ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

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

AUTOR:

Mario Humberto Paguay Cuvi

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”.

Riobamba – Ecuador

Junio 2015

CERTIFICACION

El trabajo de investigación titulado: **"ANÁLISIS DE ALGORITMOS MATEMÁTICOS DE CRIPTOGRAFÍA PÚBLICA PARA MEJORAR EL APRENDIZAJE DE LA MATERIA DE CRIPTOGRAFÍA EN LA CARRERA DE INGENIERÍA EN SISTEMAS DE LA ESPOCH",** de responsabilidad del Dr. Mario Humberto Paguay Cuvi, ha sido prolijamente revisado y se autoriza su presentación.

Tribunal de Tesis:

Ing. William Pilco. Ms.C.
PRESIDENTE _____

Ing. Gloria Arcos Medina. Ms.C.
TUTORA. _____

Dr. Mario Audelo. Ms.C.
MIEMBRO. _____

Dr. Rigoberto Muñoz. Ms.C
MIEMBRO. _____

COORDINADOR SISBIB ESPOCH _____

DERECHOS INTELECTUALES

Yo, Mario Humberto Paguay Cuvi, soy responsable de las ideas, doctrinas y resultados expuestos en el presente proyecto de investigación; y el patrimonio intelectual generado por la misma pertenece a la ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO.

_____

Mario H. Paguay C.
CI: 0601807829

DEDICATORIA

Dedico este trabajo de titulación a mi familia quienes han sido el pilar fundamental para buscar mi superación personal, a mi esposa Mayra Alvarado por ser aquella fuente inagotable de inspiración, por acompañarme y alentarme día a día en mis jornadas laborales, a mis hijos Alejandrita y Marito quienes son aquel faro que me guía hacia la felicidad en los momentos más duros, por ser esa sonrisa que jamás falta en el hogar, por tantas alegrías con sus triunfos, a mis amigos y demás compañeros que me han apoyado para que todas mis metas se cumplan.

Mario H. Paguay Cuvi.

AGRADECIMIENTO

Quiero expresar un sincero y profundo agradecimiento a la Escuela Superior Politécnica de Chimborazo por permitirme haber cursado el programa de estudios de maestría para culminar un sueño más de mi carrera profesional.

A mi tutora Ing. Msc. Gloria Arcos por haber guiado este trabajo de titulación de la forma acertada, por impartirme sus conocimientos en la elaboración de la investigación, a los miembros del tribunal de la Tesis quienes supieron brindarme sus sabios consejos y la guía oportuna.

A todas aquellas personas que han intervenido de alguna u otra forma en el proceso de realización de este proyecto para que culminara con éxitos, mi más profundo agradecimiento.

Mario H. Paguay Cuvi.

ÍNDICE

LISTA DE TABLAS

LISTA DE GRÁFICOS

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 Escuela Superior Politécnica de Chimborazo, se selecciono el algoritmo más adecuado para mejorar el aprendizaje de la materia de criptografía. Se desarrollo ambientes de prueba sobre RSA, 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 definio 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 Escuela de Ingenieria en Sistemas para que estos conceptos sean añadidos a las asignaturas de matemática lo cual beneficiará al estudiante a la mejor comprensión de la asignatura.

PALABRAS CLAVE:
<ALGORITMOS CRIPTOGRAFICOS><ALGORITMOS> <CRIPTOGRAFIA>
<ESTRUCTURAS ALGEBRAICAS><MATEMÁTICA MODULAR>

SUMMARY

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 Polytechnic School of Chimborazo, it was selected the most appropriate algorithm to improve the learning of the subject of cryptography. 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 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 Computer Systems Engineering School for these concepts to be added to the mathematics courses which will benefit the student to a better understanding of the subject.

CAPÍTULO I:

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.

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.

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, el presente trabajo de maestría 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.

La presente tesis de maestría se encuentra organizada en 4 capítulos: Introducción en el cual se exponen el planteamiento del problema, la justificación, los objetivos e hipótesis del estudio, el marco de referencia es el segundo capítulo en donde se analizan la historia y principales algoritmos de la criptografía pública, el tercer capítulo contiene el diseño de la investigación y el marco hipotético en donde se realizará un estudio de los algoritmos de clave pública y finalmente el cuarto capítulo contiene el análisis e interpretación de los resultados, comprobación de la hipótesis, finalmente conclusiones y recomendaciones.

1.1. Planteamiento del Problema

El incremento de las redes de comunicación en el mundo digitalizado así como el continuo avance del internet ha generado problemas de diversa índole, tanto como en el filtrado de la información, ataques por grupos de hackers en los cuales las celebridades no han quedado afuera cuando se filtró información de sus cuentas de iCloud, a más de ataques de información privada se dan ataques al sector público incluso se han hackeado cuentas a los presidentes de varios países.

Con la finalidad de dar una solución a este tipo de inconvenientes nace la criptografía pública que consiste en el estudio de algoritmos matemáticos que permiten asegurar la información, estos algoritmos permiten que el envío de datos de un usuario a otro sea seguro o al menos lo más confiable posible, si un atacante intercepta estos datos serán incomprensibles, esto se debe a las estructuras matemáticas, conceptos, teorías de números involucrados añadiéndole el factor informático a la criptografía. Para un estudiante de la EIS de la ESPOCH es de vital importancia el estudio de la criptografía ya que al generar sistemas de información automatizados estos pueden albergar información sumamente importante por ejemplo un sistema bancario, un sistema gubernamental, los mismos que deben guardar confidencialidad.

Si estos sistemas no poseyeran un mecanismo criptográfico fácilmente se podría vulnerar el sistema o su base de datos, por lo cual es vital mantener claves de usuario, servidores en secreto, a más de ello transmitirlos y procesarlos a través de un medio de comunicación inseguro como es el internet. En la asignatura de criptografía de la EIS se imparten los conocimientos sobre cómo asegurar los datos y dentro de los cuales existen infinidad de conceptos y aplicaciones, 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.

Al analizar la malla curricular de la EIS (Facultad de Informática y Electrónica, 2013, pág. 1), se nota que existen temas de la matemática aplicada a la criptografía que no se imparten en la carrera como por ejemplo grupos finitos, anillos de polinomios, curvas elípticas, matemática modular que entre otros son los que más se usan para encriptar y desencriptar por lo que se genera una brecha que puede afectar al aprendizaje de la asignatura es por ello que el presente estudio busca determinar el algoritmo criptográfico más óptimo para la enseñanza de la asignatura.

1.2. Justificación

La criptografía se encuentra actualmente definida como una de las principales ramas de la informática y de igual forma se encuentre interrelacionada con la matemática por lo que influye de forma significativa en la carrera de Ingeniería en Sistemas, la criptografía no se enseña de forma particular o con un estándar en específico por lo que se debe entender el concepto de criptografía desde distintas fuentes para un fin único la seguridad de los datos o de la información.

Los algoritmos criptográficos pueden ser analizados de diversos ámbitos: la informática, la matemática, se lo puede analizar por la propia teoría de algoritmos en incluso por la dificultad para su criptoanálisis con lo que es primordial realizar un enfoque de la asignatura entorno a la carrera. El objetivo principal de un estudiante de Ingeniería en Sistemas no es crear un algoritmo criptográfico pero si emplearlos de forma adecuada, pero qué conceptos previos debe tener el estudiante, qué algoritmo es el más adecuado para su aplicabilidad, son preguntas que no se pueden resolver de forma concreta ya que cada algoritmo tiene una creación y conceptualización distinta al menos en el ámbito matemático.

La deficiente asimilación de estos conceptos acarreará en un futuro problemas en la creación de sistemas informáticos, aplicaciones y desarrollo de software inseguro, con lo que los estudiantes no se mostrarán competentes en el ámbito profesional. Es por este motivo que se realizará un estudio comparativo de los algoritmos criptográficos con la finalidad de optimizar la asimilación de estos conceptos en los estudiantes a más de ello dejar información relevante para la carrera con los conceptos matemáticos necesarios a impartir y que deberían recibir los estudiantes en sus niveles de formación en la malla curricular.

1.3. Objetivos

1.3.1. *Objetivo General*

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.

1.3.2. *Objetivos Específicos*

1. Estudiar las teorías matemáticas en la que se fundamenta la criptografía pública.
2. Definir los parámetros para realizar el análisis de los algoritmos de criptografía pública.
3. 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.
4. Seleccionar el algoritmo más adecuado para mejorar el aprendizaje de la materia de criptografía en la carrera de Ingeniería en Sistemas Informáticos de la ESPOCH.

1.4. *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.

CAPÍTULO II:

MARCO DE REFERENCIA

En este capítulo se analizará de forma breve todos los conceptos necesarios para realizar el trabajo de investigación que busca determinar el mejor algoritmo para la enseñanza de la asignatura de criptografía en la Escuela de Ingeniería en Sistemas en la ESPOCH para lo cual se iniciará con la historia de la criptografía en donde se hará un recuento de los primeros algoritmos criptográficos y su uso, luego se analizarán los conceptos que se manejan en la teoría de los algoritmos criptográficos, la mayoría de las definiciones matemáticas que fundamentan la asignatura, al final se estudiarán los principales algoritmos criptográficos de clave pública con lo que será el punto de partida para generar el estudio comparativo.

2.1. Historia de la Criptografía

La criptografía ha sido usada desde tiempos antiguos para mantener la confidencialidad de la información muchos de estos usos que se le ha dado viene originado por las guerras, para comunicar las tácticas y técnicas a usarse en el campo de batalla desde los mandos superiores a sus tropas, el éxito de una batalla se reduce por lo tanto a interceptar y descifrar los mensajes enemigos. Los primeros usos de la criptografía se remonta la época de los espartanos en donde se usaba una vara de madera de un diámetro especifico, el cual tenían tanto emisor como receptor, el mensaje se escribía en una cinta de cuero que se enrollaría después en la vara especificando su inicio para que el mensaje coincidiera. La cinta por si sola posee un mensaje incoherente más al combinarla con los códigos de columna de inicio tendría sentido para el remitente.

Gráfico 1-1: Criptografía Espartana
Fuente: (Gutiérrez, 2012)

El siguiente método se llama tabla de Polybio por el historiador que lo diseño, consiste en una tabla o matriz de cinco (5) x cinco (5) la cual contenía cada letra del alfabeto con una correspondiente dupla del código de la tabla.

	A	B	C	D	E
A	A	B	C	D	E
B	F	G	H	U	K
C	L	M	N	O	P
D	Q	R	S	T	U
E	V	W	X	Y	Z

Gráfico 0-2: Cifrado de Polybio
Fuente: (informatixo, 2011)

En la antigua Roma los ejércitos de Julio César necesitaron cifrar los mensajes del emperador para ser llevados a las líneas del ejército con órdenes para los combates, esta técnica de cifrado se conoció como el cifrado cesar, era un método en el cual cada letra del mensaje original consistía en una letra del alfabeto pero sumadas tres (3) veces su posición, con ello el mensaje original quedaba oculto y seguro. Tomando en cuenta que ya se hace uso de una matemática básica para soporte, juegos de coordenadas, posiciones.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	Y	W	X	Y	Z	*Alfabeto Plano*
T	U	Y	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	*Alfabeto Cifrado*

Gráfico 3-3 Cifrado de Julio César
Fuente: (Bacon, 2013)

En el siglo XV se dan los primeros pasos hacia la criptografía moderna introduciendo los conceptos de confusión y difusión de Claude Shannon, el disco de Alberti era un cifrado de clave secreta que consistía en dos discos, estos discos proveían un mensaje cifrado el cual no poseía correspondencia con el método usado, el anillo eterno poseía veinte (20) letras más 4 números el interno tenía las mismas letras y números pero en minúsculas pero en orden inverso añadiendo el carácter &.

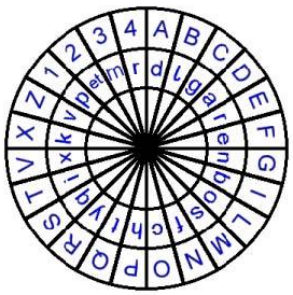


Gráfico 4-4 Discos de Alberti
Fuente: (Violat)

El tablero de Vigenere es una variación de Alberti, que usa una matriz originada por el mensaje a cifrar y una palabra clave reiterativa, la letra del mensaje más la letra de la palabra clave representan una letra del alfabeto, y este alfabeto es originado de los veinte y seis (26) alfabetos de cesar en orden. En el Siglo XVIII Beaufort crea un cifrado inverso del anterior en donde la letra de la palabra clave más la letra del alfabeto de cesar genera la letra del mensaje cifrado.

Gráfico 5-5 Tablero de Vigenere
Fuente: (Widener University)

En 1917 se crea el primer sistema criptográfico seguro ideal según la teoría de SHANNON, era el sistema de Vernan que consistía en tener una clave de cifrado al menos tan larga como el mensaje original, transcrito a un alfabeto binario de cinco (5) dígitos por cada carácter a cifrar esto se realiza con probabilidad la operación módulo veinte y seis (26) así como una operación OR entre las cadenas para obtener el mensaje final, su uso fue mayormente militar durante la segunda guerra mundial, pero otro método surgió en este periodo del tiempo con el auge de la guerra la máquina ENIGMA dejando atrás los cifrados imprecisos a mano, aunque en Estados Unidos ya existían patentes de equipos criptográficos como SIGABA, en Japón Purple y de esta era criptográfica no solo se benefició el ejército sino también bancos e industrias por medio de la creación de la compañía Aktiebolget Cryptograph. (Solana. 2009, pag. 24)

Enigma y Lorenz fueron los mecanismos criptográficos más empleados en la segunda guerra mundial y el criptoanálisis de los mismo le dieron al ejército aliado la victoria al conocer los mensaje secretos de Alemania, Enigma era una máquina que implementaba ya una matemática compleja consistía de tablero, panel de visualización y rotores, primero fue un rotor luego a tres (3), luego los rotores fueron intercambiable así dando la posibilidad de 17.576 posiciones de letras, a este tiempo ya se encontraba en auge también el criptoanálisis que es el arte de encontrar los mensajes originales desde un

mensaje cifrado, dentro del marco del proyecto Enigma por medio Alemán, los Británicos poseían el Proyecto ULTRA que básicamente buscaba romper el cifrado de Enigma, cuya única debilidad era que dos mensajes no pueden ser codificados en sí mismos, es decir ninguna letra debe coincidir entre el resultado y el mensaje ingresado.

Lorenz fue un cifrado mucho más complejo aún que Enigma pero también fue construida la máquina COLOSSUS para obtener el mensaje. Con surgimiento de la computación brevemente los métodos indescifrables y seguros se fueron quedando de lado, la potencia operacional y la matemática de ese entonces comenzaban a dar origen a cifrados mucho más potentes y revelando el criptoanálisis de otros.

2.2. Conceptos básicos

Al conocer ya mejor la historia de la criptografía en este capítulo definiremos algunos de los términos más empleados cuando se habla de criptografía, la palabra criptografía proviene de los términos griegos “KRIPTOS” y “GRAPHOS” que quiere decir escritura oculta, a más de este concepto el tesista propone delinear los siguientes:

Criptosistema

Según (Navarro, Ciarlante, & Sanhueza, pág. 4) un criptosistema es una 5-upla donde:
M: conjunto de todos los mensajes sin cifrar (texto claro).
C: conjunto de todos los posibles mensajes cifrados, o criptogramas.
K: conjunto de claves que se pueden emplear en el criptosistema.
E: conjunto de transformaciones de cifrado o familia de funciones que se aplica a cada elemento de M para obtener un elemento de C
D: conjunto de transformaciones de descifrado, análogo a E.
Todo criptosistema ha de cumplir la siguiente condición:

$$D * k\big(E * k(m)\big) = m$$

Criptosistema de llave pública

La criptografía asimétrica fue propuesta en 1976 por Diffie y Hellman, es aquel método que utiliza algoritmos de llave asimétrica, para lo cual las claves tanto para el cifrado como el descifrado son distintas. Esta usa un par de clases para envío de mensajes, usando llaves criptográficas pública y privada.

Una llave o clave pública es entregada a cualquier persona, es decir que puede ser distribuida ampliamente. Los mensajes se cifran mediante la llave pública perteneciente al destinatario.

Criptosistema de llave privada

Es el sistema de cifrado más antiguo y consiste en el conjunto de métodos que permiten tener comunicación segura entre las partes siempre y cuando anteriormente se hayan intercambiado la clave correspondiente, clave privada o simétrica. La simetría se refiere a que las partes tienen la misma clave tanto para encriptar el mensaje como para desencriptarlo.

La desventaja de utilizar este sistema de criptografía implica que si un tercero accede a esa clave secreta podrá descifrar el mensaje (Pascale, 2000, pág. 4).

Criptoanálisis

El criptoanálisis consiste en la reconstrucción de un mensaje cifrado en texto simple utilizando métodos matemáticos. Por lo tanto, todos los criptosistemas deben ser resistentes a los métodos de criptoanálisis. Cuando un método de criptoanálisis permite descifrar un mensaje cifrado mediante el uso de un criptosistema, decimos que el algoritmo de cifrado ha sido decodificado (Kioskea, 2014).

Encriptar – Desencriptar

Encriptar es la acción de transformar información entendible a información legible solamente mediante una clave. Se implementa la encriptación como medida de seguridad, la cual es usada para almacenar y transportar información delicada de tal manera que no pueda ser comunicada a terceros. Para lograr este objetivo se utilizan complejas fórmulas matemáticas.

La desencriptación es la acción contraria a la encriptación, pues se busca obtener la información legible a través de la información encriptada. Al momento de desencriptar se debe utilizar una clave como parámetro para las complejas fórmulas matemáticas usadas para la encriptación.

Confusión y Difusión

Confusión es el arte de mezclar, permutación la información, mediante cualquier conjunto de algoritmos para que provocar distracción, el método de difusión consiste en mantener el texto cifrado de la forma más compleja posible (Botaya, 2005, pág. 18)

Esteganografía

Según (Instituto Nacional de Tecnologías de la Comunicación, (s.f.), pag. 11) este es el procedimiento que permite ocultar mensajes o información dentro de otros, para que mediante esto la información pase desapercibida. Para ello no se necesita que la información este encriptada o que este oculta a la vista de todos, ya que mediante la esteganografía, dicha información pasará desapercibida.

Autenticación

Por lo general al realizar una autenticación hacemos referencia a la comprobación de la veracidad de un elemento, agente, o persona como confiable de acuerdo a criterios definidos (Santiango, 2006).

2.3. Fundamentos de la Criptografía

2.3.1. *Cantidad de Información*

La cantidad de información de un suceso viene dado como la medida de la disminución de la incertidumbre del mismo o al grado de la improbabilidad de que haya sido construido al azar, nos da más información cuando desconocemos un evento que cuando lo conocemos Shannon define a la cantidad de información como la probabilidad de ocurrencia de un suceso así: (Lucena, 2009, págs. 42, 43, 48, 61, 70, 176,182)

$$I_i = -\log_2(P(x_i))$$

Donde la probabilidad del suceso $P(x_i)$ si llegara a ser máxima no aportaría información caso contario si fuera casi nula, la cantidad de información sería infinita.

2.3.2. *Entropía*

Entropía en cambio en la cantidad de información que se conoce de dicho evento y que por lo general no aporta información adicional o nueva, la entropía de una variable aleatoria se define como el número necesario de bits para codificar el mensaje y está representada según Shannon por la siguiente ecuación: (Lucena, 2009)

$$H(v) = \sum_{i=1}^{n} P(x_i)\log_2[\frac{1}{P(x_i)}]$$

Donde H(v) se conoce como la entropía de la variable aleatoria V y $P(x_i)$ como la probabilidad del estado de x_i, las propiedades de la entropía de una variable son:

- La entropía de una variable aleatoria no es menor que 0 ni mayor que el $\log_2(N)$.
- La entropía es igual a 0 si y solo sí la probabilidad del estado x_i sea 1 y x_j sea 0 para todo evento j distinto de i.
- La entropía de n variables aleatorias es igual a la entropía de n+1 variables aleatorias si la probabilidad de la variable aleatoria n+1 es 0.

Para medir de forma más simple la cantidad de información se toma como unidad básica el bit, puesto que solo puede tener dos estados y así ser igual a la unidad, es por ello que se emplea logaritmos base 2, para codificar los mensajes se los representa por bits y se mide la entropía para determinar la cantidad de bits a usar.

La entropía condicionada emplea dos eventos o variables, suponiendo que no se conoce a la variable X pero de esta se sabe que está condicionada por y, por lo que al conocer y conoceríamos más sobre la variable X resultando así el teorema de la disminución de la entropía, por ente al conocer más sobre los sucesos no disminuye nuestra incertidumbre por lo que no aumenta nuestra cantidad de información. La cantidad de información de dos variables siguiendo la teoría de entropías del mismo autor se expresa por: $I(X,Y) = H(Y) - (Y/X)$ en donde el conocimiento de X implica una disminución de la entropía de Y, las propiedades de esta ecuación son: conmutativa y que la incertidumbre de los eventos siempre será mayor o igual que 0.

2.3.3. *Criptosistema seguro y redundancia del lenguaje*

El Criptosistema seguro es aquel sistema en donde su mensaje a cifrar posee la misma longitud de caracteres o bits que la clave que se usará, así como la clave no debe dar información sobre el contenido cifrado es decir sobre su mensaje original, pero en el lenguaje natural existe la redundancia de información y hay que tomar en cuenta este factor al momento de generar claves, en el lenguaje en español por lo general cuando un mensaje es incompleto se puede deducir la información faltante por medio de la redundancia es decir la repetición de ciertos patrones de palabras que el emisor usa en el mensaje, similar a la capacidad del cerebro humano de pasar por alto o incluir letras que en una lectura de un párrafo.

En el uso de claves por intuición y mala práctica encontramos claves como 123456, password que por más que sean sometidas a procesos de cifrado se las puede digitar por simple intuición. Aplicaciones que se manejan en este entorno son por ejemplo el código de redundancia cíclica que permite introducir un bit o carácter a un mensaje para generar la mayor redundancia posible.

Los ataques por fuerza bruta aprovechan estas facilidades del lenguaje natural de las personas para así asociar un criptoanálisis a un determinado mensaje, buscando por lo general opciones de palabras acertadas, dado que los resultados de hacer son imposibles de visualizar para las personas ya que estos ataques por lo general se los realiza por medios informáticos y algoritmos de criptoanálisis, una forma de prevenirlos es la compresión del mensaje cifrado. (Lucena, 2009)

2.4. Teoría de algoritmos

La teoría de algoritmos nos lleva a identificar una solución óptima de un problema y el tiempo que demora en ejecutarse esta solución, un algoritmo es un conjunto finito de pasos que permiten la resolución de un problema, las computadoras son capaces de ejecutar algoritmos, y a velocidades distintas, hoy en día las supercomputadoras son capaces de ejecutar muchas operaciones matemáticas por segundo por su CPU en la unidad aritmético lógica, pero cuanto es la diferencia entre un computador promedio y un súper computador al resolver una serie de algoritmos, la teoría de algoritmos permite conceptualizar el término de *invarianza,* el mismo que induce a la compresión de que el tiempo de ejecución de un algoritmo es constante en cualquier computador siempre y cuando el conjunto de datos de entrada del algoritmo sea considerado sumamente extenso.

Si para encriptar la información ya no tenemos en cuenta el tiempo que se demora un computador en resolver o criptoanalizar el algoritmo entonces podemos concentrarnos en los conceptos de Shannon sobre los criptosistemas seguros y la longitud de la clave lo que nos lleva a la complejidad algorítmica a usarse para lograr llegar a los objetivos, La complejidad algorítmica no es más que la notación asintótica del tiempo que se demora en ejecutar el algoritmo dado su orden o grado y a este orden o grado se lo denomina orden de ejecución y dará una pauta para conocer cómo crece el tiempo a medida que se resuelve el algoritmo de la siguiente forma:

1) $f(n) = O\big(g(n)\big)$

2) $f(n) = \Omega(g(n))$

En 1 la función f con datos de entrada n crece asintóticamente pero no más rápido que la función g con datos de entrada n multiplicada por una constante tiempo polinomial por ejemplo f(n) = 20n + 100 (eficientes) así en 2 la función f crece al menos tan rápido como g multiplicada por una constante tiempo exponencial (no eficientes) n!= $\Omega\ 2^n$, para que los fines pertinentes las funciones deben estar definidas en $\mathbb{N}$ y sus respuestas en $\mathbb{R}^+$.
Tomando en cuenta que nuestro conjunto de entrada debe ser extenso y que nuestra unidad de medida es en bits se definirá la entrada de las funciones como los logaritmos en base dos de los datos de entrada, con esta notación definiremos las siguientes operaciones de complejidad:

Suma y Resta: $O(\log_2 a + \log_2 b) = O(\log_2 n)$
Multiplicación y División: $O(\log_2 a \,.\log_2 b) = O((\log_2 n)^2)$

Siendo a y b valores de entrada menores o iguales a n, Manuel Lucena nos recuerda que la base del algoritmo no determinar el tiempo de ejecuciones. Así el tiempo de ejecución en función de los datos de entrada se mantiene igual ya se ejecute en un computador a16, 32, 64 bits en algoritmos determinísticos, los algoritmos probabilísticos son mucho más complejos y su resolución conlleva un tiempo de ejecución mucho mayor, puesto que no se siguen secuencias finitas y especificas sino que depende de parámetros que variaran dependiendo del problema, su tiempo de ejecución es de forma límite superior conceptualizando un tiempo polinomial para los valores de entrada aleatorios (Lucena, 2009).

2.5. Matemática modular

2.5.1. *Conceptos básicos de la matemática modular*

La aritmética modular es un conjunto de métodos que permiten determinar clases de congruencias entre número dentro del dominio de los enteros con simbología ($\mathbb{Z}_n$) introducida en los años 1800 por Carl Friedrich Gauss, que usa como principio básico la división de números. El algoritmo para la determinación de las clases de congruencia es simple, se toma un número y se divide para el número que se desea realizar la congruencia y el residuo de esta operación es de la definición de módulo, esta clase de razonamiento en conocido principalmente como aritmética de reloj en el cual se hace una serie de número que se reinicia con determinado patrón, por ejemplo los segundos se

reinician en conjuntos de 60 números al igual que los minutos, las horas se reinician en un conjunto de 24h o 12h dependiendo del formato utilizado, esto quiere decir que los segundos y minutos son módulo 60, las horas son módulo 12 o 24 cumpliendo la siguiente notación de Gauss:

$$a \equiv b \ (mod\ n)$$

Que se lee genéricamente como a es congruente con b módulo 10, es decir a = 25 y b= 45 son congruentes módulo 20 ya que al ser divididos ambos números por 20 su residuo es igual (5), donde a = (20*1) +5 y b = (20*2)+5 formando la congruencia módulo 20.

