INSTITUTO POLITÉCNICO NACIONAL

ESCUELA SUPERIOR DE CÓMPUTO

CRYPTOGRAPHY

Alumnos: Caballero Huesca Carlos Eduardo

Martínez García Brando Josué

Grupo: 3CV1

Profesora: Díaz Santiago Sandra

Modos de operación: Laboratorio 5

Fecha: 17 de octubre del 2016

Anote los datos biográficos más importantes sobre Evariste Galois.

Bourg-la-Reine, Francia, 1811 - París, 1832

Fue sin duda de Lagrange de quién aprendió por vez primera la teoría de ecuaciones, teoría a la que él mismo habría de realizar contribuciones fundamentales a lo largo de los cuatro años siguientes.

A sus 17 años estaba atacando uno de los más difíciles problemas de las matemáticas; un problema que había mantenido en jaque a los matemáticos durante más de un siglo. Lo que Galois consiguió fue dar criterios definitivos para determinar si las soluciones de una ecuación polinómica podrán o no calcularse por radicales.

En el duelo en el que Galois perdió la vida, el adversario era como él, un ardiente republicano. Más aún, al parecer, era uno de los 19 oficiales de la Guardia de Artillería cuya absolución fue ocasión del desafiante brindis que Galois ofreció al rey. El duelo fue entre amigos y se desarrolló como una especie de ruleta rusa; estando cargada solamente una de las pistolas. Muchos fragmentos de manuscritos muestran que Galois prosiguió con sus investigaciones matemáicas no sólo durante su encarcelamiento, sino hasta la hora de su muerte. [1]

Con sólo dieciséis años, interesado en hallar las condiciones necesarias para definir si una ecuación algebraica era susceptible de ser resuelta por el método de los radicales, empezó a esbozar lo que más adelante se conocería con el nombre genérico de «teoría de Galois», analizando todas las permutaciones posibles de las raíces de una ecuación que cumplieran unas condiciones determinadas. [2]

Escriban en sus propias palabras un resumen sobre la historia de Rijndael y AES.

AES (Advanced Encryption Standard).

La NIST convocó a una propuesta sobre un nuevo sistema de para cifrar y ser utilizado como un estándar en la cual se presentaron 15 propuestas, entre las cuales de presentó una llamada Rijndael, la cual fue propuesta por Joan Daemen y Vincent Dijmen. Logró llegar a ser una de las 5 que se tomaron en cuenta, juntamente con MARS de IBM, RC6TM de los laboratorios RSA, entre otras. Después de muchas pruebas y reuniones entre ellos, se adopta Rijndael como el nuevo estándar que se va a utilizar. Posteriormente se comenzó a utilizar, publicando especificaciones y documentación sobre este nuevo estándar. [3]

Rijndael

Este sistema opera con bytes, utiliza los campos finitos GF(28), se maneja por operaciones de bloques y dependiendo del tamaño de la llave se hace el número de rondas.

Bibliografía

[1]Ugr.es. (2016). Evariste Galois. [online] Disponible en: http://www.ugr.es/~eaznar/galois.htm

[2] Biografiasyvidas.com. (2016). Biografia de Évariste Galois. [online] Disponible en: http://www.biografiasyvidas.com/biografia/g/galois.htm

[3] Anon, (2016). [online] Disponible en: http://users.dsic.upv.es/asignaturas/eui/cri/des.pdf