altos, dados estos dos extremos no se han considerado impactos medios, los conocimientos que no poseen impacto son aquellos que son necesarios para comprender el algoritmo de criptografía mas no para aplicarlo estos datos producen valoraciones N/A qué quiere decir No se Aplica.

Los valores Likert han sido asignados de la siguiente manera: al impacto bajo se le ha dado una valoración de 5, al impacto medio 3 y finalmente alto impacto como 1 con esto podemos decir que el algoritmo RSA y Diffie-Hellman son algoritmos en donde los conocimientos matemáticos no son factores preponderantes para su aplicación con lo que obtenemos el Gráfico N° 10:

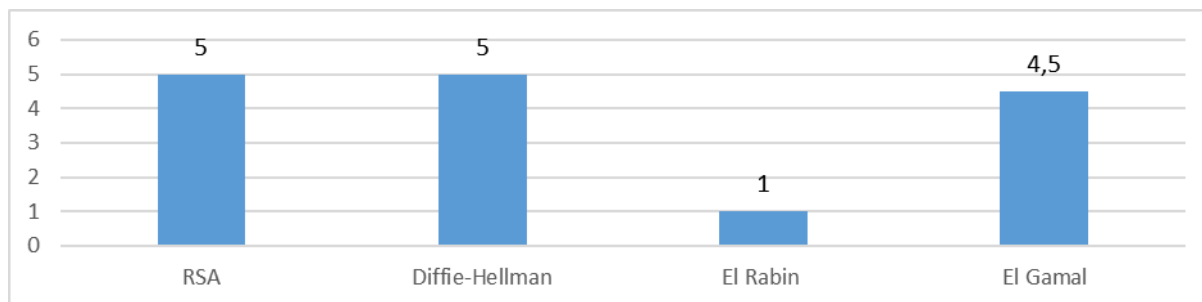


Gráfico N°10: Resumen Índice 10

Fuente: Autores

Elaboración: Autores

Variable Dependiente

Luego de haber obtenido los resultados de la variable independiente y determinado que el algoritmo RSA es óptimo para la enseñanza se realiza el estudio de la variable dependiente en donde se empleará la técnica de la encuesta para determinar entre los 4 escenarios de enseñanza a los estudiantes de séptimo semestre de la Escuela de Ingeniería en Sistemas, la encuesta se ha aplicado mediante los formularios de Google Docs. Obteniendo los siguientes datos:

Indicador 1- Nivel de Comprensión

El indicador de nivel de comprensión permitirá medir el nivel de asimilación de conocimientos de los algoritmos criptográficos al haber impartido los 4 escenarios planteados al séptimo semestre de la Escuela de Ingeniería en Sistema, para lo cual se han generado 4 índices que son:

- Entendimiento del Algoritmo Criptográfico
- Comprensión y Dominio de los Datos de Entrada
- Conceptualización del Algoritmo de Cifrado
- Conceptualización del Algoritmo de des Cifrado

Estos indicadores miden los conocimientos sobre la estructura de cada algoritmo criptográfico y se han tabulado de la siguiente manera:

Índice 1 – Entendimiento del Algoritmo Criptográfico.- Este índice permite medir de forma general cuánto ha entendido el estudiante todo el proceso del algoritmo criptográfico realizando la siguiente pregunta: ¿Considera Usted el Algoritmo RSA Comprensible?, la misma pregunta se ha realizado para los 4 algoritmos.

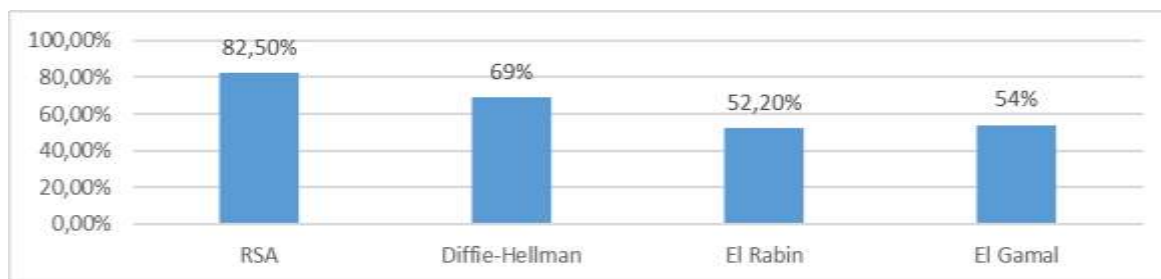


Gráfico N°11: Resumen Índice 1

Fuente: Autores

Elaboración: Autores

Luego de analizar los porcentajes y valoraciones en el Gráfico N° 11, se puede identificar que el algoritmo RSA ha sido el más comprendido de los 4 algoritmos criptográficos de 23 estudiantes encuestados en 4 cátedras dictadas, ha obtenido un 82,50% que corresponden a una valoración en la escala de Likert de 95 sobre 115 y en su opción totalmente de acuerdo 25 de 5 personas.

