

UNIVERSIDAD DE CIENFUEGOS

“Carlos Rafael Rodríguez”



UNIVERSIDAD
CIENFUEGOS
Carlos Rafael Rodríguez

Facultad de Ingeniería

Departamento de Matemática Aplicada

**Título: SUCESIONES RECURRENTES LINEALES SOBRE CAMPOS
FINITOS BINARIOS
Y SU APLICACIÓN EN LA CRIPTOGRAFÍA**

Autores: Lic. Mayara Rosa Mier Macías

MSc. Oristela Cuellar Justiz

Esp. Evaristo José Madarro Capó

2014



“Todo hombre tiene el deber de cultivar su inteligencia con respecto a sí propio y al mundo”.

José Martí

Agradecimientos

Este trabajo es una mezcla de esfuerzo y dedicación de un grupo de personas que, de una forma u otra, a lo largo de mi etapa estudiantil me han dado apoyo incondicional y sin límites, sin su ayuda esto hubiese sido imposible. Es por ello que quiero agradecer eternamente a:

- ✓ **A los 55 Años de Revolución.**
- ✓ **A mis padres:** Rosa Amelia Macías Haro y Rogelio P. Mier Font.
- ✓ **A mi hermano:** Rogelio P. Mier Macías.
- ✓ **A mi novio:** Yasiel Hernández Ruiz.

Agradecimientos

✓ **A mis suegros:** Graciela Ruiz León y Juan J. Hernández García.

✓ **A mis tutores:** Evaristo José Madarro Capó y Oristela Cuellar Justiz.

✓ **A toda mi familia .**

✓ **A todas mis amistades y compañeros especialmente a:** Laima Imbert, Yaineris Ferrán, Diana Prieto, Beatriz Pérez, Osaida, Estelio Navarro, Ariailis Carrera, Yadira Zamora, Yiset Padrón, Elizabeth Chávez, Osleri Becerra, Ernet Quintana, José M. Moya, Frank E. Álvarez.

Agradecimientos

✓ **A todos lo que eternamente han sido y serán mis profesores especialmente a:** Gerardo Hernández, Tamara, Lucía Arguelles, Eberto R. Morgado, Guillermo Sosa, Juan M. Navarro, Uvedel del Pino, Caridad Aguiar, Caridad Cuellar, Agustín Macias, Antonio Rodríguez, Fátima, a la memoria de Mercedes Rodríguez.

✓ **A los que me creyeron capaz de llegar hasta aquí y me ayudaron a que este sueño se haya hecho realidad:** ElsaNúñez.

A TODOS

¡Muchas Gracias!

Dedicatoria

Por su entrega, apoyo, esmero, esfuerzo, interés y dedicación absoluta, le dedico este trabajo de diploma a mis padres. A este par se le suma mi querido hermano por ser mi fuerza de inspiración y mi guía en todo momento. También quisiera dedicárselo a mi novio y a mis suegros, que han sido muy importantes en esta etapa de mi vida.

RESUMEN

En el presente trabajo se expone y analiza una de las herramientas más utilizadas para la construcción de criptosistemas de cifrado en flujo, los registros de desplazamiento con retroalimentación lineal (LSFRs, siglas en inglés), los cuales están basados en el principio matemático de las sucesiones recurrentes lineales (SRL) sobre los campos finitos binarios. Se brinda la fundamentación teórica de estos mecanismos presentando las definiciones y propiedades principales, que son necesarias para comprender su funcionamiento. Además, se detallan métodos teóricos y prácticos para la obtención de los parámetros de los LSFRs.

Palabras Claves: campo finito binario, sucesión recurrente lineal, registro de desplazamiento con retroalimentación lineal, cifrado de flujo.

Abstract

ABSTRACT

In this paper , one of the most used tools for building cryptosystems stream ciphers is presented and analyzed: the shift registers with linear feedback (LSFRs, English acronym), which are based on the mathematical concept of linear recurrent sequences. (LRS) over binary finite fields. The theoretical fundamentals of presenting these definitions and main properties, which are necessary to understand its functional mechanisms are offered. In addition, theoretical and practical methods to obtain the parameters of the LSFRs. are detailed .