2.5.2. *Algoritmo de Euclides*

El algoritmo de Euclides es el método más eficiente y simple para encontrar el valor del máximo común divisor de dos números (m.c.d), mediante operaciones modulo en los números enteros (Aguilera, 2013, págs. 17, 27), procedimiento:

Siendo a y b dos números enteros, diferente de 0 y no iguales:

1.- Se divide el mayor número para el menor.
2.- Se determina el residuo de la división.
3.- Si la división es exacta el último divisor generado en el m.c.d.
4.- Si la división no es exacta se divide al divisor para el resto de la división hasta obtener una división exacta.

2.5.3. Operaciones aritméticas en $\mathbb{Z}_n$

Las operaciones en $\mathbb{Z}_n$ de la aritmética modular son la suma, resta, multiplicación e inversa modular ya que no existe la división y sus complejidades son similares a las operaciones no modulares, por ejemplo la complejidad de la suma según (Lucena, 2009):

$$(a + b)\ mod\ n : O \log_2 a + O \log_2 b = O(\log_2 n)$$

2.5.4. *Algoritmo extendido de Euclides*

El algoritmo extendido de Euclides es una modificación del algoritmo original que permite expresar el m.c.d en forma de una combinación lineal $\mathrm{mcd(a,b)} = \mathrm{aX} + \mathrm{bY}$ y se obtiene despejando las divisiones obtenidas desde la última hasta la primer, también es muy

usado para determinar el inverso de un número e incluso de la inversa modular (Aguilera, 2013).

2.5.5. *Exponenciación logaritmos discretos*

En los sistemas de criptografía por lo general siempre se requieren de exponenciaciones para encriptar mensajes por lo que realizar esta operación consume muchos recursos a nivel de procesos del computador y llevaría un tiempo indefinido tomando en cuenta que las bases y los exponentes son números sumamente grandes, para ellos se necesita efectivizar procesos surgiendo así le exponenciación modular. La exponenciación modular consiste en fraccionar una potencia a números manejables incluso para una calculadora normal de la siguiente manera:

Suponiendo que se desea calcular $a^b \ mod \ z$ donde a y b son números que no son fácilmente manejables, entonces se divide la exponenciación $b = c + d$ donde c y d son números más fáciles de manejar entonces realizamos la operación $a^b \ mod \ z = a^c \ mod \ z + \ a^d \ mod \ z$ que al aplicar matemática modular obtendríamos un valor R que sería nuestra respuesta $a^b \ mod \ z = R$, sin embargo el cálculo de los logaritmos discretos es muchas más complejo aún y un problema que no se ha demostrado aún, el teorema dice que si se puede calcular un logaritmo entonces se puede factorizar fácilmente pero no se ha podido demostrar el recíproco de este enunciado es por ello que algunos de los criptosistemas se basan en este principio del cálculo de logaritmos Discretos como Diffie-Hellman y ElGamal. (Santamaría, 2013, pág. 13)

2.5.6. *Importancia de los números primos*

La criptografía moderna radica básicamente en explotar este problema de calcular logaritmos discretos supongamos que tenemos un número x y este a su vez es el resultado del producto de dos factores a, b y además estos dos números son primos, entonces sería imposible factorizar n para tener dos factores primos aún más si por ejemplo en el peor de los casos un de los factores fuera $2^{57,885,161} - 1$ que el mayor número primo conocido con hasta 17 millones de dígitos y si fuera posible pues en realidad harían falta recursos computacionales ilimitados a más de tiempo indefinido para realizarlos por ejemplo aquí radica la fuerza de la encriptación RSA.

2.5.7. *Algoritmos de factorización*

Como se ha mencionado la factorización de números primos es inviable pero existen métodos más simples para determinar factores e incluso si el número es primo o no como un test de primalidad o métodos probabilísticos, dentro de los primeros algoritmos se encuentran los siguientes:

División Tentativa en la que se recurría a dividir los números para su posibles factor y determinar si son o no primos, este método por lo general llegaba a una expresión de la forma x = a.b.

Criba de Eratóstenes, consiste en encontrar los factores primos de un número inferior a N, listándolos desde el 2 hasta la N y verificando por número que sea primo e ir tachando los múltiplos de dicho números, así sucesivamente con el 3 hasta el N los números que resten serán los factores primos del número N.

Algoritmo de Fermat, este matemático expresó métodos de factorización puntuales:

- Si un número es expresado como la diferencia de dos cuadrados se puede expresar como: $N = (x + y)(x - y)$
- Si N = a.b con b>a entonces la factorización x e y pueden ser escritas como: $x = \frac{b+a}{2}, x = \frac{b-a}{2}$

La idea general de Fermat radica en factorizar una expresión en x e y tal que $y^2 = x^2 - N$, con la condición de que los factores del número N se encuentren cerca de la raíz cuadrada del número N. Luego de la introducción de las computadoras esos procesos se realizaron de forma más rápida y simple produciendo así la mejora y surgimiento de nuevos algoritmos como la mejora de Kraitchik, Pollard, algoritmo de fracciones continuas, curvas elípticas que se analizarán más adelante.

2.5.8. *Anillos de polinomios*

Se define un anillo de número a un conjunto de números en los cuales se puede realizar las operaciones de suma, resta multiplicación con sus debidas propiedades como la propiedad asociativa, conmutativa. Por lo tanto un anillo de polinomios es un conjunto de polinomios que cumplen con las características mencionadas sobre un conjunto de números y su forma es la siguiente:

$$f(x) = \sum_{i=0}^{n} a_i \, x^i$$

Dado que cumplen con las operaciones de suma, resta, multiplicación y división podemos definir aritmética modular de polinomios con la siguiente notación:

$$g(x) \equiv h(x)\big(mod\ f(x)\big)$$

Si y solo si los residuos o módulos pertenecen al conjunto de números definido.

2.5.9. *Polinomios en* $\mathbb{Z}_n$

En la criptografía los algoritmos representados en los números enteros y más aun de forma binaria tiene suma importancia puesto que permiten generar mecanismos de cifrado muy potentes, de fácil implementación y menos costosos ya sea simplemente haciendo un OR exclusivo entre dos polinomios definidos, al generar un conjunto de valores definidos para un polinomio se considera un cuerpo finito (cuerpo de Galois) y muchas de las estructuras de criptografía como el estándar de cifrado AES dependen principalmente de esta técnica.

2.6. Curvas elípticas en criptografía

La aparición de las curvas elípticas ha dado un cambio significativo a la criptografía puesto que por su constitución matemática las hacen ideales para ser aplicadas en los cifrados pero siendo un arma de doble filo, si es muy simple pudiera ser criptoanalizada, y si es muy compleja su costo de cifrado podría ser elevado tanto en operaciones y cálculos como en tiempo y dinero, las curvas elípticas representan teóricamente mejor cifrado con una longitud de clave mucho menor.
La definición formal de una curva elíptica viene dado por la FORMA NORMAL de WEIERSTRASS, una curva elíptica E definida sobre un cuerpo k (los números enteros) admite un único punto en el infinito de la siguiente manera:

$$E\colon y^2 + a_1xy + \ a_3y \ \equiv \ x^3 + \ a_2x^2 + \ a_4x + \ a_6, a_i \in k$$

2.6.1. *Curvas elípticas en* $\mathbb{R}$

Una curva elíptica en el grupo finito de los números $\mathbb{R}$ no es más que una curva que cumple la siguiente condición: $y^2 = x^3 + ax + b$ Donde a y b caracterizan unívocamente a cada curva, al asumir el grupo de curva elíptica hacemos referencia a la suma y al punto en el infinito. (Delgado & Vallejo, 2009, págs. 3, 36, 45, 54)

2.6.2. *Suma en* $E(\mathbb{R})$

La suma en un grupo finito de puntos viene dada por la suma de los puntos de la curva elíptica, cumpliendo las siguientes propiedades (Delgado & Vallejo, 2009):

- El elemento neutro de la suma de puntos es el punto en el infinito.
- Si la coordenadas en x de dos puntos son opuestos se dice que los puntos son opuesto.
- Si los puntos no son iguales ni opuestos la suma es una recta que corta a la curva elíptica en un punto.
- Cumple la propiedad asociativa (P1 + P2) + P3 = P1 + (P2 + P3).

2.6.3. *Curvas Elípticas en Cuerpo de Galois*

Un cuerpo de Galois es un conjunto de números que tienes representaciones finitas e infinitas, un grupo finito de números está conformado por valor que cumplen una cierta característica, la principal en el grupo de Galois es que estos número se basan en grupos de enteros llamados morfismos y al ser grupos finitos con características uniformes se cumple que se verifican propiedades análogas a los anillos de polinomios. (Delgado & Vallejo, 2009)

Una curva elíptica en GF(n) se define como:

$$y^2 = x^3 + ax + b \ (mód\ n)$$

2.6.4. *Logaritmos Discretos en Curvas Elípticas*

Los logaritmos discretos son la llave de la criptografía hoy en día puesto que los métodos computacionales y operacionales actuales no permiten que se realizase una operación de este tipo de forma eficiente y rápida la computación cuántica es una salida probable pero

no se ha comprobado dicha afirmación, el punto radica en encontrar un número en el caso de RSA a partir de dos números generados por el algoritmo, si el número primo es lo suficientemente grande sería casi improbable factorarlo por métodos convencionales. (Delgado & Vallejo, 2009)

2.7. Cifrados Asimétricos

Debido a que en la utilización de cifrados simétricos se presentan dificultades con el intercambio de claves dentro de una comunicación segura entre el remitente y destinatario, se han desarrollado los algoritmos asimétricos, los cuales responden muy bien ante problema de las claves. Es así que los sistemas de cifrados de clave pública implementan para su funcionamiento dos claves, una pública que puede ser de conocimiento general, y una clave privada que es conocida solamente por una persona, por lo cual debe ser celosamente guardada.

De este modo para llevar a cabo una comunicación segura y secreta, es indispensable tener conocimiento de la clave pública utilizada por el destinatario, para que de esta manera el mensaje al enviarse sea cifrado y pueda ser descifrado posteriormente a través de la clave privada de la cual el destinatario es propietario. Por ello se necesitará un par de claves (pública y privada), por cada usuario que desee establecer una conversación con el destinatario que posee la clave privada.

La única aparente desventaja de este método de cifrado radica en que para encriptar la información se requieren de recursos computacionales mucho mayores que los de clave simétrica, para solucionar un poco este inconveniente de ambos métodos se ha generado el cifrado híbrido. Dentro de los principales algoritmos de claves asimétricas podemos citar los siguientes:

2.7.1. ***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 ves 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.

2.7.2. *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 que este algoritmo se utiliza para el envío de claves por lo general pero luego usa sistemas de clave pública , como por ejemplo el RSA no puede intercambiar claves a mas de 2 personas entonces Diffie – Hellman si podrá distribuir claves a mas persona mediante esté 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.

2.7.3. 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.

2.7.4. *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.

2.8. Análisis de los Algoritmos Criptográficos

En este capítulo se analizarán los algoritmos descritos anteriormente de forma más detallada, determinando la dificultad de cada uno de ellos así como su filosofía, su algoritmo y su fortaleza frente al criptoanálisis.

2.8.1. *Algoritmo RSA*

El algoritmo RSA es el más popular de los algoritmos asimétricos de clave pública, y radica su fuerza en cálculos y factorización de números primos para generar claves públicas y privadas, puesto que encontrar la inversa de la factorización mediante la operación modular de números grandes es imposible en la actualidad y no se han generado algoritmos lo suficientemente eficientes para romper este cifrado, uno de los métodos más simples por así decirlo sería en interceptar la clave privada del usuario de alguna forma, la relación de encriptar y desencriptar es simple cualquier persona puede encriptar un mensaje con conocer la clave del receptor pero sólo él puede conocer el mensaje original enviado, además las claves no pueden ser deducidas unas de otras. (Lucena, 2009).

Datos necesarios

p y q -> números primos generados al azar (aprox. 200 dígitos)
n -> base para la operación módulo
e y d -> números primos que son las claves pública y privada respectivamente.

Algoritmo de obtención de datos

1.- Se generan dos números primos grandes aleatorios.
2.- Se obtiene el valor de n = p * q.
3.- Se calcula la operación phi(n) = (p-1)*(q-1).
4.- Se obtiene e por un proceso aleatorio, dado que: $1 \leq e \leq phi(n)$.
5.- Se obtiene d dado que: e * d = 1 mod n.

Algoritmo de cifrado

Se eleva el dato a la clave e y se obtiene su operación módulo n.

Algoritmo de descifrado

El dato cifrado es elevado a la clave privada y se obtiene su operación módulo n.

2.8.2. *Algoritmo Diffie-Hellman*

El algoritmo Diffie-Hellman es un método que permite el intercambio de claves entre emisor y receptor cuando se desea encriptar información teniendo en consideración que los usuarios no han establecido contactos previos, se comunican por una red sin protección, no confiable y se realiza la comunicación de manera pública es decir no se podría definir si el usuario que emite el mensaje es el real. (Lucena, 2009)

Datos necesarios

g y p -> son dos números primos grandes base y modulo respectivamente (mínimo 300 dígitos).

a y b -> números secretos de emisor y receptor.

Algoritmo de obtención de datos

1.- El emisor envía los datos g y p.

2.- Emisor y receptor generan un número secreto a y b respectivamente.

3.- El emisor realiza la siguiente operación y envía su resultado.

3.1.- $x = g^a \ mod \ p$

3.2.- envía el valor de x.

4.- El receptor realiza la misma operación.

4.1.- $y = g^b \ mod \ p$

4.2.- envía el valor de y.

5.- Emisor y receptor cambian a las bases Y y X respectivamente y obtienen la clave genérica de la siguiente forma.

5.1.- emisor realiza la operación $C = y^a \ mod \ p$

5.2.- receptor realiza la operación $C = x^b \ mod \ p$

Algoritmo de cifrado

1. Ésta clave C obtenida sirve de llave privada para cifrar información con métodos de cifrado.

Algoritmo de descifrado

1.- consiste en ejecutar las siguientes operaciones para obtener los números secretos:

$$a = \log d_g(x) \ \ y \ \ b = \log d_g(y)$$

Tomándose en cuenta que log d es la operación logaritmo discreto.

2.8.3. *Algoritmo El Gamal*

El Gamal es un algoritmo que se usaba principalmente para generar firmas digitales aunque hoy en día se pueden generar mensajes cifrados, este procedimiento se lo realiza en un grupo finito y se basa en los principios de Diffie-Hellman y el concepto de los logaritmos discretos, existen dos tipos de algoritmos El Gamal el clásico y el elíptico que usa las curvas elípticas sobre grupos discretos, se analizará El Gamal clásico para establecer parámetros similares de comparación con los demás algoritmo, estas dos formas se diferencian en la obtención y uso del grupo finito. (Departamento de Sistemas Informáticos y Computación, págs. 13, 18).

Datos necesarios

Definir un grupo finito sobre p (primo fuerte) ->$\mathbb{Z}_p^*$.

Definir un g generador del cuerpo finito.

x, y claves aleatorias privadas de cada usuario -> 1 < x , y <p.

Algoritmo de Obtención de Datos

Las claves públicas se generan a partir de las siguientes ecuaciones $X = g^x \ mod \ p$ y $Y = g^y \ mod \ p$ -> (X, g, p) y (Y, g, p).

Algoritmo de cifrado

1.- El mensaje se divide en bloques de bits.

2.- cada bloque se representa con un número z, 1 < z < p-1.

3.- el usuario receptor envía su clave pública (Y, g, p).

4.- el usuario emisor genera un número aleatorio k, 1 < k < p-1 y lo envía al receptor.

5.- el emisor emite el mensaje codificado: $C = [g^k \ mod \ p, \ M * \ Y^k \ mod \ p \ ]$

Algoritmo de descifrado

1.- El receptor recibe el mensaje codificado.

2.- El receptor toma el primer elemento del par ordenado ($g^k \ mod \ p$) y genera $g^{-ky} \ mod \ p$

3.- Este factor se multiplica por el segundo elemento del par ordenado y se descifra el Criptosistema.

2.8.4. *Algoritmo El Rabin*

El algoritmo de cifrado de Rabin se basa en la característica principal de obtener las raíces cuadradas de un número compuesto, y su fortaleza es similar a la de los

logaritmos anteriores, factorizar dicho número para encontrar las claves respectivas. (Departamento de Sistemas Informáticos y Computación).

Datos necesarios

p y q -> claves privadas

N -> clave pública.

Algoritmo de obtención de datos

1.- p y q deben ser primos congruentes en 3 mod 4 y a su vez sus 2 últimos bits deben ser 1

2.- la clave pública se genera al multiplicar estos dos valores N = p * q.

Algoritmo de cifrado

1.- Se toma el mensaje C

2.- Se calcula $Z = C^2 \ mod \ n$

Algoritmo de descifrado

Para descifrar el Criptosistema de Rabin se necesita tener conocimiento sobre la teoría de números, el teorema chino del resto y el algoritmo extendido de Euclides.

El teorema chino del resto enuncia que sean p y q números N tales que mcd(n,m) = 1, en conclusión son números primos relativos en donde dados b_1 y b_2 en Z existe un X tal que: $X \equiv \ b_1(mod\ n)$ y $X \equiv \ b_2(mod\ m)$. A más de estas congruencias pudieren existir un v y w en Z que satisfagan las congruencias de la misma forma entonces: $v \equiv$ w $(mod\ n * m)$.

1.- Utilizando los principios del TCR (Teoría Chino del Resto) se buscan dos números a, b que satisfagan ap + bp = 1.

2.- Se calculan las siguientes ecuaciones:

2.1.- $r = \ c^{(p+1)/4} mod\ p$

2.2.- $s = \ c^{(q+1)/4} mod\ q$

2.3.- $m_1 = (aps + brq) mod\ n$

2.4.- $m_2 = (aps - brq) mod\ n$

Las raíces obtenidas son las siguientes: $m_1, m_2, -m_1\ mod\ n, -m_2\ mod\ n$

Lamentablemente aún después de descifrar correctamente el mensaje no se puede saber en sí si la clave o el mensaje obtenido son los verídicos por lo que es de vital importancia

colocar un mecanismo en el mensaje cifrado que permita saber cuáles son los datos correctos.

2.9. Estado del arte

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: clarificar el papel que el lenguaje numérico debería tener en su formación. Para tal objetivo, se tienen en cuenta el aspecto curricular y cognitivo, de cuyo análisis se derivan conocimientos necesarios para la toma de decisiones sobre el problema planteado. La criptografía ha demostrado ser una de las aplicaciones más importantes y prácticas de la matemática actual, sin ella por ejemplo no sería posible la existencia del denominado dinero plástico, del cual dependemos en la actualidad; de ahí que se plantee la necesidad de su enseñanza en cursos de educación media. El marco teórico desde el que se plantea el problema atribuye un papel esencial a los aspectos fundacionales, esto es, la fortaleza en los conocimientos matemáticos necesarios para aprender criptografía. Por tal motivo se estudia, en primer lugar, el papel de la teoría de números, analizando algunos aspectos de su origen, con el fin de poder abordar algunos problemas y ciertos algoritmos de la criptografía, que se sustentan en el lenguaje de la teoría de números como elemento central y mostrando una aplicación de este, que es el criptosistema.” (Ibáñez, 2012, pág. 9).

El estudio realizado para la enseñanza de la criptografía en la educación media sobre conceptos criptográficos aborda temas de interés como la teoría de números y aritmética modular, como base fundamental para la enseñanza de los algoritmos de criptografía, brevemente se explican el funcionamiento de varios criptosistemas pero no se realiza un análisis profundo de que conceptos deberían recibir los estudiantes y cuál es el algoritmo de cifrado óptimo para su enseñanza puesto que se ha escogido técnicas como el cifrado de Polybio y Vigenere, no se ha realizado un estudio sobre la complejidad de los algoritmos, se recomendaría verificar el nivel de aprendizaje de los estudiantes y verificar

el uso de herramientas de software como CRYPTOOL que para ser utilizado los estudiantes también deberían poseer conocimientos informáticos básicos.

Otro estudio comparativo es “Análisis de Algoritmos Criptográficos y su aplicación al Cifrado de Archivos” (Blanco, 2010, pág. 4) realizado por Roberto Blanco analiza el funcionamiento de los algoritmos RSA, DES, AES mediante el análisis de sus vulnerabilidades, complejidad y tiempo de procesamiento en donde se ha determinado que el algoritmo óptimo es AES porque permite mantener su estabilidad de nivel de cifrado pese a las modificaciones que se puedan realizar, sin embargo es estudio comparativo no posee fines educativos es decir no permite la enseñanza de la criptografía y no se optimizan los conceptos para el análisis matemático con lo que no se podrá profundizar en el uso de conceptos matemáticos como anillos de polinomios, curvas elípticas, aritmética modular.

Un análisis matemático más profundo es el propuesto en el trabajo “Propuesta y Análisis de Criptosistemas de Clave Pública Basados en Matrices Triangulares Superiores Por Bloques” (Vicent, pág. 125) de José Vicent en donde se explican y analizan conceptos criptográficos como criptosistemas, criptoanálisis cantidad de información y matemáticamente aritmética modular, grupos finitos, complejidad computacional, problemas del logaritmo discreto sobre Algoritmos como RSA, Diffie-Hellman El Gamal, el Sistema Massey-Omura.

Como resultado principal se obtiene que los algoritmos clásicos de criptografía ya no son confiables por lo que se emite una propuesta de emplear las matrices triangulares superiores por bloques para incrementar la confiabilidad de los criptosistemas por lo que al usar matrices triangulares de orden r=2, s=89 y p=2903 se obtienen tiempos de ejecución comparables con RSA.

Incluyendo el trabajo de investigación sobre las matrices superiores se puede determinar que su objetivo es mejorar el nivel de los criptosistemas tradicionales mediante una propuesta de cifrado por bloques más esta tendencia no es aplicable al estudio actual puesto que se busca generar un análisis criptográfico direccionado al ámbito educativo y como los conceptos matemáticos influyen en el proceso enseñanza aprendizaje.
“Análisis De Algoritmos De Cifrado De Llave Secreta Y Su Uso Dentro De Una Organización Pública” es un trabajo propuesto por el Ing. Alberto Morales en donde se analizan 5 algoritmos criptográficos distintos con el objetivo de mantener los sistemas de información cifrados estas pruebas se realizaron sobre ambientes como funcionamiento,

fortalezas y obviamente las debilidades que cada uno de ellos poseen, como resultado se recomienda el uso de Camellia. (Morales, 2009, pág. 7).

El estudio representa la comparación de algoritmos de cifrado para el envío y recepción de datos en la organización, con el uso de Camellia los sistemas de cifrado se elevan a estándares internacionales, pero no es un estudio referencial para este trabajo puesto que no se analizan conceptos matemáticos sobre los métodos de cifrado, no se realiza un estudio del funcionamiento de cada criptosistema y finalmente no produce un hito importante para permitir la enseñanza de la asignatura de criptografía sobre educandos.
Se ha realizado una investigación exhaustiva sobre estudios comparativos de algoritmos criptográficos, criptosistemas, criptoanálisis y no se han encontrado resultados relacionados con el tema de investigación tanto es el caso que no existen propuestas comparativas sobre la enseñanza de la criptografía hacia los educandos, a más de ellos se ha investigado sobre la influencia de los conceptos matemáticos en estudio como son Aritmética modular, anillos de polinomios, teoría de números sin resultados aparentes, estos conceptos han sido extraídos del funcionamiento genérico de RSA, Diffie-Hellman y El Gamal.

Estudios comparativos sobre estos algoritmos de cifrado existen pero no poseen fines educativos sino de rendimiento, de valoraciones de confianza en el criptosistema e incluso son visualizados como algoritmos de firmas digitales propósito que el estudio no abarca, en el aspecto matemático se encuentran propuestas de mejoras a los algoritmos, mejoras en rendimiento a través de algoritmos matemáticos, modelos, teorías de números y mejorando la complejidad de la factorización de números primos (problema del logaritmo discreto).

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.

CAPÍTULO III:

DISEÑO DE LA INVESTIGACIÓN

En este capítulo 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 cursando la asignatura de criptografía (séptimo semestre) .

3.1. 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

3.2. 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.

3.3. Métodos

Una vez definida la población y seleccionada la muestra, para el proyecto se utiliza el método científico dado que se ha planteado el modelo de investigación de la siguiente manera:

- La investigación se produce por la necesidad de disminuir los problemas de asimilación de contenidos existente en la cátedra de Criptografía en la Escuela de Ingeniería en Sistemas de la ESPOCH.
- Se han definido los objetivos de la investigación con la finalidad de mejorar la comprensión de la asignatura de criptografía en los estudiantes.
- En el marco teórico se muestran las razones por las cuales es importante el que se realice la presente investigación.
- La hipótesis ha sido planteada como una posible solución al problema planteado.
- Una vez planteada la hipótesis se realiza la operacionalización de las variables.
- Se definen los algoritmos a ser analizados y se determina la población a la cual será aplicada el estudio.
- Se realiza la recolección de datos, indicadores e índices mediante encuestas y observación directa.
- Se realiza la comprobación de la hipótesis planteada.
- Se emiten conclusiones y recomendaciones.

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.

3.4. Técnicas de recopilación de información

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 , estas encuestas se pueden procesar inmediatamente e interpretar sus datos para el estudio de una forma más eficaz.

3.5. Escenarios

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:

1. Breve introducción al algoritmo de cifrado.
2. Tipos de conceptos matemáticos a emplearse en el algoritmo.
3. Problema práctico.
4. Descripción de los datos de entrada del algoritmo de cifrado.
5. Ejecución del algoritmo de cifrado.
6. Ejecución del algoritmo de descifrado.

Los puntos expuestos en esta sección han sido ya previamente analizados en el capítulo anterior por lo que este distributivo tuvo como fundamentación teórica los análisis de los diferente 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.

3.6. Operacionalización de las variables

Para definir los resultados de las cátedras y el análisis de los algoritmos se definieron los tipos de variables, además se realizó la operacionalización conceptual y metodológica de

las variables con la finalidad de estandarizar el estudio investigativo para lo cual se detalla de la siguiente forma:

3.6.1. *Hipótesis de la investigación*

En la investigación se ha definido en el primer capítulo la siguiente hipótesis y se genera su hipótesis:
H_1: "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".

H_0: "El algoritmo RSA **NO** 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".