Índice 2 – Comprensión y Dominio de los Datos de Entrada.- El algoritmo Criptográfico entre sus componentes posee los datos de entrada y el algoritmo de obtención de datos, a través de estos se ha planteado la siguiente pregunta: ¿Considera Usted que la Obtención de los Datos de Entrada es un Proceso Fácil?

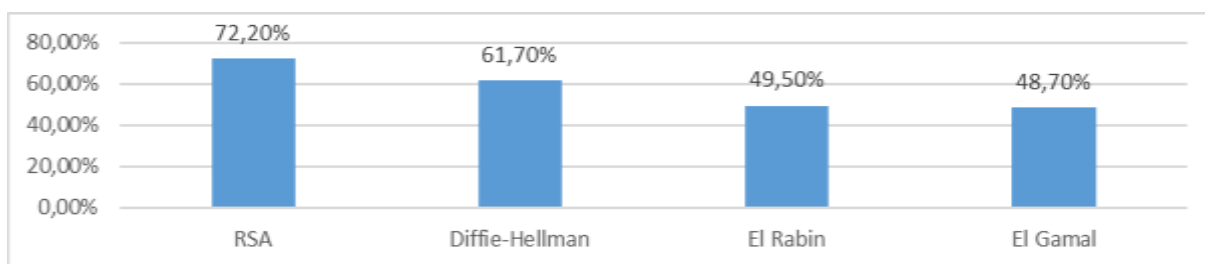


Gráfico N° 12: Resumen Índice 2

Fuente: Autores

Elaboración: Autores

Se ha permitido observar según el Gráfico N° 12, que el algoritmo criptográfico que más comprensión posee sido RSA con un 72,20% de valoración total, esta cifra corresponde a 83 puntos en la escala de Likert de 115 estimados, con 23 personas encuestadas, 16 personas están de acuerdo con la pregunta.

Índice 3 – Conceptualización del Algoritmo de Cifrado.- El algoritmo de cifrado de un algoritmo criptográfico permite que el usuario encripte el texto en claro antes de ser enviado mediante confusión y difusión de datos, empleando claves públicas y privadas, para su medición se ha generado la siguiente pregunta: ¿Defina cuánto ha comprendido del algoritmo de cifrado de "RSA"?

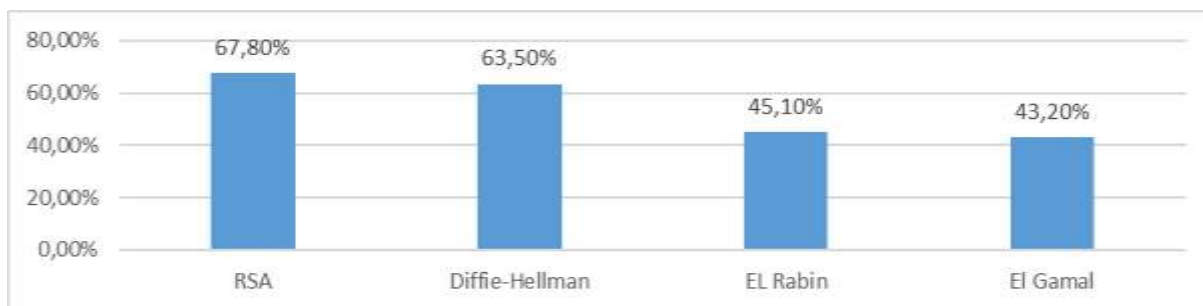


Gráfico N° 13: Resumen Índice 3

Fuente: Autores

Elaboración: Autores

El Gráfico N° 13 indica que, RSA en esta pregunta, es el algoritmo criptográfico que mejor permite el entendimiento de la encriptación de datos para los estudiantes, obtiene el 67,80% correspondiendo a una valoración Likert de 78 puntos sobre 23 encuestados con 9 personas que han optado por la respuesta de comprensión alta.