Abstract

Tabla de Contenido

Contenido

INTRODUCCIÓN	1
CAPÍTULO I. SUCESIONES RECURRENTE LINEALES SOBRE	7
CAMPOS FINITOS BINARIOS.....	7
1.1 Conceptos básicos	8
1.1.1 Campos finitos	8
1.1.2 Polinomios.....	9
1.1.3 Caracterización de los campos finitos	11
1.2 Sucesiones recurrentes lineales sobre un campo finito.....	19
1.2.1 Definición de sucesión recurrente lineal	19
1.2.3 Métodos básicos de representación de las SRL	21
1.2.2 Período de una sucesión recurrente lineal.	23
1.2.4 Sucesiones Recurrentes Lineales Binarias.....	27
CAPÍTULO II. REGISTROS DE DESPLAZAMIENTO CON.....	29
RETROALIMENTACIÓN LINEAL.....	29
2.1 Registros de desplazamiento con retroalimentación lineal	29
2.3 Relación entre los LFSR y las sucesiones recurrentes lineales	34
2.4 Propiedades de pseudo	39
aleatoriedad en las sucesiones de los LFSRs.....	39
2.5 Complejidad lineal y LFSR.....	43
CAPÍTULO III. ANÁLISIS CRIPTOGRÁFICO DE LOS LFSR.....	48
3.1 Cifrado en flujo.....	48
3.2 Ataques de texto claro conocido	49
3.3 Obtención del polinomio primitivo de los LFSRs	51

Tabla de Contenido

3.4 Procedimientos para la recuperación del estado inicial de los LFSR	54
CONCLUSIONES	61
Recomendaciones	62
Bibliografía	63
ANEXOS	65

INTRODUCCIÓN

La teoría de los campos finitos es una rama del Álgebra moderna que se ha convertido en muy actual desde la última mitad del siglo pasado, teniendo sus múltiples aplicaciones en la combinatoria, la teoría de códigos, la teoría matemática de los esquemas de conmutación, la teoría de números, la geometría algebraica, la teoría de Galois y en particular en Criptografía, donde se utilizan en la construcción de la mayoría de los códigos conocidos y su decodificación (Niederreiter, 1986).

Las sucesiones sobre campos finitos cuyos términos dependerán de una manera sencilla de sus predecesores son de importancia para una variedad de aplicaciones ejemplo en la criptografía. Dichas sucesiones son fáciles de generar mediante procedimientos recursivos, lo cual es sin duda una característica ventajosa desde el punto de vista computacional y también tienden a tener propiedades estructurales útiles (Menezes, VanOorschot, & Vanstone, 1996).

En 1917, J. Mauborgne y G. Vernam inventaron un criptosistema perfecto según el criterio de Shannon. Dicho sistema consistía en emplear una sucesión aleatoria de igual longitud que el mensaje, que se usaría una única vez, combinándola mediante alguna función simple e inversible (xor) con el texto en claro bit a bit.

En este trabajo analizaremos una herramienta para la construcción de este tipo de criptosistema, denominado en la criptografía moderna como algoritmo de cifrado en flujo, sobre campos finitos específicos: los binarios, o sea, los campos finitos de característica dos. Dichos criptosistemas no son más que la especificación de un generador pseudoaleatorio, que permiten cifrar mensajes de longitud arbitraria, combinando el mensaje con la sucesión (conjunto de elementos encadenados o sucesivos) mediante la operación or exclusivo bit a bit. Los mismos no proporcionan seguridad perfecta, ya que mientras en el cifrado de Vernam el número de posibles claves es tan grande como el de posibles mensajes, cuando empleamos un generador tenemos, como mucho, tantas sucesiones distintas como posibles valores del estado inicial del registro. Una herramienta a emplear para la construcción de estos

Introducción

criptosistemas la constituye los registros de desplazamiento con retroalimentación lineal (LSFR, estos son un tipo especial de circuitos electrónicos de conmutación que procesan la información presentada de una manera adecuada en forma de elementos del campo), los cuales están basados en el principio matemático de las sucesiones recurrentes lineales (SRL, ecuación que define una sucesión recursiva donde cada término de la sucesión es definido como una función de términos anteriores).

Debido a que permiten generar sucesiones con períodos muy grandes y con buenas propiedades estadísticas, además de su bien conocida estructura algebraica y su facilidad para ser implementados por hardware, estos se encuentran presentes en muchos de los generadores de sucesión propuestos en la literatura.

En marzo del 2009 se inauguró en nuestra Universidad Central “Martha Abreu” de Las Villas un Laboratorio de Criptografía Académica (LCA), ubicado en la facultad de Matemática, Física y Computación. Con el objetivo de potenciar investigaciones, en el centro del país, relacionadas con el análisis y diseño de algoritmos de cifrado en flujo.

Actualmente existe una gran variedad de principios de diseño para construir algoritmos de cifrado en flujo, pero uno de los más utilizados desde hace décadas son los registros de desplazamiento con retroalimentación lineal. Hoy por hoy, se reportan algunas deficiencias de seguridad, lo cual ha limitado su utilización y han impuesto transformaciones en su estructura y funcionamiento. No obstante, muchos de estos reportes no presentan información en detalle e incluso en algunos se especula acerca de los resultados planteados.