3.6.2. *Tipo de variables*

Analizando la hipótesis se han determinado las siguientes variables para el estudio:

Variable independiente: Algoritmos de criptografía pública.
Variable dependiente: Aprendizaje de los alumnos.

Con lo que podemos darnos cuenta que el aprendizaje de los estudiantes depende únicamente de los algoritmos de criptografía pública que fueron impartidos en los escenarios con lo cual damos cumplimiento al modelo de diseño cuasi experimental.

3.6.3. *Operacionalización de las variables*

Al realizar la operación conceptual de las variables de la hipótesis se está definiendo el criterio con el cual serán empleadas y el mismo que permitirá a un investigador reproducir su análisis, dentro de la operacionalización de las variables se encuentran dos procedimiento que son la operacionalización conceptual y la operacionalización metodológica, la primera nos permite definir de forma precisa que se entiende por el tipo de variable para evitar que existan confusiones o que se puedan mal interpretar las mediciones cada una de ellas en sí define su papel en la hipótesis, al realizar la segunda operacionalización determinamos la forma en las que estas serán medidas sus indicadores e índices, los indicadores son cifras que son obtenidas al haber realizado una

medición y permiten mantener un ámbito de control además los índices permiten realizar valoración cualitativas de un estado situacional a los indicadores.

3.6.4. *Operacionalización conceptual*

Al cumplir con los criterios de la operacionalización de variables y teniendo las variables dependientes e independientes se realizó la siguiente generalización de conceptos para definir que es un algoritmo criptográfico y que es el aprendizaje de los estudiantes.

Tabla 1-3: Operacionalización conceptual de las variables

VARIABLE	TIPO	CONCEPTO
Los algoritmos de criptografía pública	Independiente	Algoritmos matemáticos que permiten el cifrado de la información que se transmite por un medio inseguro, los mismos que constan de datos de entrada, algoritmos de cifrado, algoritmo de des-cifrado y conceptos matemáticos para su comprensión.
El aprendizaje de los estudiantes	Dependiente	El nivel de conocimientos de criptografía asimilados por los estudiantes de la carrera al haberse dictado las cátedras.

Fuente: Paguay Mario.2015

Con la operacionalización de variables de la tabla III-1 se define un algoritmo criptográfico como un conjunto de datos de entrada, algoritmo de cifrado, algoritmo de descifrado y conceptualización matemática con lo que se puede definir la operacionalización metodológica.

3.6.5. Operacionalización metodológica variable independiente

Al realizar la operación metodológica de las variables se estarán estableciendo los indicadores e índices que nos permitirán evaluar la variable y obtener resultados a partir de las mediciones, este proceso se realiza mediante descripciones de tablas en donde se ingresan la hipótesis, la variable y su tipo, los indicadores, índices, técnicas e instrumentos de medición de la siguiente manera:

Tabla 2-3: Operacionalización Metodológica Variable Independiente

HIPÓTESIS	VARIABLE INDEPENDIENTE	INDICADORES	ÍNDICES	TÉCNICAS	INSTRUMENTO
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.	Algoritmos de criptografía pública.	1. Datos de Entrada.	1. Número de los datos de entrada. 2. Dificultad para la preparación de los datos.	Comparación Directa	Revisión de Literatura Fuentes Bibliográficas
		2. Algoritmo de Cifrado.	3. Número de pasos. 4. Dificultad de los pasos. 5. Orden de complejidad.		
		3. Algoritmo de Descifrado.	6. Número de pasos. 7. Dificultad de los pasos. 8. Orden de complejidad.		
		4. Conceptos Matemáticos.	9. Cantidad de definiciones matemáticas empleadas. 10. Importancia de los conceptos matemáticos.		

Realizado por: Paguay Mario .2015

La variable se ha dividido en los siguientes indicadores como lo muestra la Tabla III-2:

Datos de entrada.- Son aquellos parámetros definidos en el capítulo 2 de cada algoritmo criptográfico que permiten que se realicen los algoritmos de cifrado y de descifrado son por ejemplo las claves públicas y privadas de los usuarios y el mensaje cifrado transmitido.

Número de Datos de Entrada.- El índice hace referencia al número de datos completo que requiere el algoritmo para su funcionamiento es decir el total de número de claves más el mensaje cifrado.

Dificultad para la preparación de los datos.- El índice controla la cantidad de procesos matemáticos (cálculos y conceptos matemáticos que los generan) que se deben aplicar a un dato de entrada para que éste sea considerado como útil para el algoritmo de cifrado o descifrado.

Algoritmo de cifrado.- Es el método por el cual el algoritmo criptográfico cifra la información antes de ser enviada al receptor, este algoritmo hace uso de los datos de entrada ya sea en su totalidad o parcialidad es decir el algoritmo de cifrado no necesita la clave privada del receptor en criptosistemas de clave pública, analógicamente el mismo procedimiento se produce en el algoritmo de des cifrado.

Número de pasos.- El índice determina la cantidad de procedimientos que debe realizar el algoritmo para cifrar la información en claro desde el ingreso de la información hasta la salida del texto cifrado.

Dificultad de los pasos.- El índice determinar la dificultad de un paso de ejecución del algoritmo de cifrado en contraste a los conceptos matemáticos que se emplean para dicho procedimiento.

Orden de complejidad.- El grado de complejidad del algoritmo viene dado por la cantidad de estructuras de decisión, bucles de repetición y condicionales que poseyera el algoritmo.

Conceptos matemáticos.- Se busca relacionar todos los conceptos matemáticos que usa el algoritmo criptográfico para tener una idea de la importancia de los fundamentos matemáticos para comprender la criptografía.

Cantidad de definiciones matemáticas empleadas.- es la suma de las definiciones que se obtengan de los datos de entrada, algoritmos de cifra y des cifrado.

Importancia de los conceptos matemáticos.- define si es crítico el conocimiento de los mismos en base a la operación del algoritmo en la que se requiera o ejecute.

3.6.6. Operacionalización metodológica variable dependiente

Esta operacionalización se pretende definir las preguntas de las encuestas a ser aplicadas a los estudiantes puesto que se busca el mejor algoritmo para la comprensión de la criptografía y medir que nivel de conocimientos poseen los estudiantes sobre los fundamentos matemáticos.

Tabla 0-1 Operacionalización Metodológica de la Variable Dependiente

HIPÓTESIS	VARIABLE DEPENDIENTE	INDICADORES	ÍNDICES	TÉCNICA	INSTRUMENTO
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.	Aprendizaje de los estudiantes.	1. Nivel de comprensión.	1. Entendimiento del algoritmo matemático. 2. Comprensión y dominio en la obtención de los datos de entrada. 3. Conceptualización del algoritmo de cifrado. 4. Conceptualización del algoritmo de descifrado.	Encuesta	Cuestionario
		2. Nivel de aplicación de conocimientos.	5. El estudiante es capaz de implementar al menos un algoritmo criptográfico. 6. El estudiante es capaz de crear un algoritmo criptográfico personalizado. 7. El estudiante puede descifrar un texto encriptado.		
		3. Conceptos Matemáticos.	8. Conocimiento sobre aritmética modular. 9. Conocimiento sobre estructuras algebraicas. 10. Conocimiento sobre logaritmos. 11. Conocimiento sobre la obtención de raíces cuadradas. 12. Conocimiento sobre el Teorema chino del resto. 13. Conocimiento sobre el algoritmo Extendido de Euclides. 14. Conocimiento sobre Curvas Elípticas. 15. Conocimiento sobre Grupos Finitos		

Fuente: Paguay.2015

3.7. Procesamiento de la información

Para el procesamiento de la información se ha considerado los modelos de ejecución de los algoritmos por lo cual han sido divididos en 4 fases que han sido estandarizadas por el tesista en el marco teórico usando principalmente las referencias de (Lucena, 2009) y (Departamento de Sistemas Informáticos y Computación) con lo que al aplicar los algoritmos se puede cifrar un dato desde el proceso de obtención de los datos necesarios, por lo cual se realizará un estudio comparativo entre los algoritmos de criptografía para así determinar por metodología cuál es el mejor algoritmo.

Este estudio hace uso de los indicadores e índices de la operacionalización de las variables a los mismos que se les somete a un proceso de valoración es decir que cada uno de ellos debe tener un valor y este debe ser obtenido mediante una escala, en este caso emplearemos la escala de Likert que es una escala que nos permite medir actitudes de los sujetos que se han sometido a la encuesta, la escala Likert tiene un umbral de valoración de 5 puntos los cuales generalmente se manejan en: Totalmente de Acuerdo, de Acuerdo, Indiferente, en Desacuerdo, Totalmente en desacuerdo con esto podremos medir los indicadores con un alto nivel de precisión además estos 5 parámetros serán modificados con valores de acuerdo a la necesidad de la investigación y el modelo de encuesta además Likert nos permite hacer preguntas cerradas lo que se ha diseñado para las encuestas del trabajo investigativo. (Malave, 2007, pág. 3).

CAPÍTULO IV:

RESULTADOS Y DISCUSIÓN

Para el desarrollo del IV Capítulo Resultados y Discusión de la investigación se toman los indicadores e índices de las Tabla III-2 y Tabla III-3 que 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.

4.1. Variable independiente

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

4.1.1. *Indicador 1 – Datos de entrada*

Los algoritmos criptográficos por lo general necesitan de ciertos datos para su funcionamiento, estos datos pueden ser utilizados en el proceso de cifrar un texto y para ser cifrado se necesita de la clave pública del usuario destinatario más la clave privada del usuario emisor y el texto a cifrar, ejecutado el algoritmo ya obtendremos un texto que solo 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 mediante la Tabla IV-1:

Tabla 1-4 Índice 1 - Número de Datos de Entrada

Algoritmo	**Número de Datos de Entrada**	**Valoración (%)**
RSA	5	100
Diffie-Hellman	4	80
El Rabin	4	80
El Gamal	3	60

Fuente: Paguay Mario. 2015

Se ha considerado para el estudio que manejar un número de datos de entrada más alto permite a los estudiantes tener un mejor entendimiento del algoritmo debido a que no necesitan realizar cálculos adicionales para determinar más variables al momento de encriptar la información al contrario se toman los datos ya generados, en 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 80% respectivamente, manejando la escala Likert se establecen los siguientes valores:

Tabla 0-4 Índice 1 Escala Likert

Algoritmo	Valoración (%)	Escala Likert
RSA	100	5
Diffie-Hellman	80	4
El Rabin	80	4
El Gamal	60	3

Fuente: Paguay Mario.2015

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, valores reflejados en la Tabla IV-2 y resumidos en el siguiente gráfico:

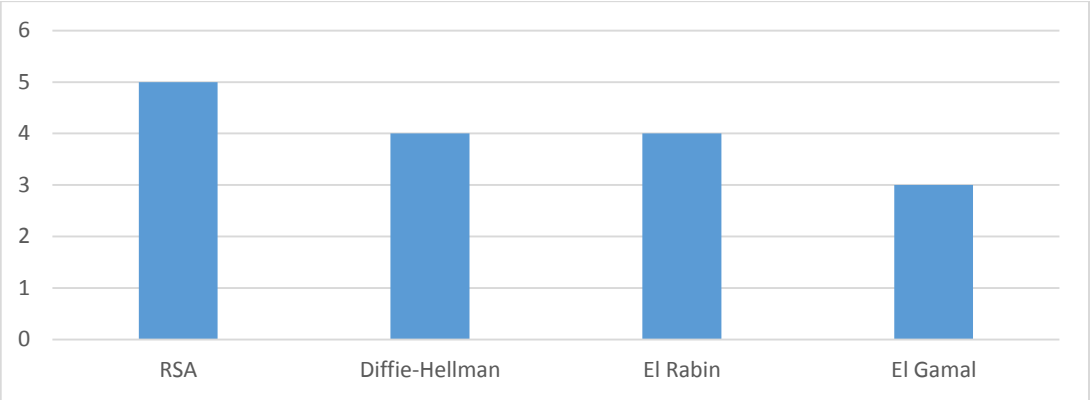


Gráfico 1-1 Gráfico Resumen Índice 1
Fuente: Paguay Mario.2015

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, estos conceptos y definiciones son considerados de los algoritmos de obtención de los datos de entrada por lo que se dará una valoración por la dificultad de operaciones matemáticas considerando como las más sencillas a las operaciones aritméticas básicas.

Tabla 0-4 Índice 2 Dificultad para la Obtención de los Datos de Entrada

Algoritmo	Dificultad para la preparación de Datos de Entrada	Valoración Cualitativa	Escala de Likert
RSA	Operación multiplicación Operación módulo	Baja	5
Diffie-Hellman	Operación potencia Operación módulo	Baja	5
El Rabin	Determinar la congruencia de números primos	Media	3
El Gamal	Comprensión de grupos finitos	Alta	1

Fuente: Paguay Mario. 2015

En base a la escala empleada en la Tabla IV-3 se da un valor alto a los procesos que poseen una dificultad baja por lo que los puntos de referencia serían uno a las operaciones matemáticas de baja dificultad, tres a las operaciones de mediana dificultad y cinco a las operaciones que implican una alta dificultad y se resume en el siguiente gráfico:

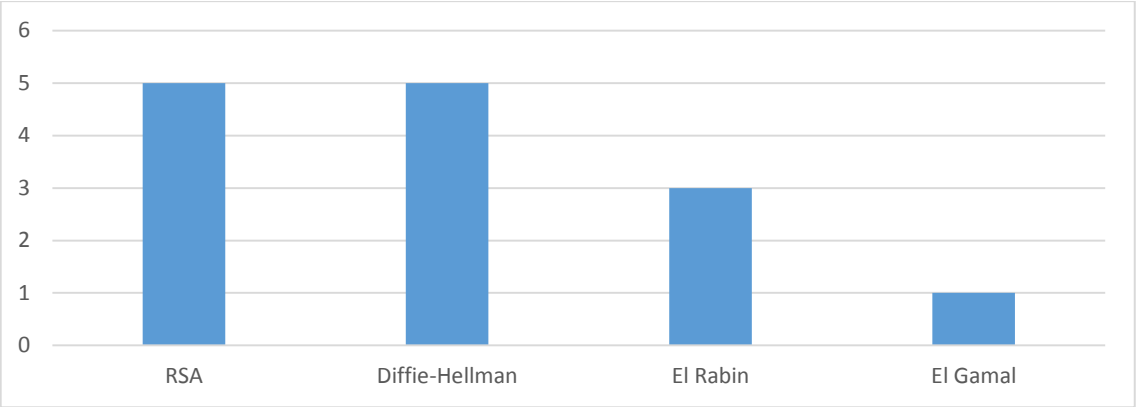


Gráfico 2-2 Gráfico Resumen Índice 2
Fuente: Paguay Mario. 2015

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.

4.1.2. *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 la siguiente manera:

Tabla 0-1 Número de pasos del algoritmo de cifrado

Algoritmo	Número de Pasos	Valoración (%)
RSA	1	20
Diffie-Hellman	0	0
El Rabin	2	40
El Gamal	5	100

Fuente: Paguay Mario. 2015

En la Tabla IV-4 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 porque se debe mantener

secuencia de resultados, realizar mayor número de transformaciones a los datos y es más probable que el estudiante no obtenga el resultado deseado creando una analogía a la escala del proyecto se definirían los siguientes valores:

Tabla 0-4 Indice 3 Escala Likert

Algoritmo	Valoración (%)	Escala Likert
RSA	20	5
Diffie-Hellman	0	0
El Rabin	40	2
El Gamal	100	1

Fuente: Paguay Mario. 2015

La valoración de cada punto corresponde al 20% del total de pasos como muestra la Tabla IV-5, para realizar el algoritmo de cifrado de los mismos que se ha dado la valoración de 5 puntos al algoritmo RSA porque posee un solo 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 siguiente gráfico:

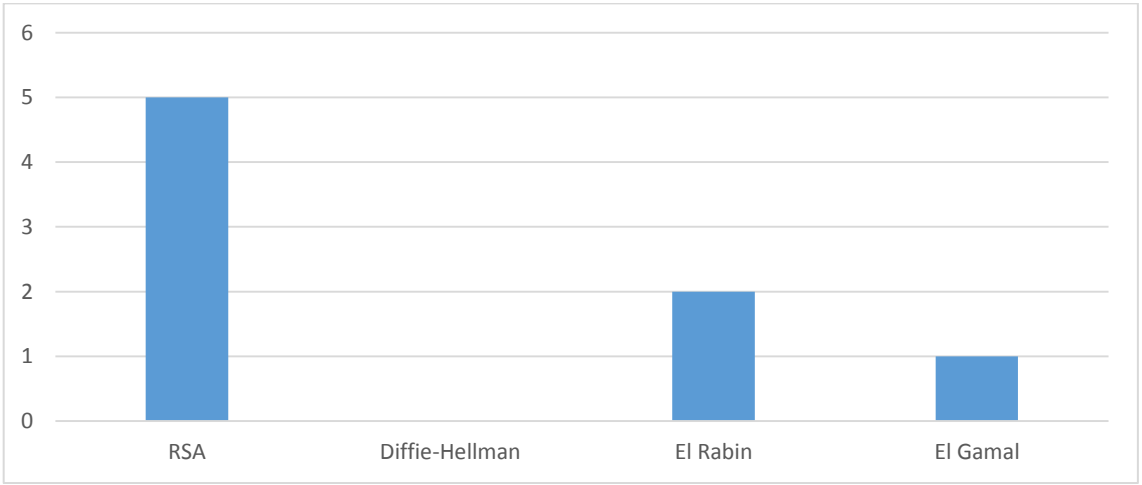


Gráfico 3-3 Gráfico Resumen Índice 3
Fuente: Paguay Mario. 2015

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 detallarán las operaciones necesarias y se realizará un comparativo, en este análisis

también se lo excluye al algoritmo Diffie-Hellman puesto que no se puede realizar una continuidad de análisis con el índice anterior.

Tabla 0-4 Dificultad de los Pasos del Algoritmo de Cifrado

Algoritmo	**Dificultad de los Pasos del Algoritmo de Cifrado**	**Valoración Cualitativa**	**Valoración Cuantitativa**
RSA	Operación Potenciación Operación Módulo	Baja	5
Diffie-Hellman	N/A	N/A	0
El Rabin	Operación Potenciación Operación Módulo	Baja	5
El Gamal	Dividir el dato a cifrar en bloques de bits Representación numérica de los bloques Generación de números aleatorios Operación Multiplicación Operación Módulo	Alta	1

Fuente: Paguay Mario. 2015

La escala Likert en la Tabla IV-6 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 el gráfico resumen es el siguiente:

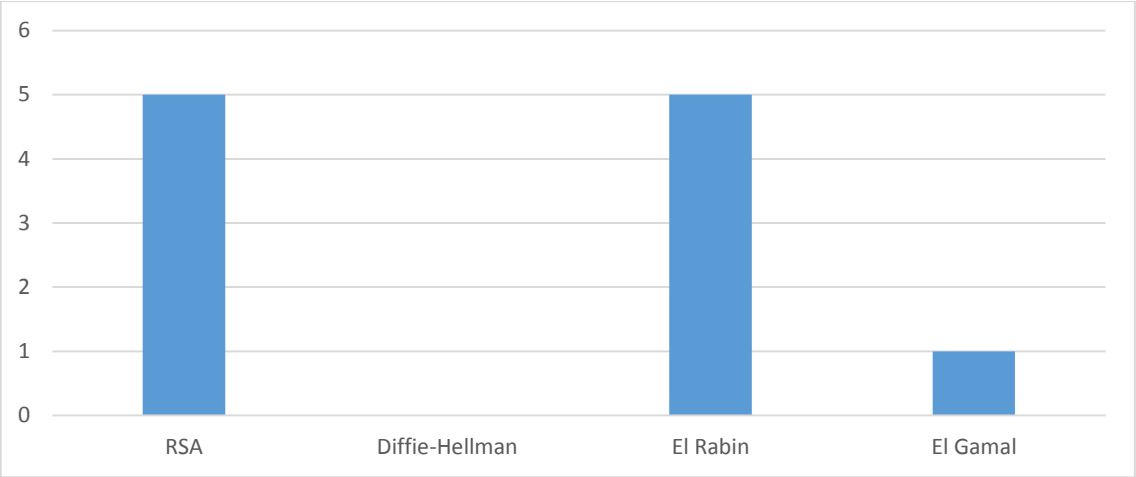


Gráfico 0-4 Gráfico Resumen Índice 4
Fuente: Paguay Mario. 2015

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), analizando los pasos del algoritmo obtenemos los siguientes:

Tabla 0-4 Orden de Complejidad del Algoritmo

Algoritmo	Orden de Complejidad	Valoración
RSA	Bajo (nulo)	5
Diffie-Hellman	N/A	0
El Rabin	Medio	3
El Gamal	Bajo (nulo)	5

Fuente: Paguay Mario. 2015

Los valores obtenidos en la Tabla IV-7 se han tomado de los algoritmos de cifrado en donde se determinó que los algoritmos RSA y el Rabin no poseen estructuras de decisión ni estructuras de repetición por lo que se le asigna una valoración de bajo, el algoritmo el ramal posee 2 estructuras condicionales por lo que se le asigna una complejidad de medio en relación a los anteriores, 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 la siguiente figura:

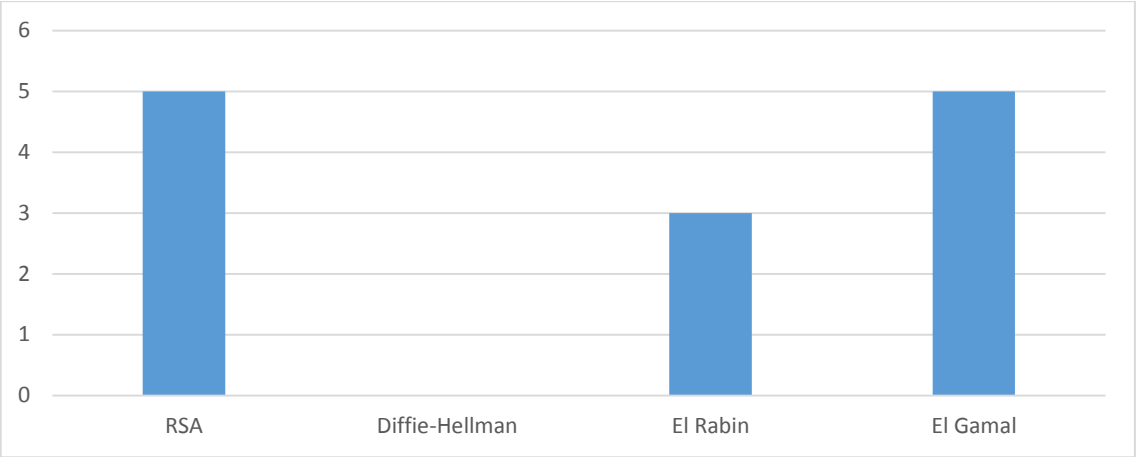


Gráfico 5-5 Gráfico Resumen Índice 5
Fuente: Paguay Mario.2015

4.1.3. *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 volverle 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 puesto que de no ser así o emplear otra técnica el algoritmo no devolvería el resultado esperado, para realizar la comparación se han determinado los siguientes pasos en los algoritmos de des cifrado:

Tabla 0-4 Número de Pasos del Algoritmo de Descifrado

Algoritmo	Número de Pasos	Valoración (%)
RSA	1	100
Diffie-Hellman	2	66,67
El Rabin	2	66,67
El Gamal	3	33,33

Fuente: Paguay Mario. 2015

En la tabla IV-8 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 de la siguiente manera:

Tabla 0-4 Índice 6 Escala Likert

Algoritmo	Valoración	Escala Likert
RSA	100	5
Diffie-Hellman	66,67	3
El Rabin	66,67	3
El Gamal	33,33	1

Fuente: Paguay.2015

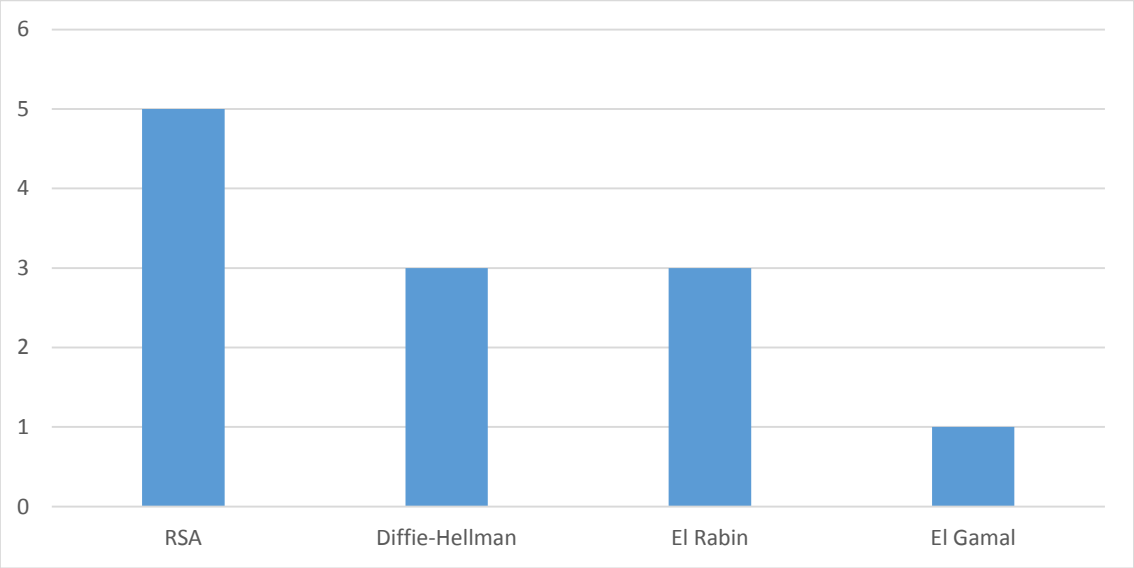


Gráfico 6-6 Gráfico Resumen Índice 6
Fuente: Paguay Mario. 2015

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, estos métodos de descifrado poseen un dato importante y es que en los algoritmos de criptografía siempre conoceremos nuestra llave privada gracias a este dato se pueden des cifrar de manera inmediata un texto codificado que mientras no tengamos este valor tendríamos que generar números al azar para determinarlo con lo que llevaría por la construcción del algoritmo años en encontrar estos valores o incluso segundos por lo cual es necesario definir el nivel de dificultad de los pasos de los algoritmos.