Índice 4 – Conceptualización del Algoritmo de DES Cifrado.- El algoritmo de descifrado de un algoritmo criptográfico permite que el usuario descifre el texto codificado en claro al ser recibido del emisor, para su medición se ha generado la siguiente pregunta: ¿Defina cuánto ha comprendido del algoritmo de descifrado de "RSA"?

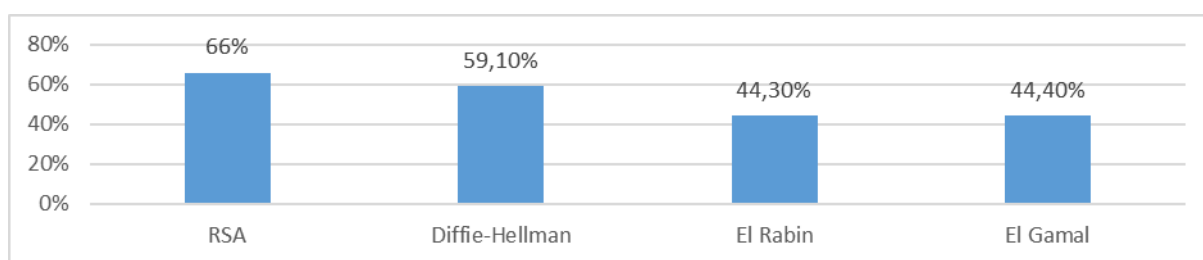


Gráfico N° 14: Resumen Índice 4

Fuente: Autores

Elaboración: Autores

En el nivel de comprensión del algoritmo de descifrado, según se observa en el Gráfico N° 14 que el algoritmo RSA tiene una valoración del 66% siendo la valoración más alta de los algoritmos, esto puede ser explicado por la simplicidad y el número de pasos del algoritmo, de 23 estudiantes encuestados 8 estudiantes han manifestado haber tenido una comprensión alta.

Indicador 2 – Nivel de Aplicación de Conocimiento

El indicador permite evaluar el nivel que poseen los estudiantes para aplicar todos los conocimientos adquiridos en las cátedras para lograr replicar los algoritmos criptográficos, desde la obtención de datos, su preparación, el algoritmo de cifrado y de descifrado, por lo cual se han generado los siguientes índices:

- El estudiante es capaz de implementar al menos un algoritmo criptográfico
- El estudiante es capaz de crear un algoritmo criptográfico personalizado
- El estudiante puede descifrar un texto encriptado

Índice 5 – El estudiante es capaz de implementar al menos un algoritmo criptográfico.- Para determinar si el estudiante es capaz de implementar un algoritmo criptográfico se ha generado la siguiente pregunta: ¿Cuán difícil le resultaría resolver un problema usando "RSA"?

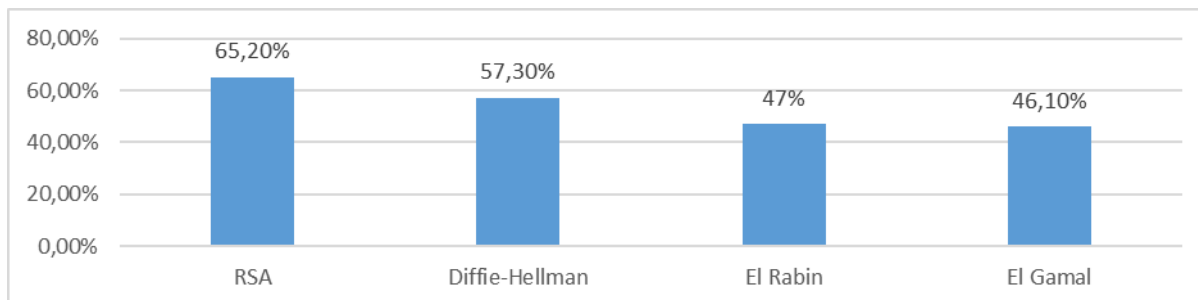


Gráfico N°15: Resumen Índice 5

Fuente: Autores

Elaboración: Autores

Se evidencia en el Gráfico N° 14, que los estudiantes consideran más fácil resolver un problema con el algoritmo RSA con una valoración de 65,20% de 115 puntos con 8 estudiantes que consideran fácil implementar este algoritmo de un total de 23 estudiantes.