Problema científico:

Debido a lo anterior se hace necesario realizar un estudio sobre la base matemática de este principio de diseño, específicamente de las sucesiones recurrentes lineales sobre campos finitos binarios. De manera que facilite el análisis criptográfico de estos mecanismos y de esta forma explorar y determinar las potencialidades reales de utilización de los registros de desplazamiento con retroalimentación lineal en la construcción de criptosistemas de cifrado en flujo.

Introducción

Hipótesis de investigación:

El análisis criptográfico de los registros de desplazamiento con retroalimentación lineal, basado en la teoría de las sucesiones recurrentes lineales sobre campos finitos binarios, permitirá determinar las potencialidades reales de utilización de los LFSR en la construcción de criptosistemas de cifrado en flujo.

Objetivo general:

Realizar un análisis criptográfico de los registros de desplazamiento con retroalimentación lineal, basado en la teoría de las sucesiones recurrentes lineales sobre campos finitos binarios.

Para lograr dicho objetivo general, se proponen los siguientes **objetivos específicos:**

1. Exponer la teoría general sobre los campos finitos binarios.
2. Profundizar en el estudio de las sucesiones recurrentes lineales sobre campos finitos binarios.
3. Presentar las propiedades generales de los LFSRs.
4. Determinar la relación entre las sucesiones recurrentes lineales y los registros de desplazamiento con retroalimentación lineal.
5. Analizar el funcionamiento de los registros de desplazamiento con retroalimentación lineal.

Para dar cumplimiento a estos objetivos es necesario plantearse las siguientes **interrogantes científicas:**

1. ¿Cuándo un campo finito es binario?
2. ¿Qué es una sucesión recurrente lineal binaria?
3. ¿Qué es un registro de desplazamiento con retroalimentación lineal?
4. ¿Qué relación existe entre las sucesiones recurrentes lineales y los registros de desplazamientos con retroalimentación lineal?

Introducción

Con el propósito de resolver las interrogantes científicas que responden a los objetivos específicos fue necesario plantearse y solucionar las siguientes **tareas de investigación**:

1. Revisión bibliográfica sobre la teoría de los campos finitos, particularizando en los de característica dos. Consulta de libros, artículos y páginas de internet, entre otras fuentes.
2. Estudio de las sucesiones recurrentes lineales en campos finitos binarios.
3. Profundización en el estudio de los conceptos generales y funcionamiento de los registros de desplazamiento con retroalimentación lineal.
4. Representación de las salidas de los LFSRs como sucesiones recurrentes lineales.
5. Caracterización de las salidas de los LFSRs según los postulados de Golomb.
6. Exposición de la relación entre el polinomio de conexión y los coeficientes de la recurrencia lineal.
7. Explicación de los principios básicos de los ataques con texto claro conocido.
8. Obtención de los parámetros de los registros de desplazamiento con retroalimentación lineal.
9. Recuperación del estado inicial de los LFSRs.

Métodos de investigación científica:

Método hipotético-deductivo: Al elaborar la hipótesis de investigación a partir de los resultados de la revisión bibliográfica.

Inducción – deducción: Para en el estudio de las fuentes de información, extraer de ellas regularidades y tendencias relacionadas con el tema de investigación y la lógica de pensamiento cuyas interrelaciones y generalizaciones permiten la argumentación y la coherencia de la propuesta que se realice.

Histórico-lógico: Para el análisis de la trayectoria evolutiva de la investigación a partir de su objeto, antecedente y desarrollo. En la revisión de la literatura adecuada para la

Introducción

determinación de las tendencias actuales de cómo son usados los campos finitos en los criptosistemas.

Aportes de la investigación:

Los principales aportes de esta investigación son fundamentalmente teóricos, debido a que se presenta un procedimiento para la determinación del polinomio de retroalimentación de los LFSRs, a partir del conocimiento de cierta cantidad de elementos de salida y se exponen métodos para la recuperación del estado inicial, basados en la teoría de las sucesiones recurrentes lineales, bajo ciertos supuestos. Como resultado práctico se propone un algoritmo para la obtención del polinomio de retroalimentación de un LFSR.

Estructura del trabajo:

La tesis está estructurada en tres capítulos:

En el primer capítulo se abordan aspectos fundamentales de la teoría de los campos finitos particularizando en los binarios que son los de interés criptográfico y sobre los que se desarrolla la investigación. Además, especifican algunos conceptos y propiedades sobre las sucesiones recurrentes lineales definidas sobre estos tipos de campos finitos.

En el segundo capítulo se brindan las principales propiedades de los registros de desplazamientos con retroalimentación lineal, así como, de las sucesiones que estos generan. También, se representa la relación existente entre los registros de desplazamientos con retroalimentación lineal y las sucesiones recurrentes lineales.

En el tercer capítulo se exponen algunos métodos para el análisis de los registros de desplazamientos con retroalimentación lineal. Se presenta un procedimiento para la obtención de algunos parámetros de estos mecanismos a partir de la sucesión de salida. Además, se proponen métodos para la recuperación del estado inicial de los registros de desplazamiento con retroalimentación lineal.

