EL USO DE CAMPOS DE GALOIS EN LA CIBERSEGURIDAD

AUTOR

DOBLE GRADO EN INGENIERÍA INFORMÁTICA Y MATEMÁTICAS.
FACULTAD DE MATEMÁTICAS.
UNIVERSIDAD COMPLUTENSE DE MADRID

Trabajo Libre Ecuaciones Algebraicas

Octubre 2024

Participante:

Diego Martínez López

Índice general

0. Introducción

0.1. Objetivos del trabajo y relación de la ciberseguridad con la asignatura.

El objetivo de este trabajo libre es realizar un breve estudio sobre algún tema en concreto que hayamos visto en alguna asignatura o que conozcamos, y que esté directamente relacionado con la asignatura de ecuaciones algebraicas. En este caso, hablaremos de la relación de la ciberseguridad con la asignatura, en particular del uso de campos de Galois en la encriptación AES, un tipo de encriptación que se utiliza ampliamente para proteger datos confidenciales y se considera uno de los algoritmos de cifrado simétrico más seguros.

1. Los campos de galois

1.1. Qué son los campos de Galois

Un cuerpo finito o campo de Galois K es un cuerpo con un número finito de elementos, en particular un cuerpo cuyo cardinal es siempre una potencia de un número primo p. Cabe destacar que $\mathrm{Char}(K) = p$.

Así, para todo número primo p y todo entero positivo no nulo n,existe un cuerpo de cardinal p^n, que se presenta como la única extensión $E \mid \mathbb{Z}/p\mathbb{Z}$ tal que $[E : \mathbb{Z}/p\mathbb{Z}]$=n. Además, el cuerpo finito de cardinal $q = p^n$ se denota $GF(q)$.

1.2. Construcción de los campos de Galois.

Sea p un número primo, tomamos el cuerpo $\mathbb{Z}/p\mathbb{Z} = \mathbb{GF}(p)$. Sea $f(x) \in \mathbb{GF}(p)[x]$ un polinomio irreducible de grado n, tomamos

$$\mathbb{GF}(p)[x]/(f(x)) = \{a + (f) : a \in \mathbb{GF}(p)[x]\}.$$

Como $\mathbb{GF}(p)[x]$ es un DIP y, en particular, un DE, dado $a(x) \in \mathbb{GF}(p)[x]$, dividiendo por $f(x)$ tenemos (por el teorema de la división) que un representante de $a(x) + (f(x))$ es de la forma:

$$a_0 + a_1x + \cdots + a_{n-1}x^{n-1}, \quad a_i \in \mathbb{GF}(p)[x]$$

Por tanto, podemos ver $\mathbb{GF}(p)[x]/(f(x))$ como el conjunto:

$$F = \{a_0 + a_1x + \cdots + a_{n-1}x^{n-1} \mid a_i \in \mathbb{GF}(p)[x]\}$$

Ahora bien, $(F, +, \cdot)$ es un cuerpo con las operaciones de suma y producto en el anillo cociente, el cual tiene cardinal p^n y que identificamos con el cuerpo $\mathbb{GF}(p^n)$.
Observamos que $\mathbb{GF}(p^n) \setminus \{0\}$ es un grupo cíclico de orden $p^n - 1$ y que, si $\alpha \in \mathbb{GF}(p^n)$ con $\alpha = x + (f)$, entonces α es una raíz de $f(x)$.

Observemos que $\mathbb{GF}(p^n)|\mathbb{Z}/p\mathbb{Z}$ es una extensión de cuerpos, y como ya sabemos, el grado de la extensión $[\mathbb{GF}(p^n) : \mathbb{Z}/p\mathbb{Z}]$ coincide con el grado del polinomio irreducible f, es decir, en este caso el grado de esta extensión es n. Por tanto, $\mathbb{GF}(p^n)$ es un $\mathbb{Z}/p\mathbb{Z}$-espacio vectorial de dimensión n y una base suya es:

$$\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$$

Por último, es importante recordar que $\mathbb{GF}(p^n)$ es único salvo isomorfismo.

1.3 Un ejemplo relevante de campo finito.

Cabe destacar un campo finito importante que utilizará la encriptación que explicaremos a continuación, que es el cuerpo $\mathbb{GF}(2^8)$, que tal y como hemos visto se construye tomando un polinomio irreducible de grado 8 con coeficientes en el cuerpo $\mathbb{GF}$(p)[x] y tomando el anillo cociente $\mathbb{GF}$(p)[x]/(f(x)).

2. La encriptación AES

2.1 Explicación de la encriptación AES

La encriptación AES, o Estándar de Cifrado Avanzado, es un método de cifrado que transforma los datos para proteger la privacidad al enviarlos de un emisor a un receptor. AES opera sobre bloques de datos de 128 bits, es decir, paquetes de 16 bytes, los cuales se organizan en una matriz de 4x4, llamada matriz estado. Cada celda de esta matriz contiene uno de los bytes de los datos a cifrar. Para realizar el cifrado, se usa también una clave, que es una cadena de bits necesaria tanto para cifrar como para descifrar la información.

AES aplica una serie de operaciones matemáticas, como sustituciones, permutaciones y transformaciones, para convertir el texto sin formato en texto cifrado. Estas operaciones involucran los Campos de Galois, especialmente en las fases de sustitución y de transformación, con el fin de mejorar la seguridad.

Uno de los pasos fundamentales es la transformación SubBytes, que reemplaza cada byte de la matriz estado con un byte específico de una tabla llamada S-box. Esta S-box se genera combinando transformaciones afines y propiedades de los Campos de Galois, específicamente el campo $\mathbb{GF}(2^8)$. Al operar en este campo, se asegura que la sustitución sea no lineal y ofrezca una mayor difusión de la información a lo largo del cifrado.