Índice 6 – El estudiante es capaz de crear un algoritmo criptográfico personalizado.- Todo algoritmo criptográfico estándar posee una vulnerabilidad y es el conocimiento de su estructura es por ello que se ha generado la siguiente pregunta: ¿Podría Usted personalizar el algoritmo "RSA"?

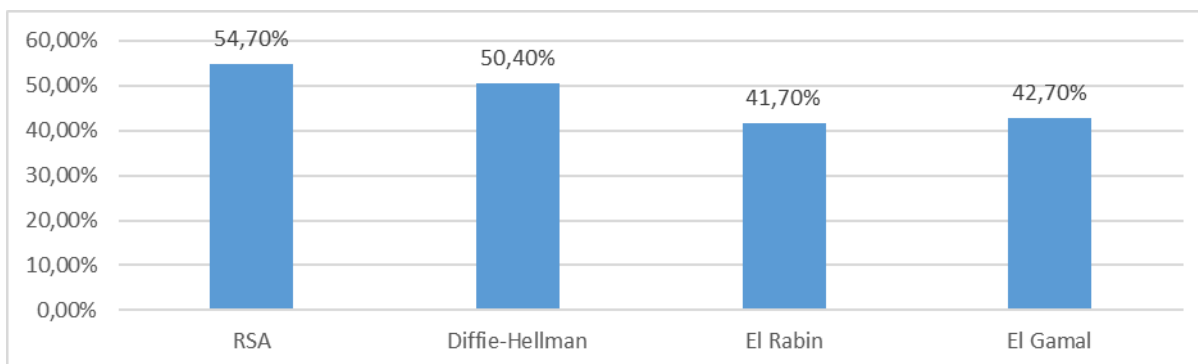


Gráfico N°16: Resumen Índice 6

Fuente: Autores

Elaboración: Autores

Se ha podido determinar según los datos expuestos en el Gráfico N° 16, que el algoritmo RSA es el algoritmo más personalizable para los estudiantes por lo cual ha obtenido una valoración del 54,70% de 115 puntos entre 23 encuestas donde 7 estudiante estuvieron de acuerdo.

Índice 7 – El estudiante puede descifrar un texto encriptado.- Se ha realizado la siguiente pregunta: ¿Cuán difícil le resultaría descifrar un mensaje usando "RSA"?

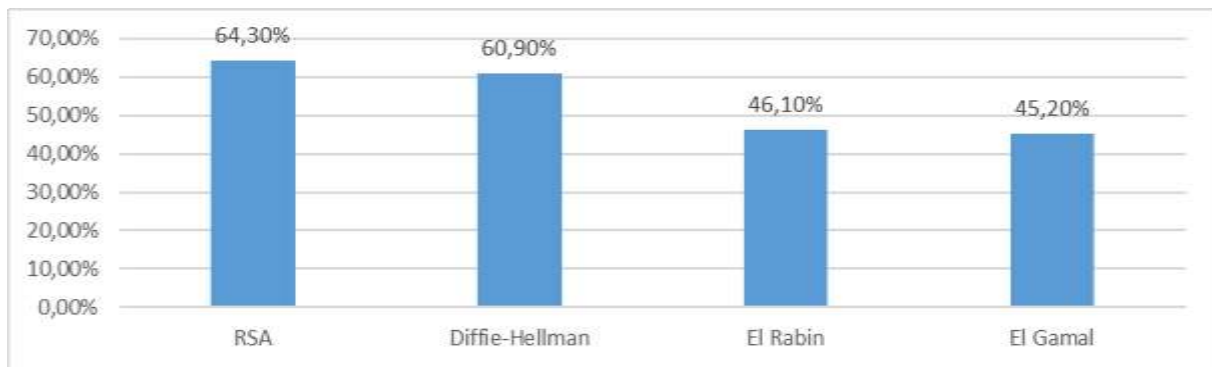


Gráfico N°17: Resumen Índice 7

Fuente: Autores

Elaboración: Autores

Se observa que los estudiantes consideran que es más fácil descifrar un texto en claro usando RSA por lo cual este algoritmo ha alcanzado una valoración de 64,30% de 115 encuestas entre 23 encuestados, como se puede apreciar en el Gráfico N° 17.