Tabla 0-2 Dificultad de los Pasos del Algoritmo de Descifrado

Algoritmo	Dificultad de los Pasos del Algoritmo de Des Cifrado	Valoración Cualitativa	Valoración Cuantitativa
RSA	Operación Potenciación Operación Módulo	Baja	5
Diffie-Hellman	Operaciones con Logaritmos	Media	3
El Rabin	Operación Módulo Conocimiento del Teorema Chino del Resto	Alta	1
El Gamal	Operación Potenciación Operación Módulo (Inversa)	Baja	5

Fuente: Paguay Mario. 2015

Las operaciones matemáticas en la Tabla IV-10 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 de la siguiente manera:

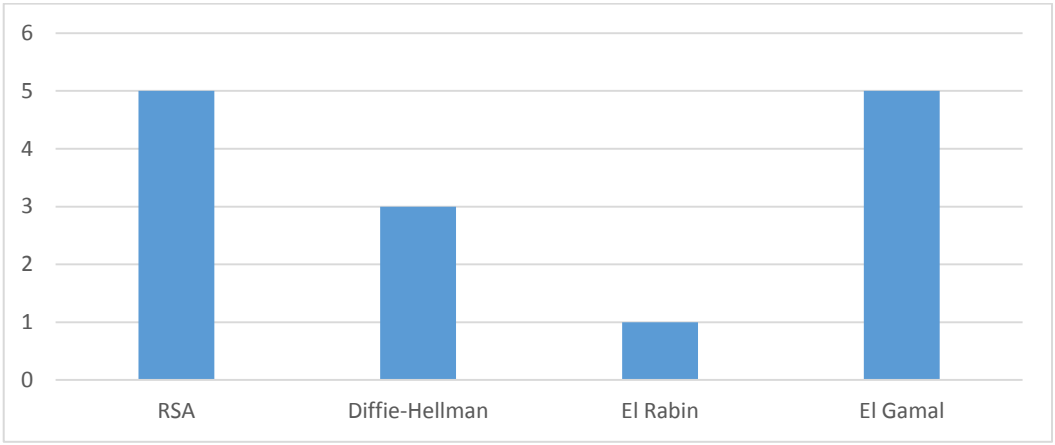


Gráfico 7-7 Gráfico Resumen Índice 7
Fuente: Paguay Mario. 2015

Índice 8 – Orden de complejidad

El orden de complejidad del algoritmo se define por la cantidad de estructuras de decisión y bucles de repetición, analizando los pasos del algoritmo de descifrado obtenemos los siguientes:

Tabla 0-3 Orden de Complejidad del Algoritmo

Algoritmo	Orden de Complejidad	Valoración
RSA	Bajo (nulo)	5
Diffie-Hellman	Bajo (nulo)	5
El Rabin	Alto	1
El Gamal	Bajo (nulo)	5

Fuente: Paguay Mario. 2015

Los valores obtenidos en la Tabla IV-11 se han tomado de los algoritmos de cifrado en donde 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 asignado 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.

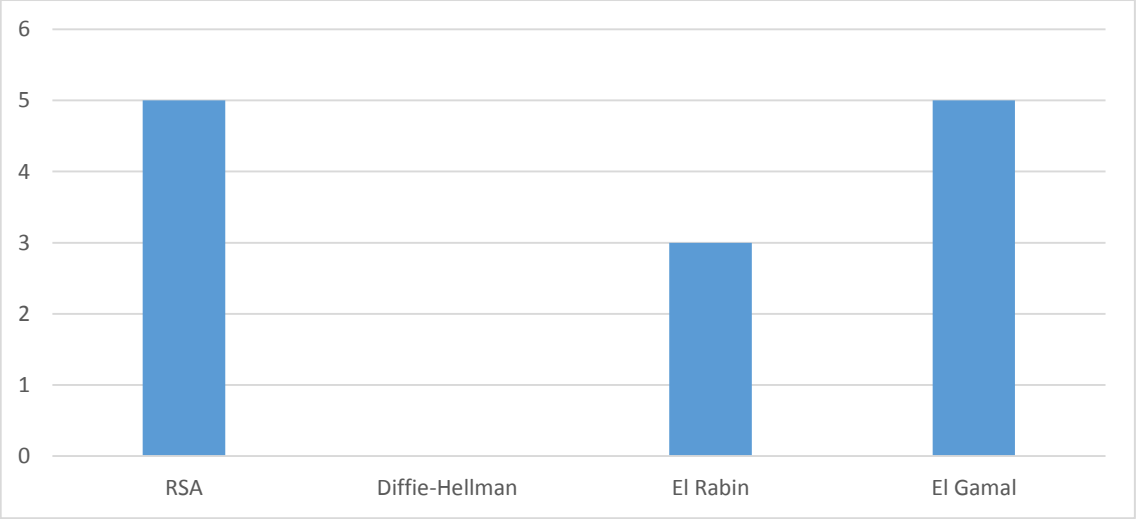


Gráfico 8-8 Gráfico Resumen Índice 7

Fuente: Paguay Mario. 2015

4.1.4. *Indicador 4 – Concepto Matemáticos*

El indicador conceptos matemáticos genera evidencia de la matemática que se emplea en cada algoritmo es decir las definiciones que sirven para cifrar y descifrar 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.

.

Índice 9 – Cantidad de definiciones matemáticas

En los algoritmos de encriptación es importante conocer de donde provienen cada uno de sus componentes, como funcionan, fortalezas y debilidades con la finalidad de usarlos correctamente, fortificarlos o simplemente adecuarlos a las necesidades particulares es por esto que se cuantificarán la cantidad de conceptos matemáticos que necesita cada algoritmo criptográfico.

Tabla 0-4 Cantidad de Definiciones Matemáticas

Algoritmo	**Definiciones Matemáticas**	**Cantidad de definiciones Matemáticas**
RSA	• Números Primos • Algoritmo de Euclides • Aritmética Modular	3
Diffie-Hellman	• Números Primos • Aritmética Modular • Logaritmos	3
El Rabin	• Número Compuesto • Número Primos Congruentes • Teoría de Números • Teorema Chino del Resto • Algoritmo Extendido de Euclides	5
El Gamal	• Número Primos • Primos Fuertes • Grupos Finitos • Aritmética Modular • Algoritmo Extendido de Euclides	5

Fuente: Paguay Mario. 2015

Los conceptos matemáticos en la Tabla IV-12 describen cuáles son 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, de la siguiente manera:

Tabla 0-5 Cantidad de Definiciones Matemáticas

Algoritmo	Definiciones Matemáticas	Valoración (%)	Escala Likert
RSA	3	60%	5
Diffie-Hellman	3	60%	5
El Rabin	5	100%	3
El Gamal	5	100%	3

Fuente: Paguay Mario.2015

Con la Tabla IV-13 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 quedan resumidos de la siguiente manera:

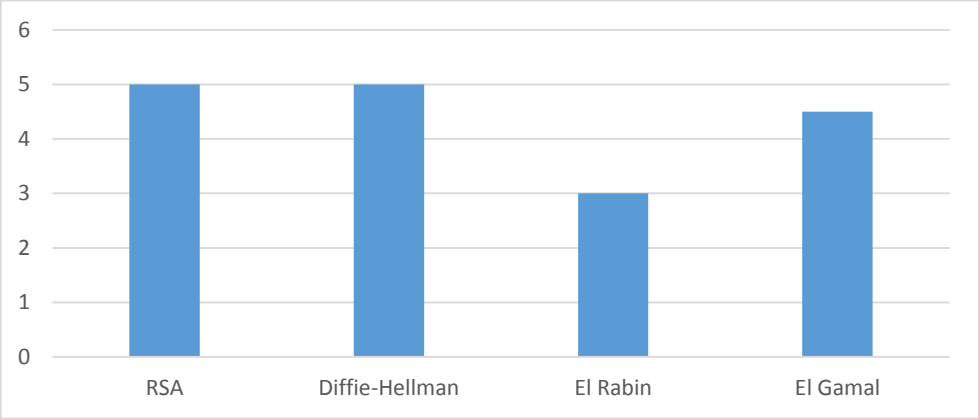


Gráfico 9-9 Gráfico Resumen Índice 9
Fuente: Paguay Mario. 2015

Índice 10 –Importancia de las definiciones matemáticas

Define si para el estudiante es necesario conocer los conceptos matemáticos en el Índice 9, tomando en consideración el área de impacto de los mismos es decir si intervienen en la obtención de los pasos, en los algoritmos de cifrado o des cifrado, en la preparación de los datos, si los conceptos son requeridos se analizará el impacto y se les asignará una valoración de alta media o baja, por lo que la valoración superior será la valoración del algoritmo de la siguiente manera:

Tabla 0-6 Impacto de los Conocimientos Matemáticos

Algoritmo	**Concepto Matemático**	**Área de Impacto**	**Impacto**	**Impacto General**
RSA	Números Primos	Datos de Entrada	Bajo	Bajo
	Algoritmo de Euclides	Ninguna	N/A	
	Aritmética Modular	Preparación de los datos, A. cifrado, A. Descifrado	Bajo	
Diffie-Hellman	Números Primos	Datos de Entrada	Bajo	Bajo
	Aritmética Modular	Preparación de los datos	Bajo	
	Logaritmos	A. Descifrado	Bajo	
El Rabin	Número Compuesto	Ninguna	N/A	Alto
	Número Primos Congruentes	Preparación de los datos	Medio	
	Aritmética Modular	A. Cifrado, A. Descifrado	Bajo	
	Teoría de Números	A. Descifrado	Alto	
	Teorema Chino del Resto	A. Descifrado	Alto	
	Algoritmo Extendido de Euclides	A. Descifrado	Alto	
El Gamal	Número Primos	N/A	N/A	Alto
	Primos Fuertes	Datos de Entrada	Alto	
	Grupos Finitos	Datos de Entrada	Alto	
	Aritmética Modular	Preparación de los Datos	Bajo	
	Algoritmo Extendido de Euclides	A. Des cifrado	Bajo	

Fuente: Paguay Mario. 2015

En la Tabla IV-14 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 (son también operaciones que se realizan frecuentemente en programación), 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 obteniendo ya los resultados del impacto se han dado las siguientes valoraciones en escala de Likert:

Tabla 0-7 Índice 9 Escala de Likert

Algoritmo	**Impacto General (Cualitativo)**	**Escala Likert (Cuantitativo)**
RSA	Bajo	5
Diffie-Hellman	Bajo	5
El Rabin	Alto	1
El Gamal	Alto	1

Fuente: Paguay Mario. 2015

Los valores Likert han sido asignados a las niveles de impacto 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 si bien es cierto son de importancia no son factores preponderantes para su aplicación es decir que el estudiante puede o no poseer dichos conocimientos que para entenderlos no le causarían mayor dificultad con lo que obtenemos el siguiente gráfico resumen:

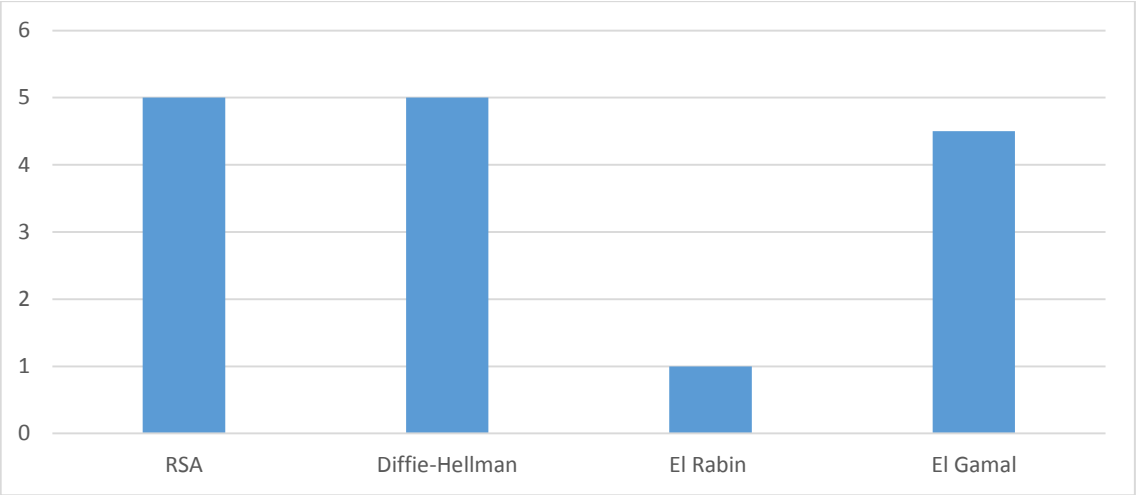


Gráfico 0-10 Gráfico Resumen Índice 10
Fuente: Paguay Mario. 2015

4.1.5. *Tabla resumen de análisis comparativo de los algoritmos criptográficos*

Tabla 0-8 Tabla Resumen Del Análisis Comparativo

INDICADORES	ÍNDICES	ALGORITMOS CRIPTOGRÁFICOS			
		RSA	Diffie-Hellman	El Rabin	El Gamal
1. Datos de Entrada	1. Números de Datos de Entrada	5	4	4	3
	2. Dificultad para la preparación de los Datos de Entrada	5	5	3	1
2. Algoritmo de Cifrado	3. Número de Pasos del Algoritmo	5	0	2	1
	4. Dificultad de los Pasos	5	0	5	1
	5. Orden de Complejidad	5	0	3	5
3. Algoritmo de Descifrado	6. Número de Pasos del Algoritmo	5	3	3	1
	7. Dificultad de los Pasos	5	3	1	5
	8. Orden de Complejidad	5	5	1	5
4. Conceptos Matemáticos	9. Cantidad de Definiciones Matemáticas Empleadas	5	5	3	3
	10. Importancia de los Conceptos Matemáticos	5	5	1	1
TOTALES		50/50	30/50	26/50	24/50

Fuente: Paguay Mario. 2015

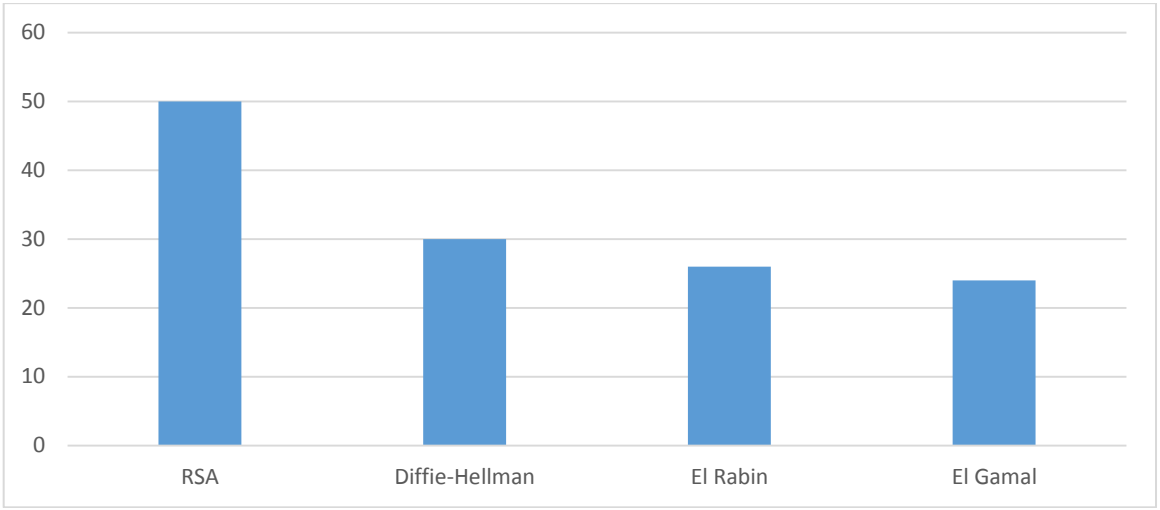


Gráfico 0-11 Gráfico Resumen Del Análisis Comparativo
Fuente: Paguay.2015

Al finalizar el análisis comparativo de los indicadores de la variable independiente mediante la Tabla IV-16 y el Gráfico IV-11 se ha determinado que el algoritmo criptográfico RSA es el más óptimo para la enseñanza de la asignatura de criptografía, puesto que poseen datos de entrada que no son complejos de manera cómo dos números primos, el algoritmo de obtención de datos no posee una complejidad superior y maneja conceptos matemáticos que el estudiante puede asimilar de forma rápida como la operación modulo, multiplicaciones y exponenciaciones, el siguiente algoritmo es Diffie-Hellman que ha obtenido 30 puntos de 50, en este algoritmo no se toma en cuenta un algoritmo de cifrado puesto que se apoya de otros algoritmos, pero si posee un algoritmo de des cifrado, en esta consideración podría ser una alternativa, los algoritmos El Rabin y El Gamal han quedado con valoraciones de 26 y 24 sobre 50, los dos algoritmos manejan conceptos matemáticos más especializados como grupos finitos, algoritmo extendido de Euclides para encontrar el dato en claro, grupos finitos de números, y el teorema chino del resto que permite encontrar raíces cuadradas en aritmética modular, por esta diferencia e conceptos y dificultad matemática más que algorítmica se ha definido que el algoritmo apto para la enseñanza de la criptografía es RSA con una valoración de 50 puntos sobre 50 puntos.

4.2. 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:

4.2.1. *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 descifrado

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 y se ha dado las siguientes opciones sobre la escala de Likert con sus respectivas valoraciones:

Tabla 0-9 Índice 1 Opciones

Opciones	Escala Likert
Totalmente de Acuerdo	5
De Acuerdo	4
Indiferente	3
Poco de Acuerdo	2
Nada de Acuerdo	1

Fuente: Paguay.2015

Con estas valoraciones de la Tabla IV-17 se han aplicado las encuestas sobre Google Docs., de un total de 23 encuestados sobre 4 algoritmos se han recabado los siguientes datos:

Tabla 0-10 Tabla de Frecuencias Índice 1

Algoritmo Criptográfico	Totalmente de Acuerdo	De Acuerdo	Indiferente	Poco de Acuerdo	Nada de Acuerdo	Totales
RSA	5	17	0	1	0	23
Diffie-Hellman	1	12	5	5	0	23
El Rabin	0	4	7	11	1	23
El Gamal	0	5	6	12	0	23

Fuente: Paguay Mario. 2015

La Tabla IV–18 evidencia los datos tabulados de las encuetas realizadas en Google Docs. De las cuales se ha realizado la misma pregunta a los estudiantes y se han tabulado 23 encuestas, con lo que se procede a medir las respuestas sobre la Escala de Likert mediante las valoraciones de la Tabla IV–17 con la siguiente observación cada punto cualitativo se multiplica por su correspondiente valor Likert por ejemplo en el valor totalmente de acuerdo en RSA.

$$Frecuencia = TMA * Valor\ Likert$$

$$Frecuencia = 25 * 5 = 115$$

En el valor ideal la escala toma 115 puntos de los cuales se calcularán los valores en porcentajes, debido a que totalmente de acuerdo significa la comprensión total del algoritmo en los estudiantes se define como un 100% así sucesivamente en la escala de Likert.

Tabla 0-11 Tabla de Frecuencias Valoradas Índice 1

Algoritmo Criptográfico	Totalmente de Acuerdo		De Acuerdo		Indiferente		Poco de Acuerdo		Nada De Acuerdo		Total	
RSA	25	21.7%	68	59.1%	0	0%	2	1.7%	0	0%	95	82.5%
Diffie-Hellman	5	4.3%	48	41.7%	15	13%	10	8.7%	0	0%	78	69%
El Rabin	0	0%	16	13.9%	21	18.3%	2	19.1%	1	0.9%	60	52.2%
El Gamal	0	0%	20	17.4%	18	15.7%	24≅ 20.9%		0	0%	6	54%

Fuente: Paguay Mario. 2015

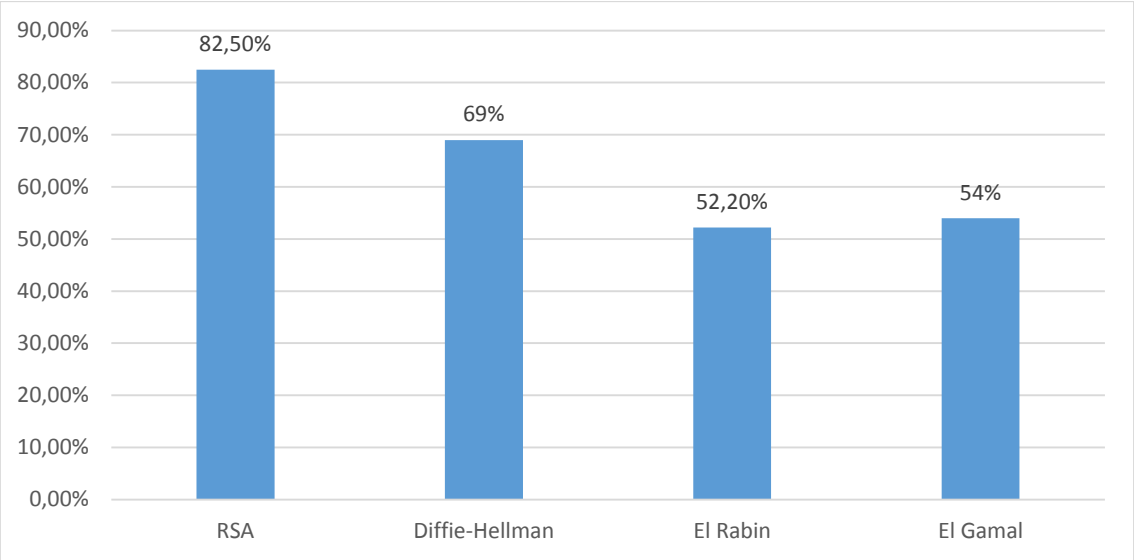


Gráfico 0-12 Gráfico Resumen Índice 1
Fuente: Paguay Mario. 2015

Luego de analizar los porcentajes y valoraciones notamos que el algoritmo RSA es 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.

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 para realizar la encuesta se ha resumido estas dos secciones en una sola y se ha planteado la siguiente pregunta: ¿Considera usted que la obtención de los datos de entrada es un proceso fácil?, de la cual se han generado las siguientes respuestas:

Tabla 0-12 Tabla de Frecuencias Índice 2

Algoritmo Criptográfico	Totalmente de Acuerdo	De Acuerdo	Indiferente	Poco de Acuerdo	Nada de Acuerdo	Total
RSA	0	16	5	2	0	23
Diffie-Hellman	1	10	2	10	0	23
El Rabin	0	3	7	11	2	23
El Gamal	0	3	6	12	2	23

Fuente: Paguay Mario. 2015

Para la valoración Likert se toma en cuenta la Tabla IV-17 debido a que se aplica la misma valoración cuantitativa a la escala cualitativa de la siguiente manera:

Tabla 0-13 Tabla de Frecuencias Valoradas Índice 2

Algoritmo Criptográfico	Totalmente de Acuerdo		De Acuerdo		Indiferente		Poco de Acuerdo		Nada de Acuerdo		Total	
RSA	0	0%	64	55.7%	15	13%	4	3.5%	0	0%	83	72.2%
Diffie-Hellman	5	4.3%	40	34.8%	6	5.2%	20	17.4%	0	0%	71	61.7%
El Rabin	0	0%	12	10.4%	21	18.3%	22	19.1%	2	1.7%	57	49.5%
El Gamal	0	0%	12	10.4%	18	15.7%	24	20.9%	2	1.7%	56	48.7%

Fuente: Paguay Mario. 2015

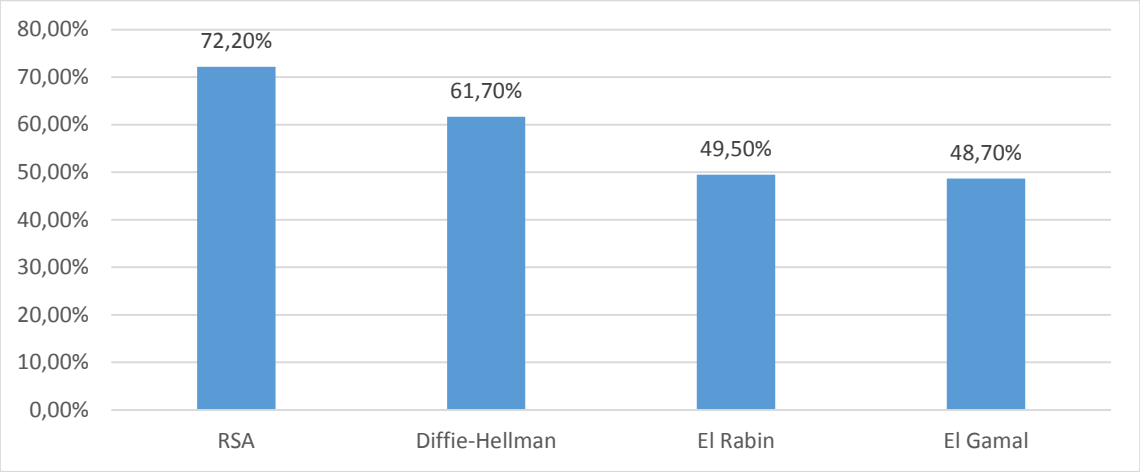


Gráfico 0-13 Gráfico Resumen Índice 2
Fuente: Paguay Mario. 2015

El Gráfico IV-13 corresponde a la pregunta 2 de las encuestas y se puede observar que el algoritmo criptográfico que más comprensión posee en su etapa inicial, es decir en los datos de entrada y su preparación es el RSA con un 72,20% de valoración total, esto puede darse por la facilidad de los conceptos matemáticos usados o por la cantidad de datos de entrada, 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"?, de la cual se han generado las siguientes respuestas:

Tabla 0-14 Tabla de Frecuencias Índice 3

Algoritmo Criptográfico	Comprensión Total	Comprensión Alta	Comprensión Media	Comprensión Baja	No se comprendió	Total
RSA	0	9	14	0	0	23
Diffie-Hellman	0	4	13	6	0	23
El Rabin	1	0	5	15	2	23
El Gamal	0	0	6	16	1	23

Fuente: Paguay Mario. 2015

Para la valoración Likert se usará la siguiente escala cuantitativa a la escala cualitativa:

Tabla 0-15 Índice 3 Opciones

Opciones	Escala Likert
Comprensión Total	5
Comprensión Alta	4
Comprensión Media	3
Comprensión Baja	2
No se comprendió	1

Fuente: Paguay Mario. 2015

Comprensión total significa que el estudiante ha comprendido todo el proceso mediante el cual un texto en claro se ha cifrado, caso contrario No se comprendió toma en consideración que el estudiante no ha podido discernir los pasos para cifrar los datos.