La SubBytes se basa en dos operaciones esenciales: la inversa multiplicativa y la transformación afín. La inversa multiplicativa encuentra el inverso de cada byte en el campo $\mathbb{GF}(2^8)$ y es fundamental para permitir que el cifrado AES pueda revertirse en el proceso de descifrado.

La transformación afín, en cambio, es una operación lineal que aplica una multiplicación de matrices seguida de una XOR bit a bit a cada byte de entrada, introduciendo no linealidad y mejorando la difusión. La matriz de la transformación afín también se crea con elementos de $\mathbb{GF}(2^8)$, lo cual aumenta la complejidad del cifrado y distribuye la influencia de cada byte de entrada.

Además de SubBytes, los Campos de Galois se emplean en la transformación MixColumns. Esta transformación se aplica a cada columna de la matriz estado y consiste en multiplicarla por una matriz fija usando operaciones en el campo $\mathbb{GF}(2^8)$ y un polinomio irreducible específico. El objetivo de MixColumns es esparcir los cambios en un byte a múltiples bytes de la columna, asegurando que las alteraciones se propaguen en las rondas siguientes.

Estos pasos se repiten múltiples veces en el cifrado hasta que el mensaje está completa-

mente transformado, envíandose al destinatario que invierte cada uno de los pasos realizados en el cifrado para recuperar el mensaje original.

2.2 Uso de campos de Galois en la encriptación AES (S-Box)

Como hemos visto en la explicación de cómo funciona la encriptación AES, hay varios pasos fundamentales en los que usamos la estructura de campos finitos. En este apartado, nos enfocamos en la construcción de la tabla de sustitución S-Box utilizando los campos de Galois.

La información se almacena en paquetes de bytes, que son secuencias de ceros y unos. Un byte (8 bits) puede representarse en el espacio vectorial $\mathbb{GF}(2^8)$. Este sistema de encriptación obtiene el grupo finito de 2^8 elementos mediante el anillo cociente $\mathbb{GF}(2^8) = \mathbb{GF}(2)[x]/(f(x))$, donde:

$$f(x) = x^8 + x^4 + x^3 + x + 1, \quad f \in \mathbb{GF}(2)[x] \text{ es irreducible.}$$

Así, los bytes, como están formados por 8 bits, se representan como polinomios en una indeterminada x con coeficientes en $\mathbb{Z}/2\mathbb{Z}$, y de grado a lo sumo 7. Las operaciones de AES usan la aritmética de polinomios en este cuerpo finito. El grupo multiplicativo $\mathbb{GF}(2^8) \setminus \{0\}$ es cíclico de orden 255, lo cual permite representar cualquier elemento no nulo como una potencia de un generador, propiedad crucial para las transformaciones en AES.

En AES, la encriptación se representa mediante tablas llamadas estados compuestas por bytes. Usando el campo finito, el estado de N bytes puede representarse en el espacio vectorial $(\mathbb{GF}(2^8))^{4N}$, correspondiente a matrices de tamaño $4\times N$ con coeficientes en $\mathbb{GF}(2^8)$. Una forma algebraica de representar un estado es a través del anillo $\mathbb{GF}(2^8)[x,y]/\langle x^4-1, y^N-1\rangle$, donde $x^4 = 1$ (representando 4 filas) y $y^N = 1$ (representando N columnas, con $N = 4, 6$, u 8 según la variante AES usada).

Para la S-Box, aprovechamos que $\mathbb{GF}(2^8)$ es un campo, por lo que todo elemento distinto de cero tiene inverso multiplicativo. Definimos la función:

$$\varphi : \mathbb{GF}(2^8) \longrightarrow \mathbb{GF}(2^8), \quad \varphi(\gamma) = \gamma^{-1}, \quad \varphi(0) = 0$$

donde φ toma un elemento y devuelve su inverso en el campo, formando una permutación en $\mathbb{GF}(2^8)$ que puede expresarse como $\varphi(x) = x^{254}$. Esta operación introduce no linealidad en el cifrado, lo cual es esencial para resistir ataques como el criptoanálisis diferencial.

Posteriormente, la S-Box aplica una transformación mediante las funciones:

$$L, \psi : \mathbb{GF}(2^8) \longrightarrow \mathbb{GF}(2^8), \quad L(\alpha) = c_0\alpha, \quad \psi(\beta) = d_0 + \beta$$

donde c_0 y d_0 son elementos fijos del campo. Componiendo estas funciones, obtenemos la S-Box:

$$S = \psi \circ L \circ \varphi$$

3. Conclusión

El uso de campos de Galois en AES es clave para asegurar las operaciones no lineales y complejas que protegen contra ataques criptográficos. Este enfoque dota al cifrado de la robustez necesaria para proteger datos bancarios y otros tipos de información sensible en un mundo digital. Así, vemos cómo las matemáticas y las estructuras algebraicas juegan un papel fundamental en la seguridad de nuestros datos.

4. Bibliografía

- Miscelánea Matemática. (2021). *Artículos de matemática*. Disponible en: https://miscelaneamatematica.org/download/tbl_articulos.pdf2.b83a7656c55ef738.353330362e706466.pdf.
- Gutiérrez, J. *Teoría de Galois para cuerpos finitos*. Disponible en: http://www.math.huji.ac.il/~jgutierrez/GaloisFinitos.pdf.
- Wikipedia. (2023). *Cuerpo finito*. Disponible en: https://es.wikipedia.org/wiki/Cuerpo_finito.
- Last, I. (2016). *Campos de Galois*. Blog. Disponible en: https://iagolast.github.io/blog/2016/11/06/campos-galois.html.
- Universidad de Santiago de Compostela. *Apuntes sobre teoría de Galois*. Disponible en: https://www.usc.es/regaca/apuntes/Galois.pdf.