Indicador 3 – Conceptos Matemáticos

El indicador de conceptos matemáticos, permite medir el nivel de conocimientos que posee el estudiante en séptimo semestre, se ha asumido que los estudiantes ya han recibido cátedras sobre matemática de nivelación y matemática informática, se han generado varios índices dependiendo de cada algoritmo con su respectiva pregunta de la siguiente manera:

- Conocimiento sobre aritmética modular;
- Conocimiento sobre estructuras algebraicas;
- Conocimiento sobre logaritmos;
- Conocimiento sobre la obtención de raíces cuadradas;
- Conocimiento sobre el Teorema chino del resto;
- Conocimiento sobre el algoritmo Extendido de Euclides;
- Conocimiento sobre Curvas Elípticas;
- Conocimiento sobre Grupos Finitos;

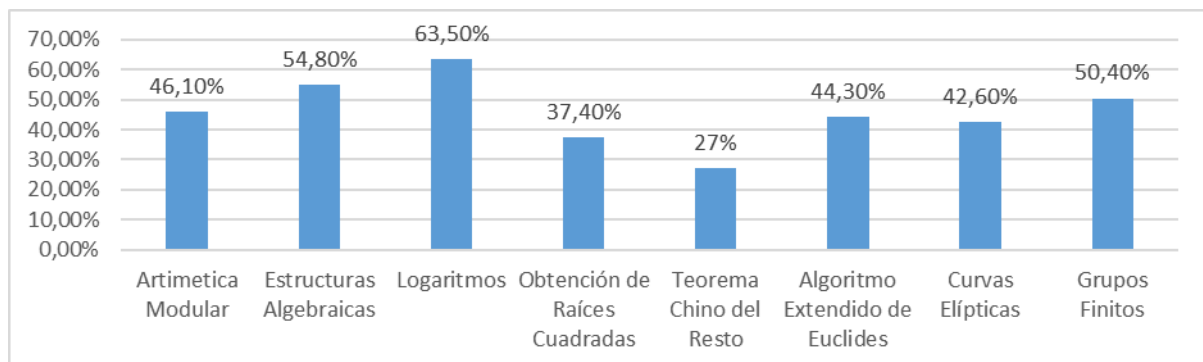


Gráfico N°18: Resumen Valoración Total Likert Indicador 3

Fuente: Autores

Elaboración: Autores

En el Gráfico N° 18, los estudiantes tienen un conocimiento alto sobre logaritmos con un 63,50% y en su defecto no tienen mucho conocimiento sobre el teorema chino del resto, hay que tomar en cuenta que estos porcentajes corresponden a un total de 115 puntos por cada concepto matemático a continuación se realizará un estudio del nivel de conocimientos matemáticos por cada algoritmo criptográfico, se discrimina los conceptos que se pueden asimilar rápidamente como es la conceptualización de números primos y operaciones matemáticas básicas, según muestra el Gráfico N° 19.

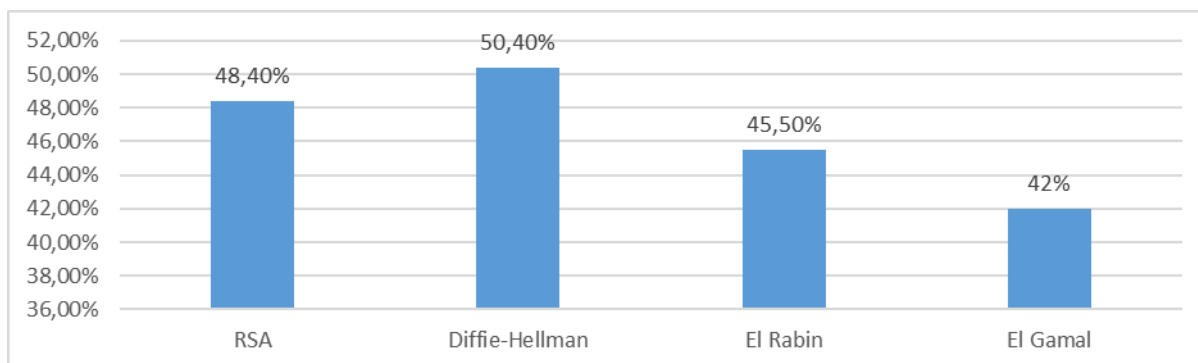


Gráfico N° 19: Resumen Conceptos Matemáticos

Fuente: Autores

Elaboración: Autores

Resumen del Análisis de la Variable Dependiente

Se pueden apreciar los resultados finales de las tabulaciones y comparaciones de los algoritmos criptográficos analizados en los 4 escenarios encuestados a los estudiantes del total de cada algoritmo por pregunta y por indicador se han verificado valores obtenidos y valores esperados, como se puede apreciar en el Gráfico N° 20.