Tabla 0-16 Tabla de Frecuencias Valoradas Índice 3

Algoritmo Criptográfico	Comprensión Total		Comprensión Alta		Comprensión Media		Comprensión Baja		No se comprendió		Totales	
RSA	0	0%	36	31.3%	42	36.5%	0	0%	0	0%	78	67.8%
Diffie-Hellman	0	0%	16	13.9%	39	33.9%	18	7%	0	0%	73	63.5%
El Rabin	5	4,3%	0	0%	15	13%	30	26.1%	2	1.7%	52	45.1%
El Gamal	0	0%	0	0%	18	15.7%	31	26.6%	1	0.9%	50	43.2%

Fuente: Paguay Mario. 2015

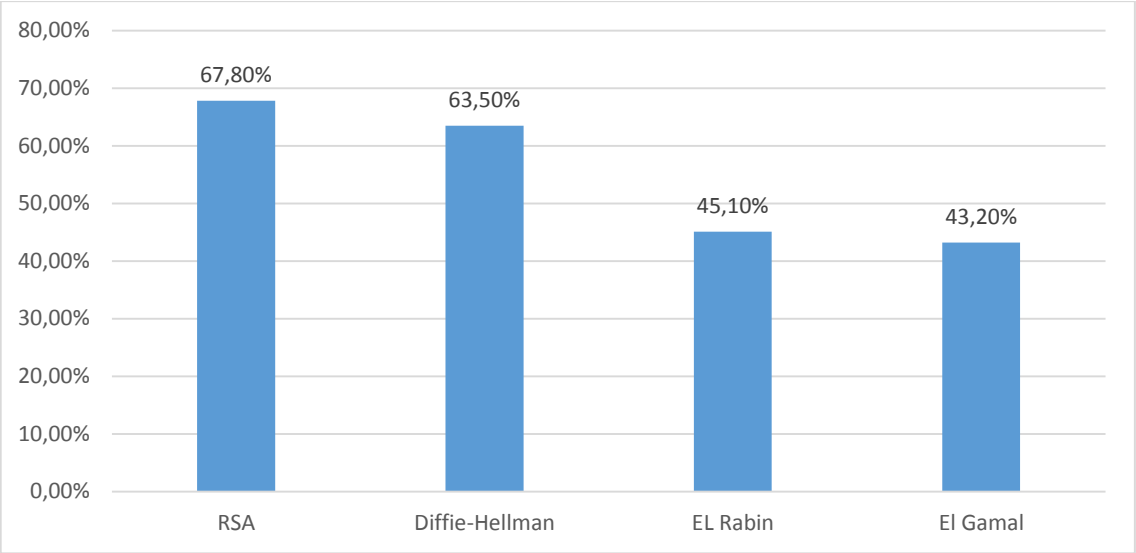


Gráfico 0-14 Gráfico Resumen Índice 3
Fuente: Paguay Mario. 2015

RSA en esta pregunta es el algoritmo criptográfico que mejor permite el entendimiento de la encriptación de datos para los estudiantes, en esta pregunta se observa que RSA obtiene el 67,80% correspondiendo a una valoración Likert de 78 puntos sobre 23 encuestados con 9 personas que han optado por la repuesta de comprensión alta, esta valoración puede darse ya que el algoritmo para encriptar los dato de RSA posee un solo paso.

Índice 4 – Conceptualización del algoritmo de descifrado

El algoritmo de des cifrado 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 des cifrado de "RSA"?, de la cual se han generado las siguientes respuestas:

Tabla 0-17 Tabla de Frecuencias Índice 4

Algoritmo Criptográfico	Comprensión Total	Comprensión Alta	Comprensión Media	Comprensión Baja	No se comprendió	Totales
RSA	0	8	14	1	0	23
Diffie-Hellman	0	4	14	5	0	23
El Rabin	0	1	5	15	2	23
El Gamal	0	0	6	16	1	23

Fuente: Paguay Mario. 2015

Para la valoración Likert se toma en cuenta la Tabla IV-23 debido a que se aplica la misma valoración cuantitativa a la escala cualitativa de la siguiente manera:

Tabla 0-18 Tabla de Frecuencias Valoradas Índice 4

Algoritmo Criptográfico	Comprensión Total		Comprensión Alta		Comprensión Media		Comprensión Baja		No se comprendió		Totales	
RSA	0	0%	32	27.8%	42	36.5%	2	1.7%	0	0%	76	66%
Diffie-Hellman	0	0%	16	13.9%	42	33.9%	10	8.7%	0	0%	68	59.1%
El Rabin	0	0%	4	3.5%	15	13%	30	26.1%	2	1.7%	51	44.3%
El Gamal	0	0%	0	0%	18	15.6%	32	27.8%	1	0.9%	51	43.3%

Fuente: Paguay Mario. 2015

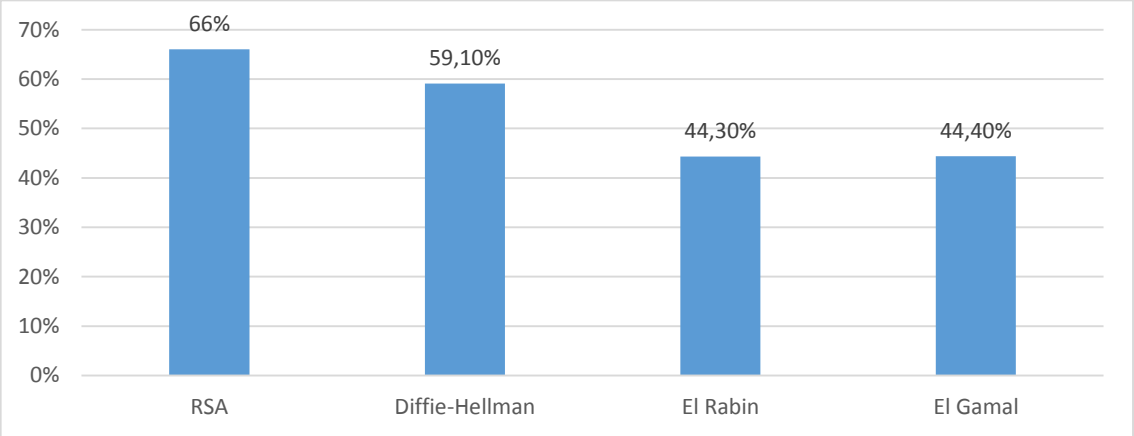
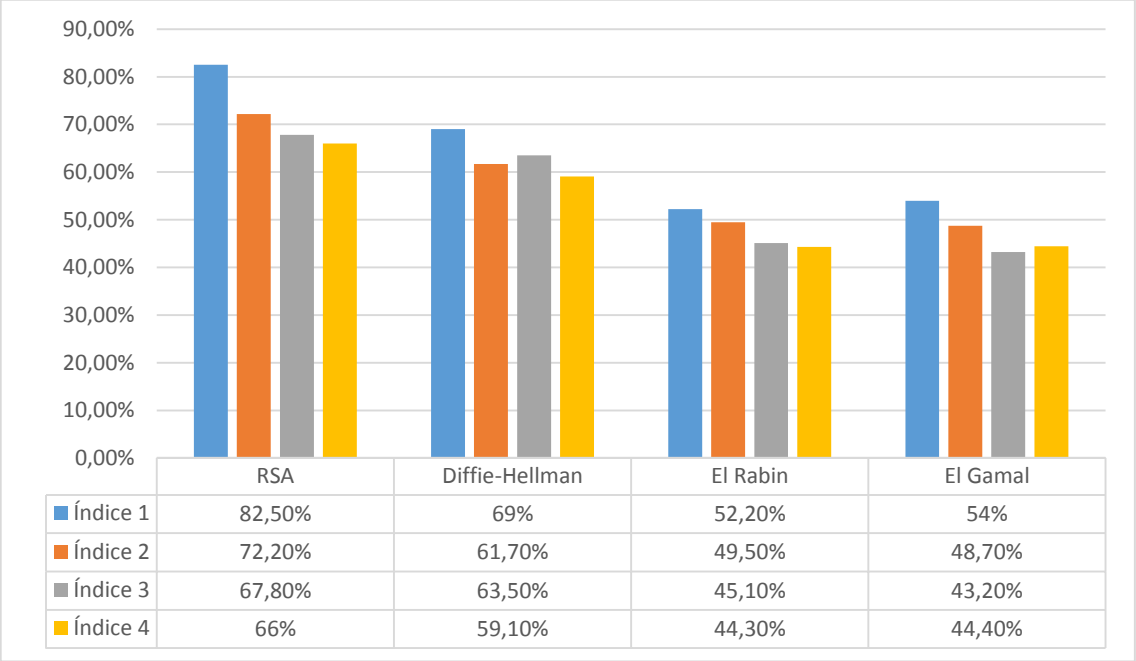


Gráfico 0-15 Gráfico Resumen Índice 4
Fuente: Paguay Mario. 2015

En el nivel de comprensión del algoritmo de descifrado Gráfico IV-15 se observa 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 del proceso de transformación del texto cifrado a texto en claro.

Resumen comparativo



	RSA	Diffie-Hellman	El Rabin	El Gamal
Índice 1	82,50%	69%	52,20%	54%
Índice 2	72,20%	61,70%	49,50%	48,70%
Índice 3	67,80%	63,50%	45,10%	43,20%
Índice 4	66%	59,10%	44,30%	44,40%

Gráfico 0-16 Gráfico Resumen Comparativo Indicador 1
Fuente: Paguay Mario. 2015

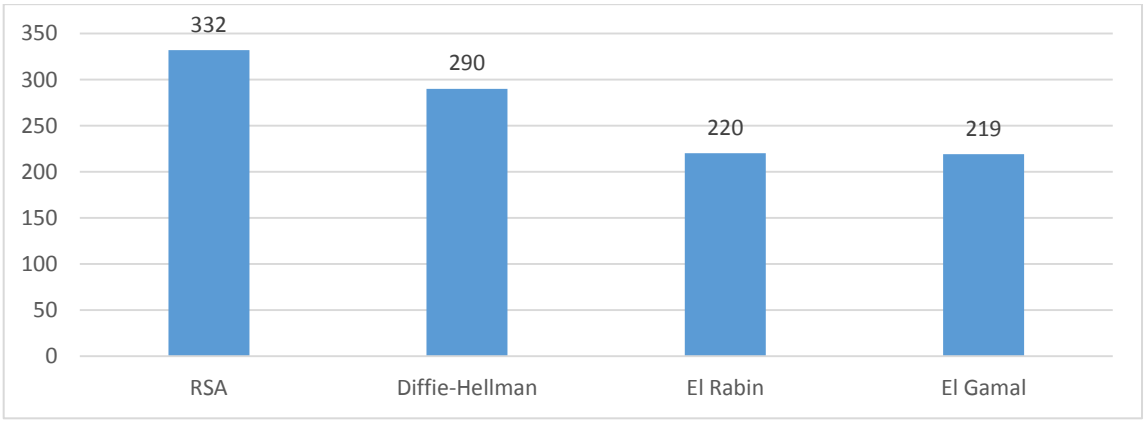


Gráfico 0-17 Gráfico Resumen Valoración Likert Indicador 1
Fuente: Paguay Mario. 2015

Al finalizar la tabulación de los índices del primer indicador Gráfico IV-16 y Gráfico IV-17 se observa que el algoritmo RSA posee una valoración de 332 puntos mientras que El Gamal posee 219 puntos, lo que nos indica que el nivel de comprensión más alto posee el algoritmo RSA, siendo 4 las preguntas tabuladas en donde se ha definido la comprensión del algoritmo criptográfico, los datos de entrada y su preparación así como el algoritmo de cifrado y de descifrado, con un total de 23 estudiantes encuestados en las cátedras dictadas al séptimo semestre de la Escuela de Ingeniería en Sistemas.

4.2.2. *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 des cifrado, 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"? haciendo referencia a la comprensión de los procesos y cuan capaz se siente el estudiante para ejemplificar los conceptos, se han generado los siguientes resultados:

Tabla 0-19 Tabla de Frecuencias Índice 5

Algoritmo Criptográfico	Sumamente Fácil	Fácil	Complicado	Difícil	Sumamente Difícil	Totales
RSA	0	8	13	2	0	23
Diffie-Hellman	0	3	16	2	2	23
El Rabin	0	0	13	5	5	23
El Gamal	0	0	12	6	5	23

Fuente: Paguay Mario. 2015

Para la valoración Likert se usará la siguiente escala cuantitativa a la escala cualitativa:

Tabla 0-20 Tabla de Opciones Índice 5

Opciones	Escala Likert
Sumamente Fácil	5
Fácil	4
Complicado	3
Difícil	2
Sumamente Difícil	1

Fuente: Paguay Mario. 2015

Para la valoración Likert se toma en cuenta la Tabla IV-31 y se obtiene las siguientes valoraciones y porcentajes del índice:

Tabla 0-21 Tabla de Frecuencias Valoradas Índice 5

Algoritmo Criptográfico	Sumamente Fácil		Fácil		Complicado		Difícil		Sumamente Difícil		Totales	
RSA	0	0%	32	27.8%	39	33.9%	4	3.5%	0	0%	75	65.2%
Diffie-Hellman	0	0%	12	10.4%	48	41.7%	4	3.5%	2	1.7%	66	57.3%
El Rabin	0	0%	0	0%	39	33.9%	10	8.7%	5	4.3%	54	47%
El Gamal	0	0%	0	0%	36	31.3%	12	10.4%	5	4.3%	53	46.1%

Fuente: Paguay.2015

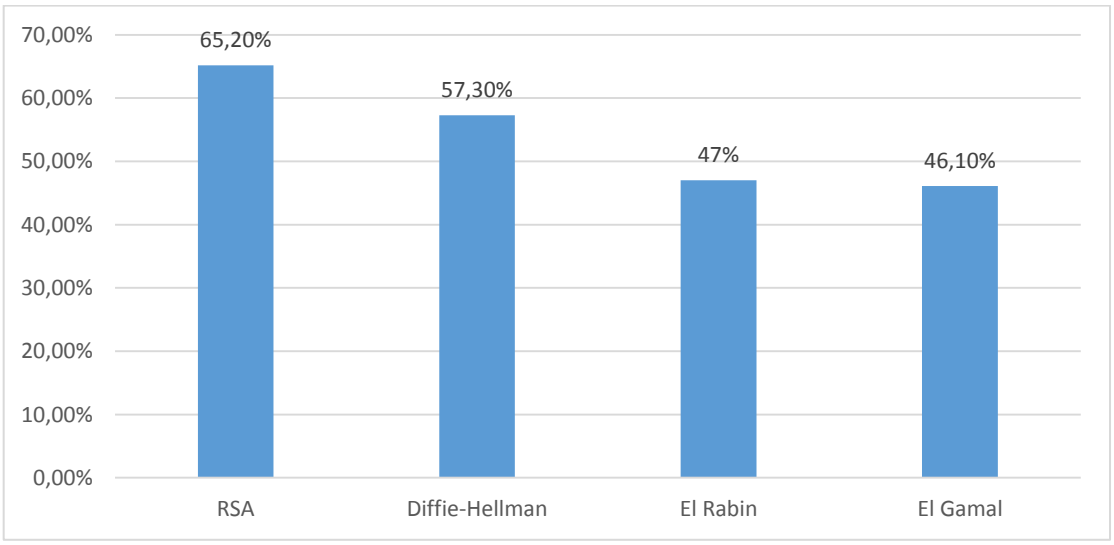


Gráfico 0-18 Gráfico Resumen Índice 5
Fuente: Paguay Mario. 2015

En la pregunta número 5 Gráfico IV-18 se busca medir si un estudiante puede resolver un problema usando un algoritmo criptográfico de los impartidos en la cátedra se evidencia 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 indagado entre los estudiantes sí podrían personalizar los algoritmos criptográficos o al menos un algoritmo para lo cual se ha generado la siguiente pregunta: ¿Podría Usted personalizar el algoritmo "RSA"? y se ha obtenido los siguientes resultados:

Tabla 0-22 Tabla de Frecuencias Índice 6

Algoritmo Criptográfico	Totalmente de Acuerdo	De Acuerdo	Indiferente	Poco de Acuerdo	Nada de Acuerdo	Totales
RSA	0	7	5	9	2	23
Diffie-Hellman	0	4	7	9	3	23
El Rabin	0	2	6	7	8	23
El Gamal	0	1	7	8	7	23

Fuente: Paguay.2015

Para la valoración Likert se toma en cuenta la Tabla IV-17 debido a que se aplica la misma valoración cuantitativa a la escala cualitativa de la siguiente manera:

Tabla 0-23 Tabla de Frecuencias Valoradas Índice 6

Algoritmo Criptográfico	Totalmente de Acuerdo		De Acuerdo		Indiferente		Poco de Acuerdo		Nada de Acuerdo		Totales	
RSA	0	0%	28	24.3%	15	13%	18	15.7%	2	1.7%	63	54.7%
Diffie-Hellman	0	0%	16	13.9%	21	18.3%	18	15.7%	3	2.6%	58	50.4%
El Rabin	0	0%	8	7%	18	15.7%	14	12.2%	8	7%	48	41.7%
El Gamal	0	0%	4	3.5%	21	18.3%	16	13.9%	7	6.1%	48	41.7%

Fuente: Paguay Mario. 2015

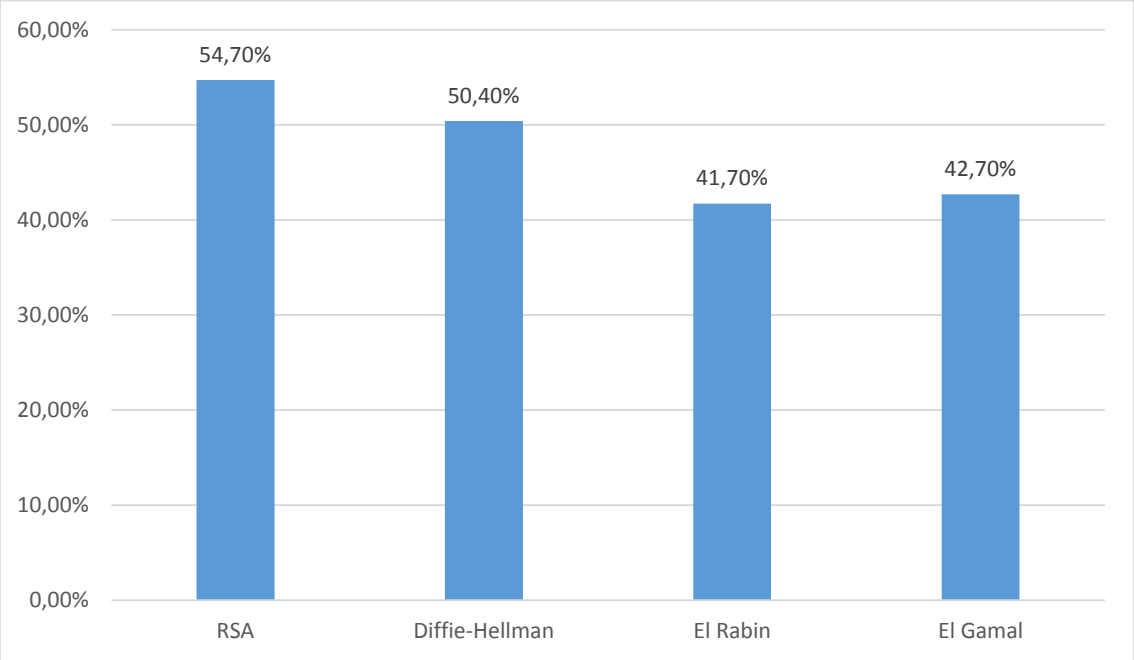


Gráfico 0-19 Gráfico Resumen Índice 6

Fuente: Paguay Mario. 2015

De la pregunta número 6 se ha podido determinar que el algoritmo RSA es el algoritmo más personalizable para los estudiantes es decir en algún punto de su estructura se puede modificar o cambiar 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.

Para determinar si el estudiante es capaz de transformar un texto cifrado en texto en claro se ha realizado la siguiente pregunta: ¿Cuán difícil le resultaría descifrar un mensaje usando "RSA"?, se han generado los siguientes resultados:

Tabla 0-24 Tabla de Frecuencias

Algoritmo Criptográfico	Sumamente Fácil	Fácil	Complicado	Difícil	Sumamente Difícil	Totales
RSA	0	9	11	2	1	23
Diffie-Hellman	0	5	15	2	1	23
El Rabin	0	0	12	6	5	23
El Gamal	0	0	10	9	4	23

Fuente: Paguay Mario. 2015

Para la valoración Likert se toma en cuenta la Tabla IV-31 y se obtiene las siguientes valoraciones y porcentajes del índice:

Tabla 0-25Tabla de Frecuencias Valoradas Índice 7

Algoritmo Criptográfico	Sumamente Fácil		Fácil		Complicado		Difícil		Sumamente Difícil		Totales	
RSA	0	0%	36	31.3%	33	28.7%	4	3.5%	1	0.9%	74	64.3%
Diffie-Hellman	0	0%	20	17.4%	45	39.1%	4	3.5%	1	0.9%	70	60.9%
El Rabin	0	0%	0	0%	36	31.3%	12	10.4%	5	4.3%	53	46.1%
El Gamal	0	0%	0	0%	30	26.1%	18	15.7%	4	3.5%	52	45.2%

Fuente: Paguay Mario. 2015

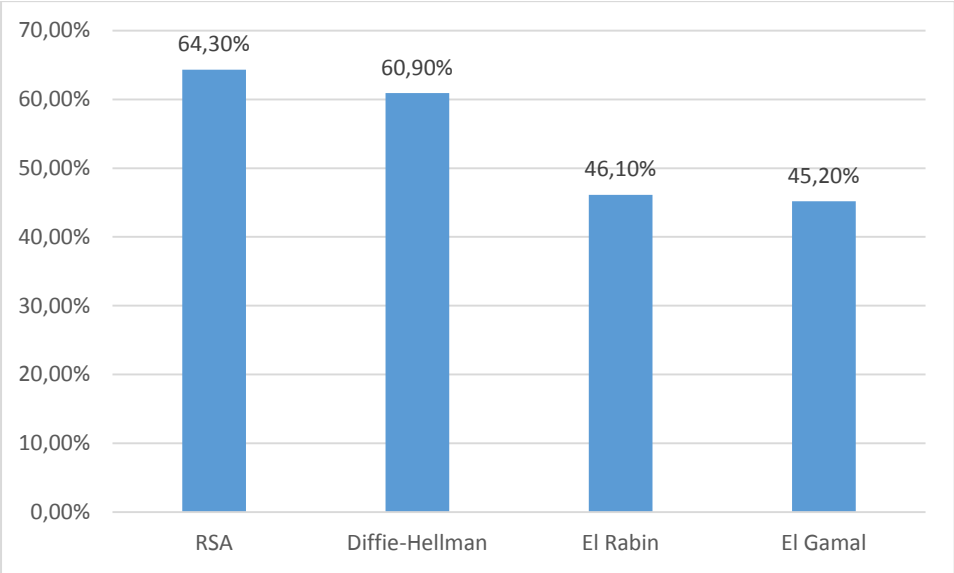
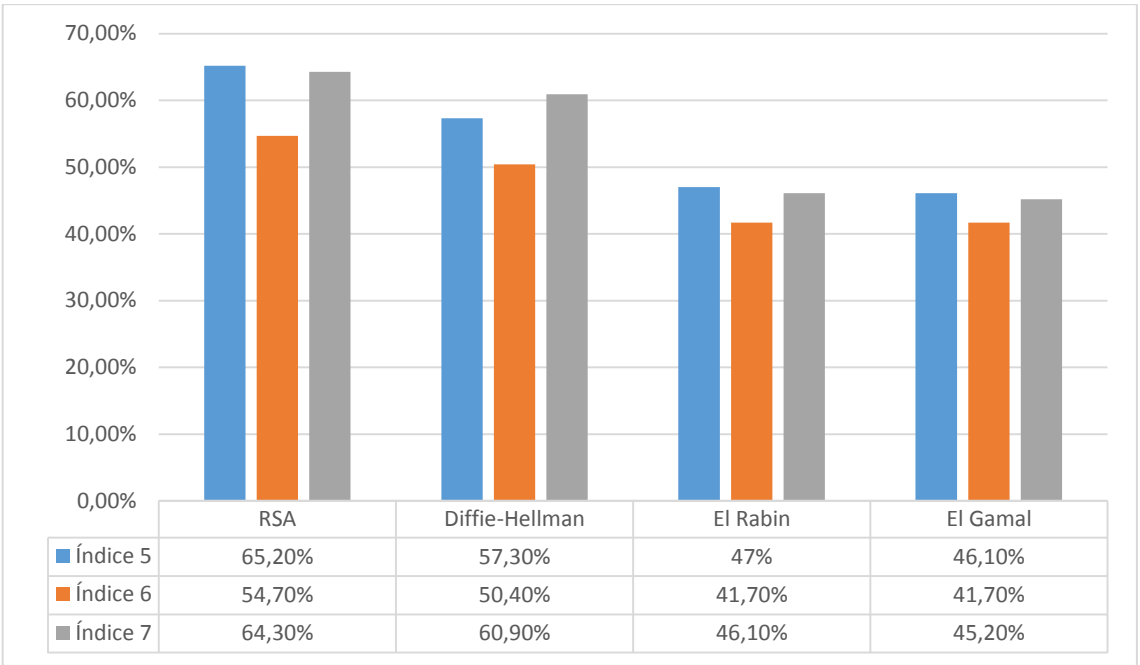


Gráfico 0-20 Gráfico Resumen Índice 7
Fuente: Paguay Mario. 2015

En la pregunta 7 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, lo que permite distinguir que RSA es mucho más fácil de comprender para los estudiantes considerando que su algoritmo de descifrado es el de menor complejidad en comparación a los demás.