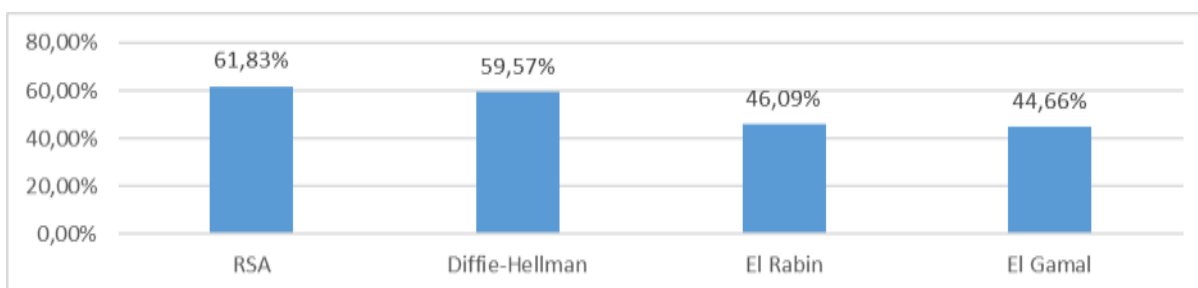


Gráfico N° 20: Resumen Variable Dependiente

Fuente: Autores

Elaboración: Autores

Prueba de Hipótesis Mediante el Estadístico χ^2 (Chi - cuadrado)

RSA vs DIFFIE-HELLMAN

Para realizar la comprobación entre estos dos algoritmos se plantea la Hipótesis general como particular para el caso de la siguiente manera:

H1: El Algoritmo RSA es Mejor que el Algoritmo Diffie-Hellman.

De esta hipótesis se abstrae la siguiente afirmación: H1: Existen diferencias significativas entre los procedimientos, con su correspondiente negación H₀: No hay diferencias entre los procedimientos. Para esta comprobación se emplea la tabla de contingencias observadas con los datos de los algoritmos en análisis en la Tabla N° 3:

Tabla 3: Tabla de Contingencia 3x2 con Frecuencias Observadas

Nivel de Enseñanza en la Criptografía Pública	Algoritmos de Criptografía		Total
	RSA	Diffie-Hellman	
Mejor	83	49	132
Indiferente	66	76	142
No Mejor	35	59	94
Totales	184	184	368

Fuente: Autores
Año: 2015

Frecuencias Esperadas

Para obtener las frecuencias esperadas se emplea la siguiente fórmula:

$$fe_{ij} = \frac{\text{Total Fila}_i * \text{Total Columna}_j}{N}$$

Dónde:

fe_{ij} = frecuencia esperada;

N = total de frecuencias observadas;

Al aplicar la fórmula se obtienen los siguientes valores esperados, que se visualizan en la Tabla 4:

Tabla 4: Tabla Frecuencias

Nivel de Enseñanza en la Criptografía Pública	Algoritmos de Criptografía		Total
	RSA	Diffie-Hellman	
Mejor	66	66	132
Indiferente	71	71	142
No Mejor	47	47	94
Totales	184	184	368

Esperadas

Fuente: Autores
Año: 2015

$\chi^2_{0,95} = 5.99$ Chi-cuadrado con $\delta = 2$ grados de Libertad y un $\alpha = 0.05$, $\chi^2 = 15.58$.