Resumen comparativo



	RSA	Diffie-Hellman	El Rabin	El Gamal
Índice 5	65,20%	57,30%	47%	46,10%
Índice 6	54,70%	50,40%	41,70%	41,70%
Índice 7	64,30%	60,90%	46,10%	45,20%

Gráfico 0-21 Gráfico Resumen Comparativo Índices Indicador 2
Fuente: Paguay Mario. 2015

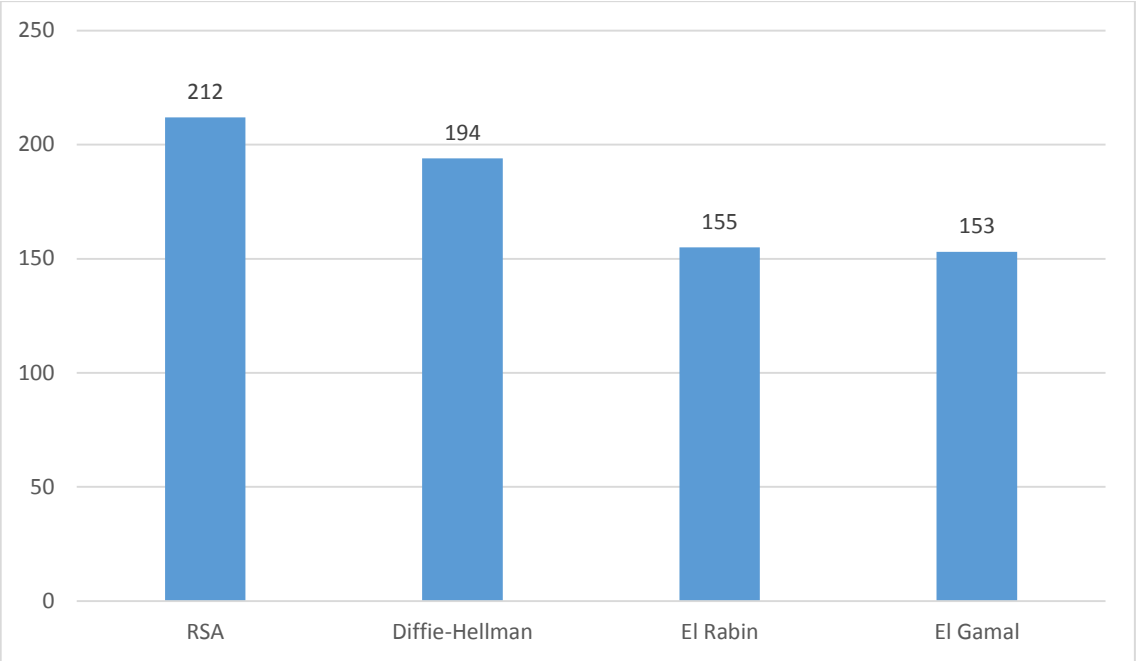


Gráfico 0-22 Gráfico Resumen Valoración Likert Indicador 2
Fuente: Paguay Mario. 2015

Al finalizar la tabulación de los índices como muestra en Gráfico IV-21 y Gráfico IV-22 del segundo indicador se observa que el algoritmo RSA posee una valoración de 212 puntos mientras que El Gamal posee 153 puntos, lo que nos indica que el nivel de aplicación de conocimientos más alto posee el algoritmo RSA, siendo 3 las preguntas tabuladas en donde se ha definido la capacidad del estudiante de replicar los contenidos asimilados, con un total de 23 estudiantes encuestados en las cátedras dictadas al séptimo semestre de la Escuela de Ingeniería en Sistemas.

4.2.3. *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;

Se han generado preguntas sobre cuánto conoce el estudiante sobre cada concepto y se han tabulado las siguientes respuestas:

Tabla 0-26 Tabla de Frecuencias Indicador 3

Concepto Matemático	**Conoce Totalmente el Tema**	**Conoce Medianamente el Tema**	**Conoce el Tema**	**No Conoce Mucho el Tema**	**No Conoce el Tema**	**Totales**
Aritmética Modular	0	4	3	12	4	23
Estructuras Algebraicas	0	6	5	12	0	23
Logaritmos	0	8	11	4	0	23
Obtención de Raíces Cuadradas	0	0	3	14	6	23
Teorema Chino Del Resto	0	0	1	6	16	23
Algoritmo Extendido de Euclides	0	2	4	14	3	23
Curvas Elípticas	0	4	2	10	7	23
Grupos Finitos	1	4	5	9	4	23

Fuente: Paguay Mario. 2015

Para realizar la valoración de la Tabla IV-34 mediante la escala de Likert se ha propuesto los siguientes valores cuantitativos a los valores cualitativos de la siguiente manera:

Tabla 0-27 Opciones Indicador 3

Opciones	Escala Likert
Conoce Totalmente el Tema	5
Conoce Medianamente el Tema	4
Conoce el Tema	3
No Conoce Mucho el Tema	2
No Conoce el Tema	1

Fuente: Paguay Mario. 2015

Tabla 0-28 Tabla de Frecuencias Valoradas Indicador 3

Concepto Matemático	Conoce Totalmente el Tema		Conoce Medianamente el Tema		Conoce el Tema		No Conoce Mucho el Tema		No Conoce el Tema		Totales	
Aritmética Modular	0	0%	16	13.9%	9	7.8%	24	20.9%	4	3.5%	53	46.1%
Estructuras Algebraicas	0	0%	24	20.9%	15	13%	24	20.9%	0	0%	63	54.8%
Logaritmos	0	0%	32	27.8%	33	28.7%	8	6.6%	0	0%	73	63.5%
Obtención de Raíces Cuadradas	0	0%	0	0%	9	7.8%	28	24.3%	6	5.2%	43	37.4%
Teorema Chino Del Resto	0	0%	0	0%	3	2.6%	12	10.4%	16	13.9 %	31	27%
Algoritmo Extendido de Euclides	0	0%	8	6.6%	12	10.4%	28	24.3%	3	2.6%	51	44.3%
Curvas Elípticas	0	0%	16	13.9%	6	5.2%	20	17.4%	7	6.1%	49	42.6%
Grupos Finitos	5	4.3%	16	13.9%	15	13%	18	15.6%	4	3.5%	58	50.4%

Fuente: Paguay Mario. 2015

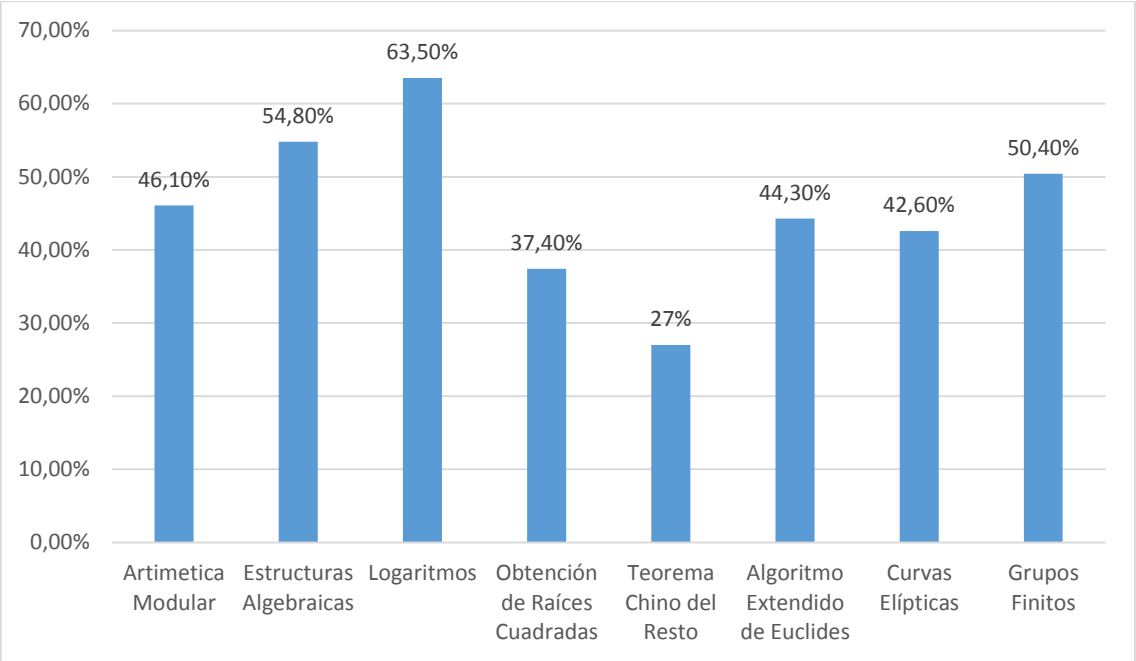


Gráfico 0-23 Gráfico Resumen Valoración Total Likert Indicador 3
Fuente: Paguay Mario. 2015

De entre todos los conceptos matemáticos Gráfico IV-23 que han sido indagados en los estudiantes en las preguntas formuladas en las encuestas podemos ver que 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:

4.2.4. *Conceptos matemáticos RSA*

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 de los cuales los estudiantes poseen más conocimiento sobre estructuras algebraicas con 63 Likert puntos sobre 115 con un total de 167 puntos sobre conocimientos matemáticos.

Tabla 0-29 Conceptos Matemáticos RSA

Concepto Matemático	Valoración Likert (/115)
Aritmética Modular	53
Estructuras Algebraicas	63
Algoritmo de Euclides extendido	51
Total	**167**

Fuente: Paguay Mario. 2015

4.2.5. *Conceptos matemáticos Diffie-Hellman*

Para la comprensión del algoritmo Diffie-Hellman se han determinado los siguientes conceptos matemáticos Aritmética Modular, Estructuras Algebraicas y Grupos Finitos de los cuales los estudiantes poseen más conocimiento sobre estructuras algebraicas con 63 Likert puntos sobre 115 con un total de 174 puntos sobre conocimientos matemáticos.

Tabla 0-30 Conceptos Matemáticos Diffie-Hellman

Conceptos Matemáticos	Valoración Likert (/115)
Aritmética Modular	53
Estructuras algebraicas	63
Grupos finitos	58
Total	**174**

Fuente: Paguay Mario. 2015

4.2.6. *Conceptos matemáticos El Rabin*

Del total de conceptos matemáticos se han distinguido 6 necesarios para la comprensión del algoritmo El Rabin los cuales son Aritmética Modular, Estructuras Algebraicas, El Algoritmo Extendido de Euclides, El Teorema Chino del Resto, Logaritmos y la Obtención de Raíces Cuadradas de los cuales los estudiantes poseen más conocimiento sobre estructuras logaritmos con 63 Likert puntos sobre 115 con un total de 314 puntos sobre conocimientos matemáticos, lo que diferencia este algoritmo de los demás es que los conocimientos necesarios son mucho más complejos que los anteriores y requieren más dominio de la matemática.

Tabla 0-31 Conceptos Matemáticos El Rabin

Conceptos Matemáticos	Valoración Likert(/115)
Aritmética Modular	53
Estructuras algebraicas	63
Teorema Chino del Resto	31
Algoritmo Extendido de Euclides	51
Logaritmos	73
Obtención de Raíces Cuadradas	43
Total	**314**

Fuente: Paguay Mario. 2015

4.2.7. *Conceptos matemáticos El Gamal*

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 de los cuales los estudiantes poseen más conocimiento sobre estructuras grupos finitos con 58 Likert puntos sobre 115 con un total de 193 puntos sobre conocimientos matemáticos, estas definiciones pueden ser equiparadas con el algoritmo El Rabin por su complejidad.

Tabla 0-32 Conceptos Matemáticos El Gamal

Conceptos Matemáticos	Valoración Likert(/115)
Grupos Finitos	58
Aritmética Modular	53
Teorema chino del resto	31
Algoritmo de Euclides extendido	51
Total	**193**

Fuente: Paguay Mario. 2015

Para realizar la comparación entre los conceptos matemáticos de la Tabla IV-40 cada algoritmo posee un total del número de conceptos necesarios y se considera el 100% de conocimientos para ese algoritmo y se contrasta con la sumatoria encuestada de la siguiente manera:

Lo optimo de cada índice es 5 x 23 =115 y como cada algoritmo tiene determinado números de índices (conocimiento sobre algún tema de matemáticas) ejemplo el RSA tiene 3 índices (conceptos matemáticos) 3 x 115= 345, así generamos lo siguiente

Tabla 0-33 Comparación Conceptos Matemáticos

Algoritmo Criptográfico	Numero de conceptos matemáticos	Total Likert	Total Likert Encuestado	Porcentaje
RSA	3	345	167	48,4%
Diffie-Hellman	3	345	174	50,4%
El Rabin	6	690	314	45.5%
El Gamal	4	460	193	42,0%

Fuente: Paguay Mario. 2015

Se puede evidenciar en la Tabla IV-41 que los estudiantes poseen más conocimientos matemáticos sobre el algoritmo Diffie-Hellman por sobre los otros algoritmos según las encuestas realizadas, haciendo referencia además que la complejidad de los mismos son mucho menores que El Rabin y El Gamal, y pueden ser similares o iguales a los del Algoritmo RSA, los resultados se pueden evidenciar en el siguiente gráfico resumen:

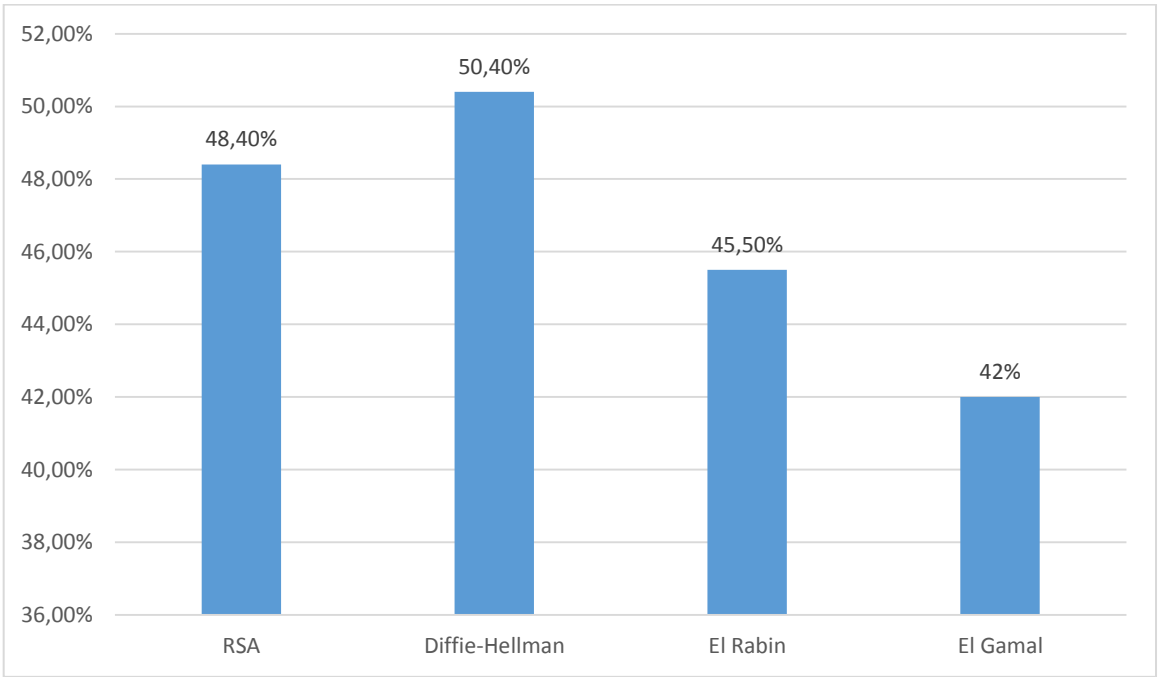


Grafico 0-34 Gráfico Resumen Conceptos Matemáticos

Fuente: Paguay Mario. 2015

4.2.8. *Tabla resumen del análisis de la variable dependiente*

Tabla 0-35 Resumen Análisis Variable Dependiente

Algoritmo Criptográfico	Indicador 1		Indicador 2		Indicador 3		Total		Porcentaje (%)
	Obt.	Opt.	Obt.	Opt.	Obt.	Opt.	Obt.	Opt.	
RSA	332	460	212	345	167	345	711	1150	61,83
Diffie-Hellman	290	460	194	345	174	345	685	1150	59,57
El Rabin	220	460	155	345	314	690	689	1495	46,09
El Gamal	219	460	153	345	193	460	565	1265	44,66

Fuente: Paguay Mario. 2015

En la Tabla IV-43 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 de los cuales el algoritmo RSA posee un 61,83% del total esperado (Indicador 1 =460= 5x23x4+ Indicador 2 + Indicador 3) y el Algoritmo El Gamal es el más Bajo con un 44,66% de su total esperado (con lo que se llega a concluir que para los estudiantes ha resultado mejor y más comprensible el Algoritmo RSA con esto tenemos una pauta general para realizar la comprobación de la Hipótesis, los datos recopilados han sido generados de la operacionalización de las variables y sus indicadores resumiéndolo en el siguiente gráfico:

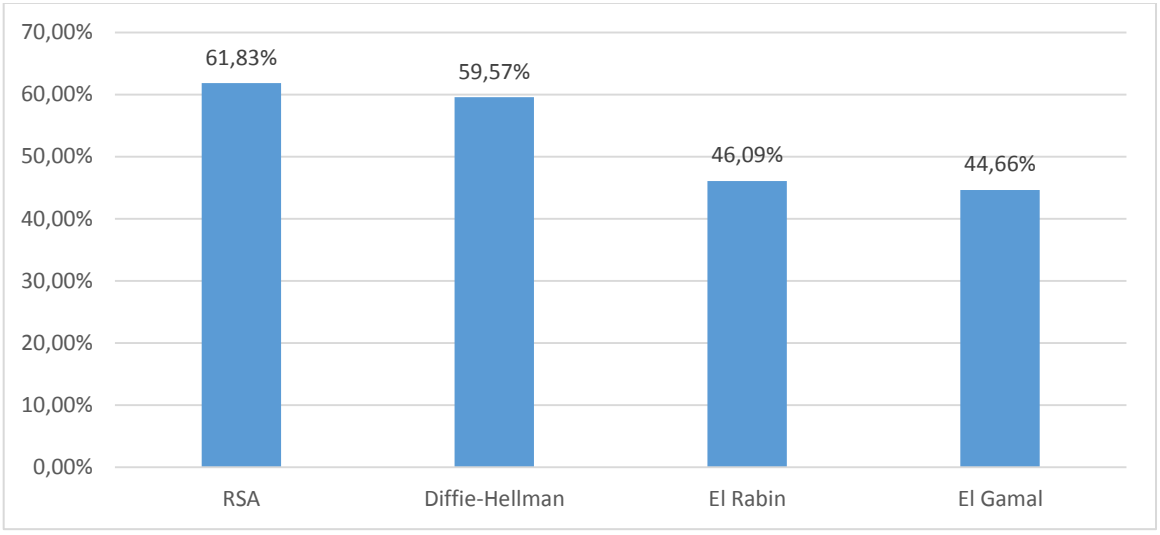


Gráfico 0-24 Gráfico Resumen Variable Dependiente

Fuente: Paguay Mario. 2015

4.2.9. Resumen de la variable dependiente por algoritmo criptográfico

Para realizar la comprobación de la Hipótesis se debe analizar el comportamiento de los algoritmos en base a las tabulaciones de las encuestas aplicadas a los estudiantes, al realizar dicha discriminación de datos se han obtenido las siguientes tablas en donde se pueden observar los totales por cada escenario realizado en donde los 5 criterios Likert han sido revalorizados y estandarizados en Mejor (5 y 4 escala Likert), Indiferente (3 escala Likert), no mejor (2 y 1 escala Likert), cada dato de la tabla ha sido contabilizado de los cuadros de los 3 indicadores de la variable dependiente en donde se han visto cuantas ocurrencias tiene cada escala Likert y ha sido reformulado.

Tabla 0-36 Tabla Resumen Algoritmo RSA

Algoritmo	Indicador	Índice	Mejor		Indiferente	No Mejor		Totales
			5	4	3	2	1	
RSA	I1	i1	5	17	0	1	0	**23**
		i2	0	16	5	2	0	**23**
		i3	0	9	14	0	0	**23**
		i4	0	8	14	1	0	**23**
		Totales	**55**		**33**	**4**		**92**
	I2	i5	0	8	13	**2**	0	**23**
		i6	0	7	5	9	2	**23**
		i7	0	9	11	2	1	**23**
		Totales	**24**		**29**	**16**		**69**
	I3	i8	0	4	4	13	2	**23**
		Totales	**4**		**4**	**15**		**23**

Realizado por: Paguay Mario.2015

Tabla 0-4 Tabla Resumen Algoritmo Diffie-Hellman

Algoritmo	Indicador	Índice	Mejor		Indiferente	No Mejor		Totales
			5	4	3	2	1	
Diffie-Hellman	I1	i1	1	12	5	5	0	**23**
		i2	1	10	2	10	0	**23**
		i3	0	4	13	6	0	**23**
		i4	0	4	14	5	0	**23**
		Totales	**32**		**34**	**26**		**92**
	I2	i5	0	3	16	2	2	**23**
		i6	0	4	7	9	3	**23**
		i7	0	5	15	2	1	**23**
		Totales	**12**		**38**	**19**		**69**
	I3	i8	0	5	4	11	3	**23**
		Totales	**5**		**4**	**14**		**23**

Fuente: Paguay Mario. 2015

Tabla 0-37 Tabla Resumen Algoritmo El Rabin

Algoritmo	Indicador	Índice	Mejor		Indiferente	No Mejor		Totales
			5	4	3	2	1	
El Rabin	I1	i1	0	4	7	11	1	**23**
		i2	0	3	7	11	2	**23**
		i3	1	0	5	15	2	**23**
		i4	0	1	5	15	2	**23**
		Totales	**9**		**24**	**59**		**92**
	I2	i5	0	0	13	5	5	**23**
		i6	0	2	6	7	8	**23**
		i7	0	0	10	9	4	**23**
		Totales	**2**		**29**	**38**		**69**
	I3	i8	0	3	5	10	5	**23**
		Totales	**3**		**5**	**15**		**23**

Fuente: Paguay Mario. 2015

Tabla 0-38 Resumen Algoritmo El Gamal

Algoritmo	Indicador	Índice	Mejor		Indiferente	No Mejor		Totales
			5	4	3	2	1	
El Gamal	I1	i1	0	5	6	12	0	**23**
		i2	0	3	6	12	2	**23**
		i3	0	0	6	16	1	**23**
		i4	0	0	6	16	1	**23**
		Totales	**8**		**24**	**60**		**92**
	I2	i5	0	0	12	6	5	**23**
		i6	0	1	7	8	7	**23**
		i7	0	0	10	9	4	**23**
		Totales	**1**		**29**	**39**		**69**
	I3	i8	0	3	3	10	7	**23**
		Totales	**3**		**3**	**17**		**23**

Fuente: Paguay Mario. 2015

Para Realizar el Indicador ocho (8) se ha realizado una media aritmética de los índices del indicador 3 que se necesitan para cada algoritmo

4.2.10. Tabla de contingencia frecuencias observadas

Para realizar la siguiente tabla de frecuencias se han sumado todos los valores de mejor, indiferente, no mejor de las tablas de resumen de los algoritmos por cada indicador y se han obtenido los siguientes valore observados luego de las encuestas:

Tabla 0-39 Tabla de Frecuencias Observadas

Algoritmo	Mejor	Indiferente	No Mejor	Totales
RSA	83	66	35	184
Diffie-Hellman	49	76	59	184
El Rabin	14	58	112	184
El Gamal	12	56	116	184

Fuente: Paguay.2015

En la Tabla IV-48 se observa claramente que el valor de mejor más alto lo obtiene el algoritmo RSA con 83 luego de sumar ocho (8) indicadores, y el valor más bajo doce (12) de El Gamal, caso contrario los mismos algoritmos poseen valores de No mejor opuestos de un total de ciento ochenta y cuatro (184) puntos.

4.3. Prueba de hipótesis mediante el estadístico X^2(Chi - cuadrado)

4.3.1. *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:

H_1: El Algoritmo RSA es Mejor que el Algoritmo Diffie-Hellman.

De esta hipótesis se abstrae la siguiente afirmación: H_1 : Existen diferencias significativas entre los procedimientos, con su correspondiente negación H_0 : ***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 siguiente tabla:

Tabla 0-40 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: Paguay Mario. 2015

Para obtener las frecuencias esperadas se emplea la siguiente fórmula:

$$fe_{ij} = \frac{Total\ Fila_i * Total\ Columna_j}{N}$$

Donde:

$fe_{ij} = frecuencia\ esperada$;

$N = total\ de\ frecuencias\ observadas$;

Al aplicar la fórmula se obtienen los siguientes valores esperados:

Tabla 0-41 Total Frecuencias Esperadas

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**

Fuente: Paguay Mario. 2015

Como $X^2 = \sum_{i=1}^{k} \frac{(o_j - e_j)^2}{e_j}$ por lo tanto:

$$X^2 = \frac{(83-66)^2}{66} + \frac{(66-71)^2}{71} + \frac{(35-47)^2}{47} + \frac{(49-66)^2}{66} + \frac{(76-71)^2}{71} + \frac{(59-47)^2}{47}$$

$$X^2 = 15{,}58.$$

Sea δ: grados de Libertad, f: número de filas y c: número de columnas

δ = (f - 1) (c - 1) = (3 - 1) (2 - 1) = 2

α = 0.05

$X^2_{0.95} = 5.99$ con δ = 2 grados de Libertad y un α = 0.05.

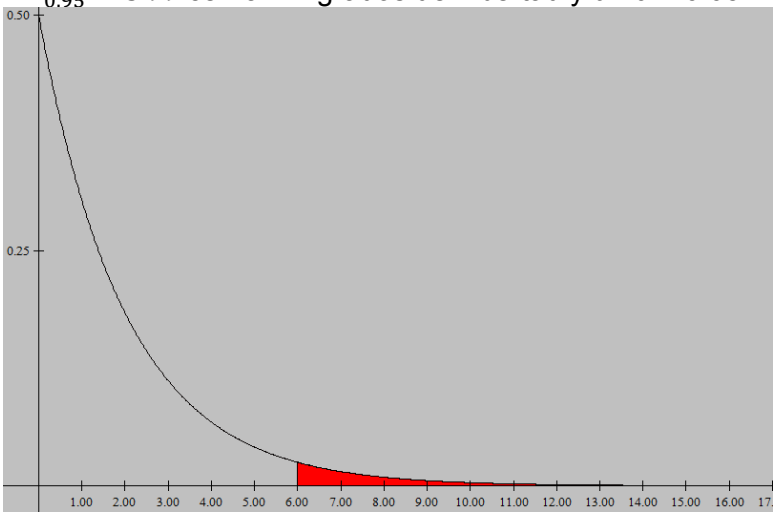


Gráfico 0-25 Chi Cuadrado 1
Fuente: Paguay Mario. 2015

Al contrastar los valores de X^2 se observa en el Gráfico IV-25 que el valor obtenidoes superior al esperado por lo cual se desecha la H_0y 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*.

4.3.2. *RSA vs El Rabin*

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

H: El Algoritmo RSA es Mejor que el Algoritmo El Rabin

De esta hipótesis se abstrae la siguiente afirmación: H_1: Existen diferencias significativas entre los procedimientos, con su correspondiente negación H_0 : ***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 siguiente tabla:

Tabla 0-42 Tabla de Contingencia 3x2 con Frecuencias Observadas

Nivel de Enseñanza en la Criptografía Pública	Algoritmos de Criptografía		Total
	RSA	El Rabin	
Mejor	83	14	97
Indiferente	66	58	124
No Mejor	35	112	147
Totales	184	184	**368**

Fuente: Paguay Mario. 2015

Para obtener las frecuencias esperadas aplicamos la formula anterior:

Tabla 0-43 Total Frecuencias Esperadas

Nivel de Enseñanza en la Criptografía Pública	Algoritmos de Criptografía		Total
	RSA	El Rabin	
Mejor	48,5	48,5	97
Indiferente	62	62	124
No Mejor	73,5	73,5	147
Totales	184	184	**368**

Fuente: Paguay.2015

$$\text{Como } X^2 = \sum_{i=1}^{k} \frac{(o_j - e_j)^2}{e_j} \text{ por lo tanto:}$$

$$X^2 = \frac{(83 - 48{,}5)^2}{48{,}5} + \frac{(66 - 62)^2}{62} + \frac{(35 - 73{,}5)^2}{73{,}5} + \frac{(14 - 48{,}5)^2}{48{,}5} + \frac{(58 - 62)^2}{62} + \frac{(112 - 73{,}5)^2}{73{,}5}$$

$$X^2 = 89{,}86.$$

Sea δ: grados de Libertad, f: número de filas y c: número de columnas

$$\delta = (f - 1)(c - 1) = (3 - 1)(2 - 1) = 2$$

$$\alpha = 0.05$$

$X^2_{0.95} = 5.99$ Chi-cuadrado con δ = 2 grados de Libertad y un α = 0.05.

Al contrastar los valores de X^2 se observa en el Gráfico 25-4 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 El Rabin de 14 por lo que se concluye que *RSA es el mejor algoritmo para la enseñanza en la asignatura de criptografía en la EIS que El Rabin*.

4.3.3. *RSA vs El Gamal*

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

H: El Algoritmo RSA es Mejor que el Algoritmo El Gamal

De esta hipótesis se abstrae la siguiente afirmación: H_1: Existen diferencias significativas entre los procedimientos, con su correspondiente negación H_0: ***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 siguiente tabla:

Tabla 0-44 Tabla de Contingencia 3x2 con Frecuencias Observadas

Nivel de Enseñanza en la Criptografía Pública	**Algoritmos de Criptografía**		**Total**
	RSA	**El Gamal**	
Mejor	83	12	95
Indiferente	66	56	122
No Mejor	35	116	151
Totales	184	184	**368**

Fuente: Paguay Mario. 2015

Para obtener las frecuencias esperadas aplicamos la formula anterior:

Tabla 0-45 Total Frecuencias Esperadas

Nivel de Enseñanza en la Criptografía Pública	**Algoritmos de Criptografía**		**Total**
	RSA	**El Gamal**	
Mejor	47,5	47,5	95
Indiferente	61	61	122
No Mejor	75,5	75,5	151
Totales	184	184	**368**

Fuente: Paguay Mario. 2015

Como $X^2 = \sum_{i=1}^{k} \frac{(o_j - e_j)^2}{e_j}$ por lo tanto:

$$X^2 = \frac{(83 - 47{,}5)^2}{47{,}5} + \frac{(66 - 61)^2}{61} + \frac{(35 - 75{,}5)^2}{75{,}5} + \frac{(12 - 47{,}5)^2}{47{,}5} + \frac{(56 - 62)^2}{62} + \frac{(116 - 73{,}5)^2}{73{,}5}$$

$$X^2 = 97{,}28.$$

Sea δ: grados de Libertad, f: número de filas y c: número de columnas

$$\delta = (f - 1)(c - 1) = (3 - 1)(2 - 1) = 2$$

$$\alpha = 0.05$$

$X^2_{0.95} = 5.99$ Chi-cuadrado con δ = 2 grados de Libertad y un α = 0.05.

Al contrastar los valores de X^2 se observa en el Gráfico 25-4 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 El Gamal de 12 por lo que se concluye que *RSA es el mejor algoritmo para la enseñanza en la asignatura de criptografía en la EIS que El Gamal*.

Tabla 0-46 Resumen de la Comprobación de la Hipótesis

Comprobación	X^2 con α = 0.05 Y δ=2	X^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: Paguay Mario. 2015

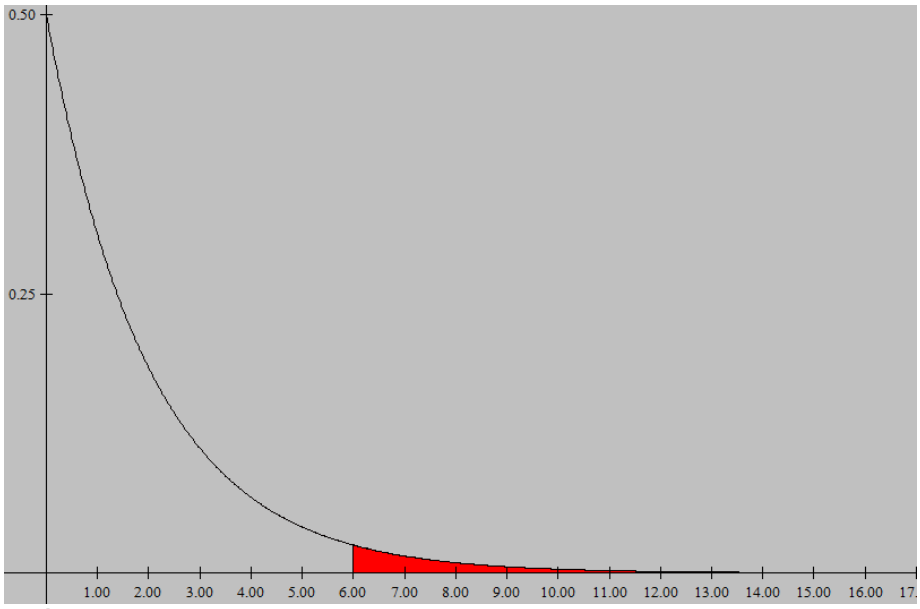


Gráfico 0-26 Chi cuadrado 2
Fuente: Paguay Mario. 2015

En la Tabla anterior así como en la Imagen Gráfico 26-4 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 α =0,05 y δ=2 el $X^2_{0.95} = 5.99$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 contrasto con los demás algoritmos obteniendo con Diffie –

Hellman $X^2_{0.95}$=15,58 , con El Rabin $X^2_{0.95}$=89,86 , con El Gamal $X^2_{0.95}$=97,28 , valores que están alejados del valor referencial $X^2_{0.95} = 5.99$ es el algoritmo con menor número de pasos para cifrar y descifrar la información además posee conceptos matemáticos básicos como la aritmética modular y estructuras algebraicas, 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.

RECOMENDACIONES

- Incluir en el proceso de enseñanza aprendizaje de la asignatura de Criptografía contenidos matemáticos como son Aritmética Modular, Estructuras Algebraicas (Grupos Finitos) el Teorema Chino de Resto, el Problema del Logaritmo Discreto, Curvas Elípticas y, el Algoritmo Extendido de Euclides que son fundamentales para la asimilación correcta de los principios de la criptografía.

- Se recomienda realizar una evaluación de las herramientas informáticas que se emplean para la enseñanza de la cátedra, debido a que los estudiantes no solo deberían conocer como encriptar información sino también como descifrarla por lo que necesitarían recursos computacionales más robustos.

- Se sugiere complementar esta investigación el tratamiento de algoritmos propuestos u otros, con la teoría de Anillos de polinomios donde los números primos son remplazados por polinomios irreducibles además la utilización de la teoría de curvas elípticas (su implementación es igual o más eficiente que la aritmética modular).

- Se recomienda verificar los niveles de complejidad de descifrado de los algoritmos matemáticos empleando recursos computacionales, con la finalidad de exponer la tendencia y tardo de cada ordenador en descifrar estos criptosistemas.

- Se recomienda realizar un estudio del criptoanálisis de los algoritmos criptográficos mediante el uso de software móvil dado que los recursos computacionales son mucho más limitados y requerirá la creación de nuevos algoritmos matemáticos o en su defecto la optimización de los mismos.

BIBLIOGRAFÍA

AGUILERA, N. (18 de Septiembre de 2013). *Centro Científico Tecnológico Santa Fe.* Obtenido de http://www.santafe-conicet.gov.ar/~aguilera/apuntes/euclides.pdf

BACON, H. (11 de Diciembre de 2013). *Horacio Bacon*. Obtenido de https://horaciobacon.wordpress.com/2013/12/11/la-escritura-secreta-parte-ii

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

BOTAYA, J. (2005). *Universitat Oberta de Catalunya* Obtenido de http://openaccess.uoc.edu/webapps/o2/bitstream/10609/674/1/34993tfc.pdf

DELGADO, L., & Vallejo, R. (2009). *Universidad de Nariño.* Obtenido de http://sired.udenar.edu.co/288/1/Curvas%20El%C3%ADpticas%20Construidas%20sobre%20Campos%20Finito%20y%20Criptograf%C3%ADa.pdf

Departamento de Sistemas Informáticos y Computación. (s.f.). *Universitat Politénica 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

GUTIÉRREZ, P. (28 de Diciembre de 2012). *Genbetadev*. Obtenido de http://www.genbetadev.com/seguridad-informatica/que-es-y-como-surge-la-criptografia-un-repaso-por-su-historia

IBÁÑEZ, F. (2012). *Universidad Nacional de Colombia.* Obtenido de http://www.bdigital.unal.edu.co/7238/1/fernandoIbanezrincon.2012.pdf

***Informatixo*.** (22 de febrero de 2011). Obtenido de https://informatix0.wordpress.com/category/sif/

Instituto Nacional de Tecnologías de la Comunicación. (s.f.). *Portal de e-governo, inclusão digital e sociedade do conhecimento*. Obtenido de http://www.egov.ufsc.br/portal/sites/default/files/esteganografia1.pdf

Kioskea. (2014). *Kioskea*. Obtenido de Kioskea: http://es.kioskea.net/contents/129-criptografia

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

MALAVE, N. (Febrero de 2007). *Universidad Politécnica Territorial de PARIA.* Obtenido de http://uptparia.edu.ve/documentos/F%C3%ADsico%20de%20Escala%20Likert.pdf

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

NAVARRO, D., CIARLANTE, J., & SANHUEZA, E. (s.f.). *Universidad de MEndoza.* Obtenido de http://www.um.edu.ar/catedras/claroline/backends/download.php?url=L0RpYXBvcy9DUlNfQ3JpcHRvZ3JhZmlhLnBkZg%3D%3D&cidReset=true&cidReq=2060

PASCALE, M. (25 de Noviembre de 2000). Compilación de Documentos presentados para el VIII Congreso Iberoamericano de Derecho e Informática. Monterrey, México.

SANTAMARÍA, J. (2013). El logaritmo discreto y sus aplicaciones en Criptografía. España.

SANTIANGO, C. (Junio de 2006). *Comisión Interamericana de Telecomunicaciones*. Obtenido de http://www.oas.org/en/citel/infocitel/2006/junio/seguridad_e.asp

SOLANA, P. (2009). *Universidad Carlos III de Madrid.* Obtenido de Universidad Carlos III de Madrid: http://e-archivo.uc3m.es/bitstream/handle/10016/6173/PFC_Patricia_Xifre_Solana.pdf;jsessionid=65F72BDDC438647FEBADDB258D9EE369?sequence=1

VICENT, J. (s.f.). *DSpace Universidad de Alicante.* Obtenido de http://rua.ua.es/dspace/bitstream/10045/4081/1/tesis_doctoral_vicent_frances.pdf

VIOLAT, F. (s.f.). *u-historia*. Obtenido de http://www.u-historia.com/uhistoria/historia/articulos/inienigma/inienigma.htm

ANEXOS

Anexo A

Nombre del Estudiante:	¿Considera usted el algoritmo criptográfico "RSA" comprensible?	¿Considera Usted que la obtención de los datos de entrada es un proceso facil?	¿Defina cuánto ha comprendido del algoritmo de cifrado de "RSA"?	¿Defina cuánto ha comprendido del algoritmo de descifrado de "RSA"?	¿Cuan difícil le resultaría resolver un problema usando "RSA"?	Podría Usted personalizar el algoritmo "RSA"	¿Cuan difícil le resultaría decifrar un mensaje usando "RSA"?	¿Cuánto conoce Usted la Aritmética Modular?	¿Cuánto conoce Usted sobre estrcuturas algebraicas?
Cristian Betancourt	de acuerdo	Indiferente	Comprensión media	Comprensión baja	Complicado	Nada de acuerdo	Complicado	No conoce el tema	Conoce medianamente el tema
Carlos Fernández	Totalmente de acuerdo	de acuerdo	Comprensión alta	Comprensión alta	Complicado	Indiferente	Complicado	No conoce mucho el tema	Conoce el tema
Miriam Rojas	de acuerdo	de acuerdo	Comprensión media	Comprensión media	Complicado	Poco de acuerdo	Complicado	Conoce medianamente el tema	No conoce mucho el tema
Thalía Veloz	de acuerdo	de acuerdo	Comprensión media	Comprensión media	Fácil	De acuerdo	Fácil	No conoce mucho el tema	Conoce el tema
Bolivar Granda	Totalmente de acuerdo	de acuerdo	Comprensión alta	Comprensión alta	Complicado	Poco de acuerdo	Sumamente difícil	No conoce el tema	Conoce medianamente el tema
Mauro Centeno	de acuerdo	de acuerdo	Comprensión alta	Comprensión alta	Fácil	De acuerdo	Fácil	No conoce mucho el tema	No conoce mucho el tema
Cristian Guayanlema	de acuerdo	de acuerdo	Comprensión alta	Comprensión alta	Complicado	Poco de acuerdo	Complicado	Conoce medianamente el tema	Conoce medianamente el tema
Carolina Ruiz	de acuerdo	Poco de acuerdo	Comprensión media	Comprensión media	Fácil	Poco de acuerdo	Fácil	No conoce el tema	Conoce medianamente el tema
Oscar Ramon	de acuerdo	de acuerdo	Comprensión media	Comprensión media	Complicado	Indiferente	Complicado	No conoce mucho el tema	No conoce mucho el tema
Dario Jimenez	Totalmente de acuerdo	Indiferente	Comprensión alta	Comprensión alta	Complicado	De acuerdo	Fácil	No conoce mucho el tema	No conoce mucho el tema
Jose Román	de acuerdo	Poco de acuerdo	Comprensión media	Comprensión media	Complicado	Indiferente	Complicado	No conoce mucho el tema	No conoce mucho el tema
Jorge Chávez	Totalmente de acuerdo	de acuerdo	Comprensión alta	Comprensión alta	Fácil	Indiferente	Fácil	No conoce mucho el tema	Conoce el tema
Valeria Valencia	Poco de acuerdo	de acuerdo	Comprensión media	Comprensión media	Complicado	Poco de acuerdo	Complicado	Conoce el tema	Conoce el tema
Washington López	de acuerdo	de acuerdo	Comprensión media	Comprensión media	Complicado	Poco de acuerdo	Complicado	Conoce el tema	Conoce el tema
Paul Benalcazar	Totalmente de acuerdo	de acuerdo	Comprensión alta	Comprensión alta	Fácil	Nada de acuerdo	Fácil	No conoce mucho el tema	No conoce mucho el tema
Pedro Morillo	de acuerdo	Indiferente	Comprensión media	Comprensión media	Complicado	De acuerdo	Complicado	No conoce mucho el tema	No conoce mucho el tema
Fausto Bautista	de acuerdo	Indiferente	Comprensión media	Comprensión media	Fácil	Poco de acuerdo	Complicado	No conoce mucho el tema	No conoce mucho el tema
Erika Arévalo	de acuerdo	de acuerdo	Comprensión media	Comprensión media	Difícil	Poco de acuerdo	Difícil	Conoce medianamente el tema	Conoce medianamente el tema
flavio chiluiza	de acuerdo	Indiferente	Comprensión media	Comprensión media	Difícil	Indiferente	Complicado	Conoce el tema	No conoce mucho el tema
Silvia Paguay	de acuerdo	de acuerdo	Comprensión alta	Comprensión media	Complicado	Poco de acuerdo	Difícil	No conoce el tema	No conoce mucho el tema
Tania Hidalgo	de acuerdo	de acuerdo	Comprensión media	Comprensión media	Fácil	De acuerdo	Fácil	No conoce mucho el tema	No conoce mucho el tema
Mariana Ponce	de acuerdo	de acuerdo	Comprensión media	Comprensión media	Complicado	De acuerdo	Fácil	No conoce mucho el tema	No conoce mucho el tema
Aracely Caiza	de acuerdo	de acuerdo	Comprensión alta	Comprensión alta	Fácil	De acuerdo	Fácil	Conoce medianamente el tema	Conoce medianamente el tema

Respuestas RSA

Anexo A

Nombre del Estudiante:	¿Considera usted el algoritmo criptográfico "El Rabin" comprensible?	¿Considera Usted que la obtención de los datos de entrada es un proceso facil?	¿Defina cuánto ha comprendido del algoritmo de cifrado de "El Rabin"?	¿Defina cuánto ha comprendido del algoritmo de descifrado de "El Rabin"?	¿Cuan difícil le resultaría resolver un problema usando "El Rabin"?	Podría Usted personalizar el algoritmo "El Rabin"	¿Cuan difícil le resultaría decifrar un mensaje usando "El Rabin"?	¿Cuánto conoce Usted sobre el Teorema Chino del Resto?	¿Cuánto conoce Usted sobre el Algoritmo Extendido de Euclides?
	Indiferente	Indiferente	Comprensión media	Comprensión media	Complicado	Indiferente	Complicado	No conoce el tema	No conoce mucho el tema
Thalía Veloz	Poco de acuerdo	Poco de acuerdo	Comprensión baja	Comprensión baja	Complicado	Poco de acuerdo	Complicado	No conoce el tema	Conoce medianamente el tema
Miriam Rojas	Poco de acuerdo	Poco de acuerdo	Comprensión baja	Comprensión baja	Sumamente difícil	Poco de acuerdo	Sumamente difícil	No conoce el tema	Conoce el tema
Dario Jimenez	Indiferente	Indiferente	No se comprendió	No se comprendió	Sumamente difícil	Nada de acuerdo	Sumamente difícil	No conoce el tema	Conoce el tema
Jorge Chávez	Indiferente	Poco de acuerdo	Comprensión baja	Comprensión baja	Complicado	Indiferente	Complicado	No conoce el tema	No conoce mucho el tema
Valeria Valencia	Indiferente	Indiferente	Comprensión baja	Comprensión baja	Complicado	Indiferente	Complicado	No conoce mucho el tema	No conoce mucho el tema
Oscar Ramon	Indiferente	Indiferente	Comprensión baja	Comprensión baja	Difícil	Poco de acuerdo	Difícil	No conoce el tema	No conoce mucho el tema
Jose Román	Poco de acuerdo	Poco de acuerdo	Comprensión baja	Comprensión baja	Complicado	Indiferente	Complicado	No conoce mucho el tema	No conoce mucho el tema
Bolivar Granda	Indiferente	Poco de acuerdo	Comprensión baja	Comprensión baja	Sumamente difícil	Nada de acuerdo	Complicado	No conoce el tema	No conoce mucho el tema
Mauro Centeno	de acuerdo	de acuerdo	Comprensión media	Comprensión baja	Complicado	Indiferente	Difícil	No conoce el tema	No conoce mucho el tema
flavio chiluiza	de acuerdo	de acuerdo	Comprensión media	Comprensión media	Difícil	De acuerdo	Complicado	Conoce el tema	Conoce el tema
Cristian Betancourt	Nada de acuerdo	Nada de acuerdo	No se comprendió	No se comprendió	Sumamente difícil	Nada de acuerdo	Sumamente difícil	No conoce el tema	No conoce mucho el tema
Fausto Bautista	Poco de acuerdo	Poco de acuerdo	Comprensión baja	Comprensión baja	Complicado	Nada de acuerdo	Sumamente difícil	No conoce el tema	No conoce el tema
Carolina Ruiz	Poco de acuerdo	Poco de acuerdo	Comprensión baja	Comprensión baja	Difícil	Nada de acuerdo	Difícil	No conoce el tema	No conoce el tema
Pedro Morillo	Indiferente	Indiferente	Comprensión baja	Comprensión baja	Difícil	Indiferente	Difícil	No conoce mucho el tema	Conoce el tema
Paul Benalcazar	de acuerdo	de acuerdo	Comprensión media	Carlos Fernández	Complicado	Nada de acuerdo	Complicado	No conoce el tema	Conoce medianamente el tema
Cristian Guayanlema	Poco de acuerdo	Poco de acuerdo	Comprensión baja	Comprensión baja	Difícil	Nada de acuerdo	Difícil	No conoce el tema	No conoce mucho el tema
Tania Hidalgo	Poco de acuerdo	Poco de acuerdo	Comprensión baja	Comprensión baja	Complicado	Poco de acuerdo	Complicado	No conoce el tema	No conoce mucho el tema
Silvia Paguay	Poco de acuerdo	Poco de acuerdo	Comprensión baja	Comprensión baja	Sumamente difícil	Poco de acuerdo	Sumamente difícil	No conoce el tema	No conoce el tema
Mariana Ponce	de acuerdo	Indiferente	Comprensión alta	Comprensión alta	Complicado	De acuerdo	Complicado	No conoce mucho el tema	No conoce mucho el tema
Washington López	Poco de acuerdo	Nada de acuerdo	Comprensión baja	Comprensión media	Complicado	Poco de acuerdo	Difícil	No conoce el tema	No conoce mucho el tema
Erika Arévalo	Poco de acuerdo	Indiferente	Comprensión baja	Comprensión baja	Complicado	Nada de acuerdo	Complicado	No conoce mucho el tema	No conoce mucho el tema
Aracely Caiza	Poco de acuerdo	Poco de acuerdo	Comprensión media	Comprensión media	Complicado	Poco de acuerdo	Complicado	No conoce mucho el tema	No conoce mucho el tema

Respuestas El Rabin

Anexo A

Nombre del Estudiante:	¿Considera usted el algoritmo criptográfico "El Gamal" comprensible?	¿Considera Usted que la obtención de los datos de entrada es un proceso facil?	¿Defina cuánto ha comprendido del algoritmo de cifrado de "El Gamal"?	¿Defina cuánto ha comprendido del algoritmo de descifrado de "El Gamal"?	¿Cuan difícil le resultaría resolver un problema usando "El Gamal"?	Podría Usted personalizar el algoritmo "El Gamal"	¿Cuan difícil le resultaría decifrar un mensaje usando "El Gamal"?	¿Cuánto conoce Usted sobre Curvas Elípticas?	¿Cuánto conoce sobre Grupos Finitos?
Carlos Fernández	Indiferente	Indiferente	Comprensión baja	Comprensión baja	Difícil	Indiferente	Difícil	No conoce el tema	Conoce el tema
Thalía Veloz	Poco de acuerdo	Poco de acuerdo	Comprensión baja	Comprensión baja	Complicado	Poco de acuerdo	Complicado	Conoce medianamente el tema	Conoce medianamente el tema
Miriam Rojas	Poco de acuerdo	Poco de acuerdo	Comprensión baja	Comprensión baja	Difícil	Poco de acuerdo	Difícil	No conoce el tema	No conoce mucho el tema
Valeria Valencia	Indiferente	Indiferente	Comprensión baja	Comprensión baja	Complicado	Indiferente	Complicado	No conoce mucho el tema	No conoce mucho el tema
Dario Jimenez	Indiferente	Indiferente	No se comprendió	No se comprendió	Sumamente difícil	Nada de acuerdo	Sumamente difícil	No conoce el tema	Conoce el tema
Oscar Ramon	Poco de acuerdo	Indiferente	Comprensión baja	Comprensión baja	Difícil	Poco de acuerdo	Difícil	No conoce mucho el tema	No conoce mucho el tema
Jorge Chávez	Indiferente	Poco de acuerdo	Comprensión baja	Comprensión media	Complicado	Indiferente	Complicado	Conoce el tema	Conoce el tema
flavio chiluiza	Indiferente	Indiferente	Comprensión media	Comprensión media	Difícil	Indiferente	Difícil	Conoce medianamente el tema	Conoce medianamente el tema
Jose Román	Poco de acuerdo	Poco de acuerdo	Comprensión baja	Comprensión baja	Complicado	Indiferente	Complicado	Conoce el tema	Conoce el tema
Bolívar Granda	Poco de acuerdo	Poco de acuerdo	Comprensión baja	Comprensión baja	Sumamente difícil	Nada de acuerdo	Difícil	No conoce el tema	No conoce el tema
Mauro Centeno	de acuerdo	de acuerdo	Comprensión media	Comprensión baja	Complicado	Poco de acuerdo	Difícil	No conoce mucho el tema	Conoce el tema
Tania Hidalgo	Poco de acuerdo	Poco de acuerdo	Comprensión baja	Comprensión baja	Complicado	Poco de acuerdo	Complicado	No conoce mucho el tema	No conoce mucho el tema
Fausto Bautista	Poco de acuerdo	Nada de acuerdo	Comprensión baja	Comprensión baja	Complicado	Nada de acuerdo	Difícil	No conoce mucho el tema	No conoce mucho el tema
Carolina Ruiz	Poco de acuerdo	Poco de acuerdo	Comprensión baja	Comprensión baja	Complicado	Poco de acuerdo	Complicado	No conoce mucho el tema	No conoce mucho el tema
Paul Benalcazar	de acuerdo	de acuerdo	Comprensión media	Comprensión media	Complicado	Nada de acuerdo	Complicado	No conoce el tema	No conoce el tema
Pedro Morillo	de acuerdo	Indiferente	Comprensión media	Comprensión media	Complicado	Indiferente	Complicado	Conoce medianamente el tema	Conoce medianamente el tema
Silvia Paguay	Poco de acuerdo	Poco de acuerdo	Comprensión baja	Comprensión baja	Sumamente difícil	Poco de acuerdo	Sumamente difícil	No conoce mucho el tema	No conoce el tema
Mariana Ponce	de acuerdo	de acuerdo	Comprensión media	Comprensión media	Complicado	De acuerdo	Complicado	No conoce mucho el tema	No conoce mucho el tema
Cristian Betancourt	Poco de acuerdo	Poco de acuerdo	Comprensión baja	Comprensión baja	Sumamente difícil	Nada de acuerdo	Sumamente difícil	No conoce el tema	No conoce el tema
Cristian Guayanlema	Indiferente	Poco de acuerdo	Comprensión baja	Comprensión baja	Difícil	Nada de acuerdo	Difícil	No conoce mucho el tema	No conoce mucho el tema
Erika Arévalo	Poco de acuerdo	Poco de acuerdo	Comprensión baja	Comprensión baja	Complicado	Nada de acuerdo	Complicado	Conoce medianamente el tema	Conoce medianamente el tema
Washington López	de acuerdo	Nada de acuerdo	Comprensión media	Comprensión baja	Sumamente difícil	Indiferente	Sumamente difícil	No conoce mucho el tema	Conoce totalmente el tema
Aracely Caiza	Poco de acuerdo	Poco de acuerdo	Comprensión baja	Comprensión media	Difícil	Poco de acuerdo	Difícil	No conoce el tema	No conoce mucho el tema