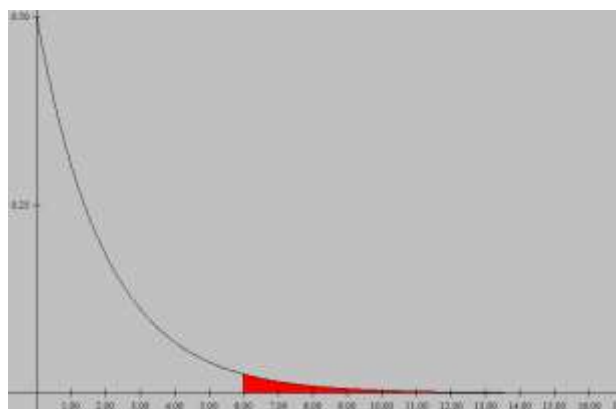


Gráfico N°21: Chi Cuadrado

Fuente: Autores

Elaboración: Autores

Al contrastar los valores de χ^2 se observa, en el Gráfico N°21, que el valor obtenido es superior al esperado por lo cual se desecha la H_0 y se acepta H_1 , es decir uno de los algoritmos es mejor que el otro al observar la tabla de frecuencias observadas se nota que RSA posee un valor de mejor de 83 y Diffie-Hellman de 49 por lo que se concluye que RSA es el mejor algoritmo para la enseñanza en la asignatura de criptografía en la EIS que Diffie-Hellman.

Para el caso de: RSA vs El Rabin, RSA vs El Gamal, se realizará un procedimiento análogo al RSA vs DIFFIE-HELLMAN.

RESUMEN DE LA COMPROBACIÓN DE LA HIPÓTESIS

Tabla 5: Resumen de la Comprobación de la Hipótesis

Comprobación	χ^2 con $\alpha = 0.05$ Y $\delta=2$	χ^2 Calculado	Prueba de H_0
RSA – Diffie Hellman	5,99	15,58	Acepta H_1
RSA – El Rabin	5,99	89,86	Acepta H_1
RSA – El Gamal	5,99	97,28	Acepta H_1

Fuente: Autores

Año: 2015

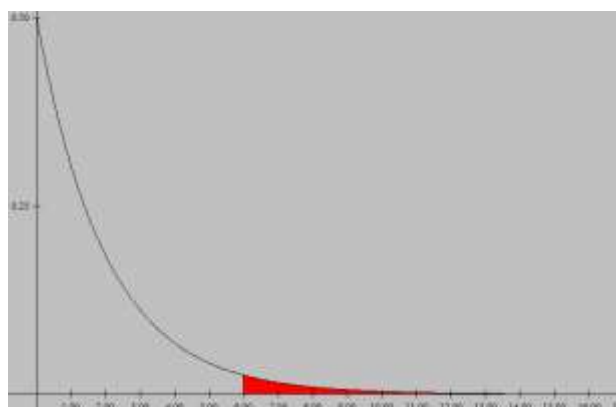


Gráfico N°22: Chi Cuadrado

Fuente: Autores

Elaboración: Autores

En la Tabla 5 así como en la Imagen Gráfico N° 22 se puede analizar claramente que en los resultados del Chi cuadrado calculado para la prueba de hipótesis los valores obtenidos son mucho mayores al valor de referencia, por lo que se ubican al lado derecho de la curva, tomando así la decisión de rechazar en todos los escenarios la H_0 y a su vez aceptar H_1 por lo que se llega a la conclusión general de que el Algoritmo RSA es el óptimo para la enseñanza de la asignatura de criptografía en la Escuela de Ingeniería en Sistemas de la ESPOCH, dado a que posee una mejor comprensión de su funcionamiento por parte de los estudiantes a más de comprenderse los datos necesarios, los procesos de cifrado y descifrado de la información, y para finalmente los conceptos matemáticos empleados en su uso no son de una complejidad alta sino que pueden ser adquiridos por los estudiantes.

CONCLUSIONES

Se ha realizado un estudio de la fundamentación matemática que poseen los 4 algoritmos de criptografía pública propuestos en este trabajo en donde resaltan conceptos como: Aritmética Modular, Estructuras Algebraicas, Logaritmos discretos, Obtención de Raíces Cuadradas (en aritmética modular), Teorema Chino Del Resto, Algoritmo Extendido de Euclides, Curvas Elípticas, Grupos Finitos, anillos de Polinomios, y se evidencia que los estudiantes poseen más conocimientos matemáticos sobre el algoritmo Diffie-Hellman con un 50,4% que El Rabin (45,5%), El Gamal (42,0%), y pueden ser similares o iguales a los del Algoritmo RSA (48,4%). Este resultado de tener mayor conocimiento matemático sobre el algoritmo Diffie-Hellman (genera clave común sin haber enviado) se debe a que este algoritmo no encripta y desencripta mensajes a diferencia de los otros y es ahí donde se requiere mayor conocimiento matemático.