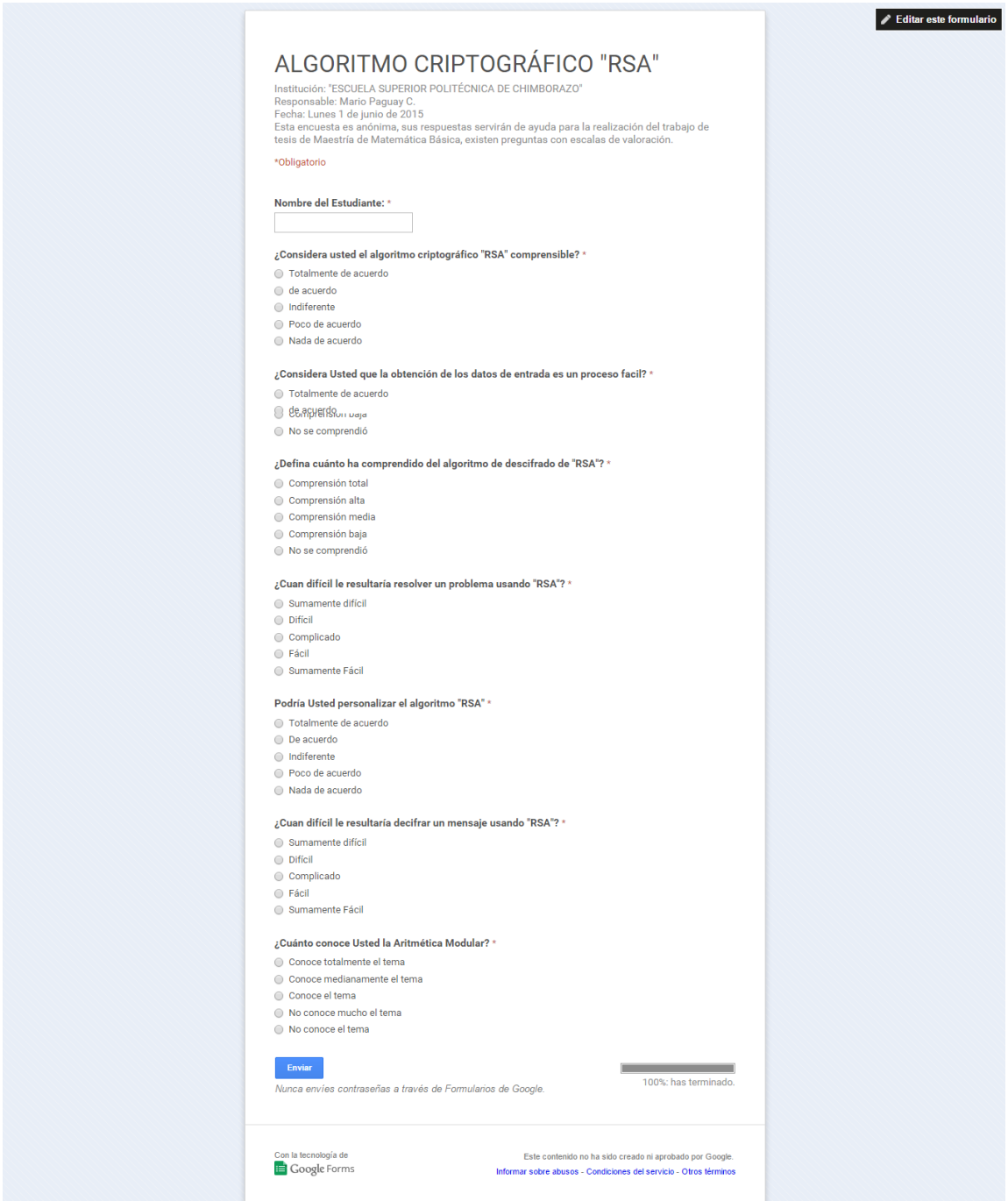
Respuestas El Gamal

Anexo A

Nombre del Estudiante:	¿Considera usted el algoritmo criptográfico "Diffie-Hellman" comprensible?	¿Considera Usted que la obtención de los datos de entrada es un proceso facil?	¿Defina cuánto ha comprendido del algoritmo de cifrado de "Diffie-Hellman"?	¿Defina cuánto ha comprendido del algoritmo de descifrado de "Diffie-Hellman"?	¿Cuan difícil le resultaría resolver un problema usando "Diffie-Hellman"?	Podría Usted personalizar el algoritmo "Diffie-Hellman"	¿Cuan difícil le resultaría decifrar un mensaje usando "Diffie-Hellman"?	¿Cuánto conoce Usted sobre la obtención de Raíces Cuadradas?	¿Cuánto conoce sobre Logaritmos?
Carlos Fernández	de acuerdo	Indiferente	Comprensión media	Comprensión media	Complicado	Indiferente	Complicado	No conoce mucho el tema	Conoce medianamente el tema
Thalía Veloz	de acuerdo	Poco de acuerdo	Comprensión media	Comprensión media	Complicado	De acuerdo	Complicado	No conoce el tema	Conoce medianamente el tema
Miriam Rojas	de acuerdo	de acuerdo	Comprensión media	Comprensión media	Complicado	Poco de acuerdo	Fácil	No conoce mucho el tema	Conoce medianamente el tema
Dario Jimenez	de acuerdo	Totalmente de acuerdo	Comprensión media	Comprensión media	Sumamente difícil	Poco de acuerdo	Complicado	No conoce mucho el tema	Conoce medianamente el tema
Valeria Valencia	Indiferente	Indiferente	Comprensión baja	Comprensión baja	Complicado	Indiferente	Complicado	No conoce mucho el tema	Conoce el tema
Jorge Chávez	Indiferente	Poco de acuerdo	Comprensión media	Comprensión media	Complicado	Indiferente	Complicado	No conoce mucho el tema	Conoce el tema
Oscar Ramon	de acuerdo	Poco de acuerdo	Comprensión baja	Comprensión baja	Complicado	Poco de acuerdo	Complicado	No conoce mucho el tema	Conoce el tema
Bolívar Granda	Poco de acuerdo	Poco de acuerdo	Comprensión media	Comprensión baja	Sumamente difícil	Poco de acuerdo	Sumamente difícil	No conoce mucho el tema	No conoce mucho el tema
Jose Román	Poco de acuerdo	Poco de acuerdo	Comprensión baja	Comprensión baja	Difícil	Indiferente	Complicado	No conoce mucho el tema	Conoce el tema
Mauro Centeno	Indiferente	de acuerdo	Comprensión baja	Comprensión media	Complicado	Poco de acuerdo	Complicado	No conoce mucho el tema	Conoce medianamente el tema
Cristian Betancourt	Indiferente	Poco de acuerdo	Comprensión media	Comprensión baja	Complicado	Poco de acuerdo	Fácil	No conoce el tema	Conoce el tema
Carolina Ruiz	Poco de acuerdo	Poco de acuerdo	Comprensión baja	Comprensión media	Complicado	Poco de acuerdo	Complicado	No conoce mucho el tema	No conoce mucho el tema
Pedro Morillo	Totalmente de acuerdo	de acuerdo	Comprensión alta	Comprensión alta	Fácil	Indiferente	Fácil	No conoce el tema	Conoce medianamente el tema
Fausto Bautista	de acuerdo	Poco de acuerdo	Comprensión media	Comprensión media	Complicado	Nada de acuerdo	Difícil	No conoce el tema	Conoce el tema
Cristian Guayanlema	de acuerdo	de acuerdo	Comprensión alta	Comprensión alta	Fácil	Indiferente	Fácil	No conoce mucho el tema	Conoce el tema
flavio chiluiza	de acuerdo	de acuerdo	Comprensión media	Comprensión media	Difícil	Indiferente	Difícil	Conoce el tema	Conoce el tema
Washington López	Indiferente	Poco de acuerdo	Comprensión media	Comprensión media	Complicado	Poco de acuerdo	Complicado	Conoce el tema	Conoce el tema
Paul Benalcazar	Poco de acuerdo	de acuerdo	Comprensión media	Comprensión media	Complicado	Nada de acuerdo	Complicado	No conoce mucho el tema	Conoce el tema
Tania Hidalgo	de acuerdo	de acuerdo	Comprensión media	Comprensión media	Fácil	De acuerdo	Fácil	No conoce el tema	Conoce medianamente el tema
Erika Arévalo	de acuerdo	de acuerdo	Comprensión alta	Comprensión alta	Complicado	Poco de acuerdo	Complicado	Conoce el tema	Conoce medianamente el tema
Silvia Paguay	de acuerdo	de acuerdo	Comprensión baja	Comprensión media	Complicado	Nada de acuerdo	Complicado	No conoce el tema	No conoce mucho el tema
Mariana Ponce	de acuerdo	de acuerdo	Comprensión alta	Comprensión alta	Complicado	De acuerdo	Complicado	No conoce mucho el tema	No conoce mucho el tema
Aracely Caiza	Poco de acuerdo	Poco de acuerdo	Comprensión media	Comprensión media	Complicado	De acuerdo	Complicado	No conoce mucho el tema	Conoce el tema

Respuestas Diffie - Hellman

Anexo B



Editar este formulario

ALGORITMO CRIPTOGRÁFICO "RSA"

Institución: "ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO"
Responsable: Mario Paguay C.
Fecha: Lunes 1 de junio de 2015
Esta encuesta es anónima, sus respuestas servirán de ayuda para la realización del trabajo de tesis de Maestría de Matemática Básica, existen preguntas con escalas de valoración.

*Obligatorio

Nombre del Estudiante: *

¿Considera usted el algoritmo criptográfico "RSA" comprensible? *
- Totalmente de acuerdo
- de acuerdo
- Indiferente
- Poco de acuerdo
- Nada de acuerdo

¿Considera Usted que la obtención de los datos de entrada es un proceso facil? *
- Totalmente de acuerdo
- de acuerdo
- Comprensión baja
- No se comprendió

¿Defina cuánto ha comprendido del algoritmo de descifrado de "RSA"? *
- Comprensión total
- Comprensión alta
- Comprensión media
- Comprensión baja
- No se comprendió

¿Cuan difícil le resultaría resolver un problema usando "RSA"? *
- Sumamente difícil
- Difícil
- Complicado
- Fácil
- Sumamente Fácil

Podría Usted personalizar el algoritmo "RSA" *
- Totalmente de acuerdo
- De acuerdo
- Indiferente
- Poco de acuerdo
- Nada de acuerdo

¿Cuan difícil le resultaría decifrar un mensaje usando "RSA"? *
- Sumamente difícil
- Difícil
- Complicado
- Fácil
- Sumamente Fácil

¿Cuánto conoce Usted la Aritmética Modular? *
- Conoce totalmente el tema
- Conoce medianamente el tema
- Conoce el tema
- No conoce mucho el tema
- No conoce el tema

Enviar

100%: has terminado.

Nunca envíes contraseñas a través de Formularios de Google.

Con la tecnología de Google Forms

Este contenido no ha sido creado ni aprobado por Google.
Informar sobre abusos - Condiciones del servicio - Otros términos

Anexo C

Editar este formulario

ALGORITMO CRIPTOGRÁFICO "El Rabin"

Institución: "ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO"
Responsable: Mario Paguay C.
Fecha: Lunes 1 de junio de 2015
Esta encuesta es anónima, sus respuestas servirán de ayuda para la realización del trabajo de tesis de Maestría de Matemática Básica, existen preguntas con escalas de valoración.

*Obligatorio

Nombre del Estudiante: *

¿Considera usted el algoritmo criptográfico "El Rabin" comprensible? *
- Totalmente de acuerdo
- de acuerdo
- Indiferente
- Poco de acuerdo
- Nada de acuerdo

¿Considera Usted que la obtención de los datos de entrada es un proceso facil? *
- Totalmente de acuerdo
- de acuerdo
- Indiferente
- Poco de acuerdo
- Nada de acuerdo

¿Defina cuánto ha comprendido del algoritmo de cifrado de "El Rabin"? *
- Comprensión total
- Comprensión alta
- Comprensión media
- Comprensión baja
- No se comprendió

¿Defina cuánto ha comprendido del algoritmo de descifrado de "El Rabin"? *
- Comprensión total
- Comprensión alta
- Comprensión media
- Comprensión baja
- No se comprendió

¿Cuan difícil le resultaría resolver un problema usando "El Rabin"? *
- Sumamente difícil
- Difícil
- Complicado
- Fácil
- Sumamente Fácil

Podría Usted personalizar el algoritmo "El Rabin" *
- Totalmente de acuerdo
- De acuerdo
- Indiferente
- Poco de acuerdo
- Nada de acuerdo

¿Cuan difícil le resultaría decifrar un mensaje usando "El Rabin"? *
- Sumamente difícil
- Difícil
- Complicado
- Fácil
- Sumamente Fácil

¿Cuánto conoce Usted sobre el Teorema Chino del Resto? *
- Conoce totalmente el tema
- Conoce medianamente el tema
- Conoce el tema
- No conoce mucho el tema
- No conoce el tema

¿Cuánto conoce Usted sobre el Algoritmo Extendido de Euclides? *
- Conoce totalmente el tema
- Conoce medianamente el tema
- Conoce el tema
- No conoce mucho el tema
- No conoce el tema

Enviar

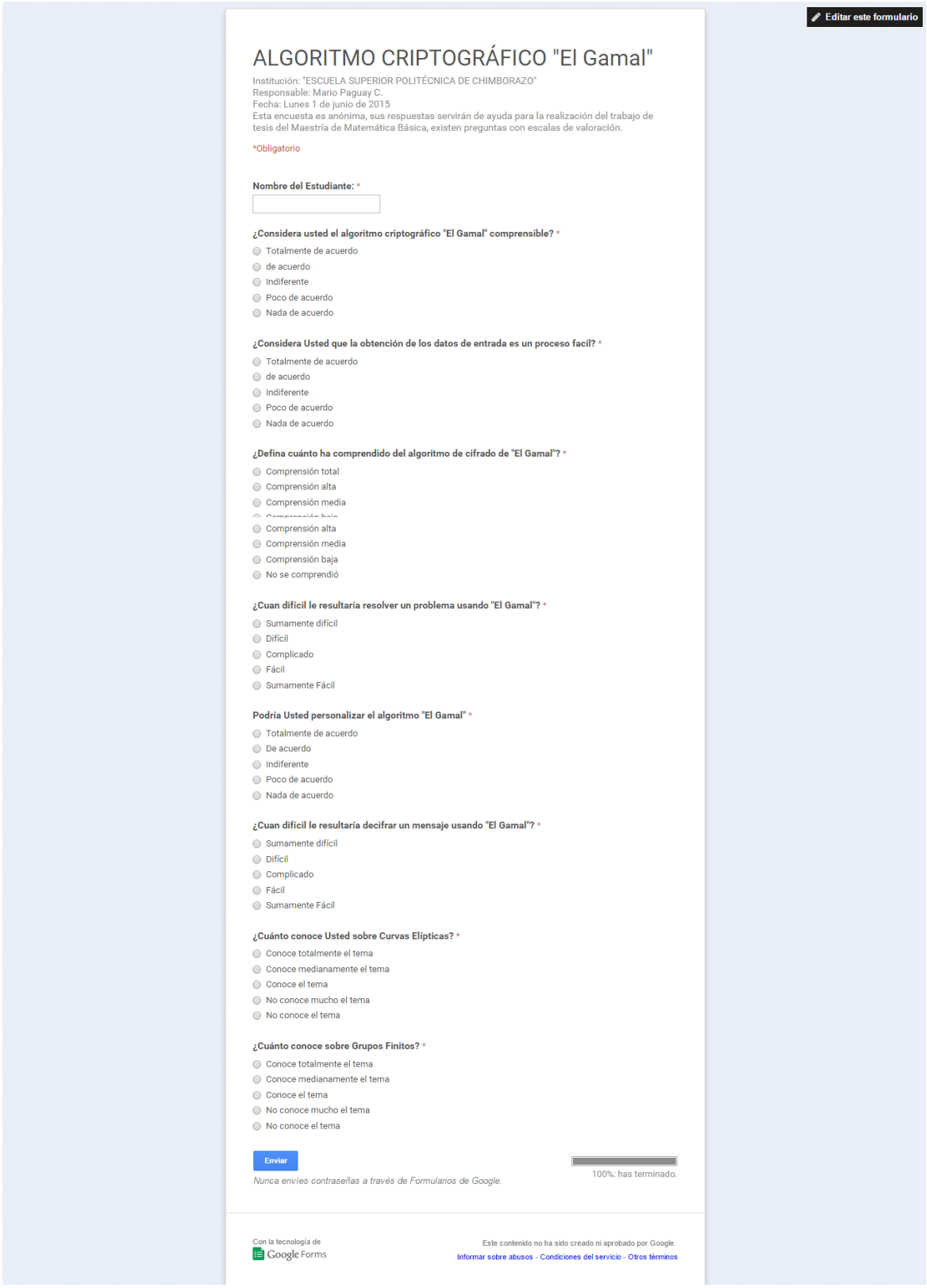
100%: has terminado.

Nunca envíes contraseñas a través de Formularios de Google.

Con la tecnología de Google Forms

Este contenido no ha sido creado ni aprobado por Google.
Informar sobre abusos - Condiciones del servicio - Otros términos

Anexo D



Editar este formulario

ALGORITMO CRIPTOGRÁFICO "El Gamal"

Institución: "ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO"
Responsable: Mario Paguay C.
Fecha: Lunes 1 de junio de 2015
Esta encuesta es anónima, sus respuestas servirán de ayuda para la realización del trabajo de tesis del Maestría de Matemática Básica, existen preguntas con escalas de valoración.

*Obligatorio

Nombre del Estudiante: *

¿Considera usted el algoritmo criptográfico "El Gamal" comprensible? *
- Totalmente de acuerdo
- de acuerdo
- Indiferente
- Poco de acuerdo
- Nada de acuerdo

¿Considera Usted que la obtención de los datos de entrada es un proceso facil? *
- Totalmente de acuerdo
- de acuerdo
- Indiferente
- Poco de acuerdo
- Nada de acuerdo

¿Defina cuánto ha comprendido del algoritmo de cifrado de "El Gamal"? *
- Comprensión total
- Comprensión alta
- Comprensión media
- Comprensión alta
- Comprensión media
- Comprensión baja
- No se comprendió

¿Cuan difícil le resultaría resolver un problema usando "El Gamal"? *
- Sumamente difícil
- Difícil
- Complicado
- Fácil
- Sumamente Fácil

Podría Usted personalizar el algoritmo "El Gamal" *
- Totalmente de acuerdo
- De acuerdo
- Indiferente
- Poco de acuerdo
- Nada de acuerdo

¿Cuan difícil le resultaría decifrar un mensaje usando "El Gamal"? *
- Sumamente difícil
- Difícil
- Complicado
- Fácil
- Sumamente Fácil

¿Cuánto conoce Usted sobre Curvas Elípticas? *
- Conoce totalmente el tema
- Conoce medianamente el tema
- Conoce el tema
- No conoce mucho el tema
- No conoce el tema

¿Cuánto conoce sobre Grupos Finitos? *
- Conoce totalmente el tema
- Conoce medianamente el tema
- Conoce el tema
- No conoce mucho el tema
- No conoce el tema

Enviar

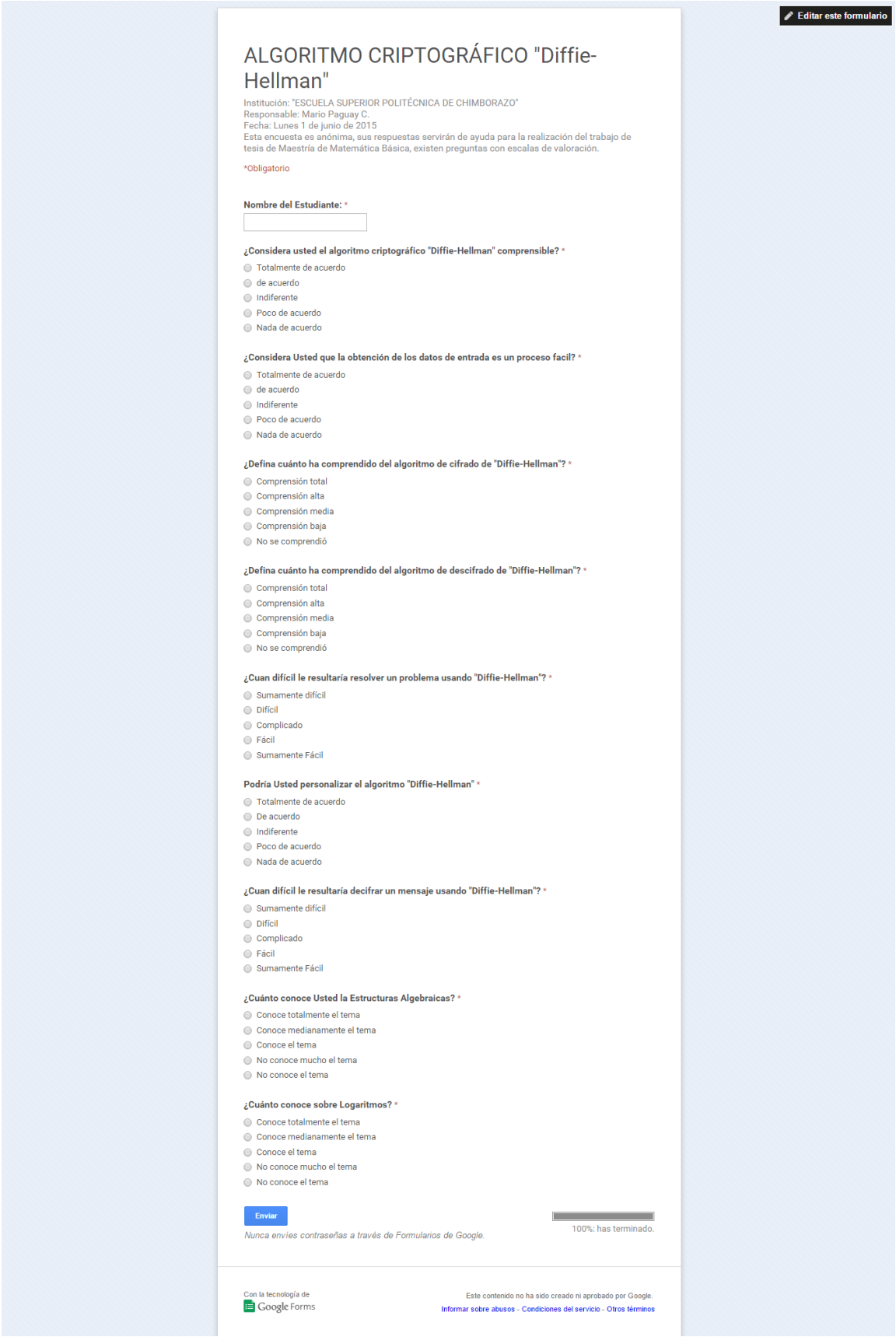
100%: has terminado.

Nunca envíes contraseñas a través de Formularios de Google.

Con la tecnología de Google Forms

Este contenido no ha sido creado ni aprobado por Google.
Informar sobre abusos - Condiciones del servicio - Otros términos

Anexo E



Editar este formulario

ALGORITMO CRIPTOGRÁFICO "Diffie-Hellman"

Institución: "ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO"
Responsable: Mario Paguay C.
Fecha: Lunes 1 de junio de 2015
Esta encuesta es anónima, sus respuestas servirán de ayuda para la realización del trabajo de tesis de Maestría de Matemática Básica, existen preguntas con escalas de valoración.

*Obligatorio

Nombre del Estudiante: *

¿Considera usted el algoritmo criptográfico "Diffie-Hellman" comprensible? *
- Totalmente de acuerdo
- de acuerdo
- Indiferente
- Poco de acuerdo
- Nada de acuerdo

¿Considera Usted que la obtención de los datos de entrada es un proceso facil? *
- Totalmente de acuerdo
- de acuerdo
- Indiferente
- Poco de acuerdo
- Nada de acuerdo

¿Defina cuánto ha comprendido del algoritmo de cifrado de "Diffie-Hellman"? *
- Comprensión total
- Comprensión alta
- Comprensión media
- Comprensión baja
- No se comprendió

¿Defina cuánto ha comprendido del algoritmo de descifrado de "Diffie-Hellman"? *
- Comprensión total
- Comprensión alta
- Comprensión media
- Comprensión baja
- No se comprendió

¿Cuan difícil le resultaría resolver un problema usando "Diffie-Hellman"? *
- Sumamente difícil
- Difícil
- Complicado
- Fácil
- Sumamente Fácil

Podría Usted personalizar el algoritmo "Diffie-Hellman" *
- Totalmente de acuerdo
- De acuerdo
- Indiferente
- Poco de acuerdo
- Nada de acuerdo

¿Cuan difícil le resultaría decifrar un mensaje usando "Diffie-Hellman"? *
- Sumamente difícil
- Difícil
- Complicado
- Fácil
- Sumamente Fácil

¿Cuánto conoce Usted la Estructuras Algebraicas? *
- Conoce totalmente el tema
- Conoce medianamente el tema
- Conoce el tema
- No conoce mucho el tema
- No conoce el tema

¿Cuánto conoce sobre Logaritmos? *
- Conoce totalmente el tema
- Conoce medianamente el tema
- Conoce el tema
- No conoce mucho el tema
- No conoce el tema

Enviar

100%: has terminado.

Nunca envíes contraseñas a través de Formularios de Google.

Con la tecnología de Google Forms

Este contenido no ha sido creado ni aprobado por Google.
Informar sobre abusos - Condiciones del servicio - Otros términos