Se ha determinado los parámetros del análisis comparativo de los algoritmos en 4 secciones a cada uno según su metodología de desarrollo, las cuales son número de datos de entrada, algoritmo de preparación de los datos de entrada, algoritmo de cifrado del texto en claro y algoritmo de descifrado con lo que se ha podido estandarizar los algoritmos de criptografía pública y se ha realizado un análisis en donde el algoritmo RSA resulta ser el más óptimo (50/50 en la valoración técnica) para la enseñanza de la cátedra de criptografía que los algoritmos Diffie-Hellman(30/50), El Rabin(26/50), El Gamal(24/50).

Se ha realizado cuatro escenarios de prueba para la enseñanza de la cátedra de criptografía, estos escenarios comprenden una breve explicación del funcionamiento de cada uno de los algoritmos criptográficos y los conceptos matemáticos necesarios para su comprensión con la finalidad de distinguir con el grupo de estudiantes cual provee mejor asimilación de contenidos, obteniendo como resultado RSA el más óptimo (45,1%) sobre los algoritmos Diffie-Hellman (26,6%), El Rabin(7,6%), El Gamal(6,5%).

Mediante la realización de la prueba de Hipótesis con el estadístico chi-cuadrado, con $\alpha = 0,05$ y $\delta = 2$ el $X_{0.95}^2 = 5.99$ se ha llegado a la conclusión de que el Algoritmo RSA es el más adecuado para la enseñanza de la asignatura de criptografía puesto que se contrastó con los demás algoritmos obteniendo con Diffie-Hellman $[X]_{0.95}^2 = 15,58$, con El Rabin $[X]_{0.95}^2 = 89,86$, con El Gamal $[X]_{0.95}^2 = 97,28$, valores que están alejados del valor referencial $X_{0.95}^2 = 5.99$ es el algoritmo con menor número de pasos para cifrar y descifrar la información además posee conceptos matemáticos como la aritmética modular y estructuras algebraicas que ya son de conocimiento de los estudiantes así como también de fácil comprensión, estas características permiten que el funcionamiento de RSA sea de fácil asimilación por ente el principio de la criptografía también.

Bibliografía

Actualización Malla Curricular: Carrera de Ingeniería en Sistemas, (2013) Escuela de Ingeniería en Sistemas (ESPOCH), Riobamba, Ecuador.

Bandura, A. (1986). *Social foundations of thought and action: A social cognitive theory*. Madrid.

Blanco, R. (2010). *Dspace Instituto Politécnico Nacional*. Obtenido de <http://tesis.ipn.mx/bitstream/handle/123456789/6239/IF2.45.pdf?sequence=1>

Consejos de Seguridad, Seguridades en Banca Virtual y Banca Móvil, (2015) Banco de Guayaquil, Ecuador. Obtenido de: <http://bancodeguayaquil.com>

Departamento de Sistemas Informáticos y Computación. (s.f.). *Universitat Politècnica de Valencia*. Obtenido de <http://users.dsic.upv.es/asignaturas/eui/cri/rsa.pdf>

Facultad de Informática y Electrónica. (30 de Enero de 2013). *ESPOCH*. Obtenido de ESPOCH: http://espoch.edu.ec/Descargas/facultadpub/MALLA_CURRICULAR_SISTEMAS_ac993.PDF

Fernández, A. (2006). *Metodologías Activas para la Formación de Competencias*.

Garrido, I. (1996). *Psicología de la motivación*. Madrid.

Ibáñez, F. (2012). *Universidad Nacional de Colombia*. Obtenido de <http://www.bdigital.unal.edu.co/7238/1/fernandolbanezrincon.2012.pdf>

Lucena, M. (2009). *Criptografía y Seguridad en Computadores*.

Morales, A. (2009). *Dspace del Instituto Politécnico Nacional*. Obtenido de <http://tesis.bnct.ipn.mx/bitstream/handle/123456789/8870/ANALGOR.pdf?sequence=1>

Morales A. Gallegos G. Toscano L. (2008). *Análisis de los algoritmos de cifrado de llave secreta y su uso dentro de una organización pública*. México, México.

Pintrich, G. (1992). *El aprendizaje cooperativo. Una alternativa eficaz a la enseñanza tradicional*. Barcelona.

Tapia, J. A. (1992). *Motivar en la adolescencia: teoría, evaluación e intervención*. Madrid.