Introducción

CAPÍTULO I. SUCESSIONES RECURRENTES LINEALES SOBRE CAMPOS FINITOS BINARIOS

La teoría de los campos finitos tiene sus orígenes en los siglos XVII y XVIII con el estudio de una clase especial de campos finitos, los llamados campos primos, gracias a los aportes de matemáticos tan reconocidos como Pierre de Fermat (1601-1665), Leonhard Euler (1707-1783), Joseph-Louis Lagrange (1736-1813) y Adrien-Marie Legendre (1752-1833). La teoría general sobre los campos finitos comienza con los trabajos de Carl F. Gauss y Evariste Galois a principios del siglo XIX. También conocidos como campos de Galois, los campos finitos han tenido en los últimos años muchas aplicaciones, entre las que se cuentan los códigos algébricos, los esquemas criptográficos, los generadores de números aleatorios, el procesamiento digital de señales y los códigos de corrección de errores (Niederreiter, 1986).

Como se dijo anteriormente las sucesiones sobre campos finitos cuyos términos dependerán de una manera sencilla en sus predecesores son de importancia para una variedad de aplicaciones. Dichas sucesiones son fáciles de generar mediante procedimientos recursivos, lo cual es sin duda una característica ventajosa desde el punto de vista computacional y también tienden a tener propiedades estructurales útiles. De particular interés es el caso en los términos dependen linealmente de un número fijo de sus predecesores, lo que resulta en una sucesión de manera lineal llamada recurrente. Estas sucesiones se emplean, por ejemplo, en la teoría de la codificación, en la criptografía (véase el Capítulo 2), y en varias ramas de la ingeniería eléctrica (Niederreiter, 1986). En estas aplicaciones, el campo subyacente que se toma a menudo es \mathbb{F}_2 , pero la teoría puede ser desarrollada bastante general para cualquier campo finito.

Este capítulo está compuesto por dos epígrafes. El primero está dividido en tres secciones, en primer lugar se aborda las definiciones y propiedades de los campos, en segundo las propiedades de polinomios sobre campos finitos, haciendo énfasis en los

Capítulo I

polinomios irreducibles y la tercera sección trata la caracterización de los campos finitos y un conjunto de propiedades que estos cumplen y que son importantes para la comprensión del trabajo y la fundamentación del tema a tratar en el próximo capítulo.

El segundo epígrafe es el más importante, está dividido en 4 secciones; el primero se dedica a definir los tipos sucesiones recurrentes lineales sobre campos finitos; el segundo, al período de una sucesión recurrente lineal, el tercero a los métodos básicos de representación de las SRL y el último aborda las SRL sobre campos finitos binarios.

Las definiciones, teoremas y propiedades que se enuncian en el capítulo, se pueden encontrar en (Niederreiter, 1986) y (Panario, 2013) y lo relacionado a sucesión recurrente lineal en (Niederreiter, 1986). Igualmente las demostraciones de todos los teoremas, lemas y definiciones correspondientes a cada epígrafe. Para profundizar en el tema de campos finitos recomendamos también (Mendoza, 2009)).

1.1 Conceptos básicos

1.1.1 Campos finitos

Definición 1.1

Un **campo** es un conjunto F no vacío con dos operaciones internas $(+ \text{ y } *)$ donde

- $(F, +)$ es un grupo conmutativo.
- $(F \setminus \{0\}, *)$ es un grupo conmutativo.
- Se cumple la ley distributiva del producto con respecto a la suma.

Es decir, un campo es un anillo conmutativo en el que todo elemento distinto de cero tiene inverso.

Un subcampo S de F es un subanillo de F que es en sí mismo un campo.

Lema 1.2

Un anillo conmutativo R es un campo, si y solo si, no contiene ideales distintos de (0) y R .

Capítulo I

Un homomorfismo de campos no es más que un homomorfismo de anillos. Este es siempre inyectivo, porque su núcleo, siendo un ideal propio, tiene que ser cero según el lema anterior.

Es fácil comprobar que la aplicación $f: \mathbb{Z} \rightarrow F : f(n) = e + \dots + e = ne$, donde e es el neutro de F para el producto, es un homomorfismo de anillos y por tanto su núcleo es un ideal de \mathbb{Z} . Pueden producirse entonces dos variantes:

1. El núcleo es (0) , entonces f puede extenderse a un homomorfismo $\bar{f}: \mathbb{Q} \rightarrow F$, lo que indica que F contiene una copia de \mathbb{Q} . En este caso se dice que **F es de característica cero**.

2. El núcleo es $p\mathbb{Z}$ para algún p natural, que además tiene que ser primo (de lo contrario existen en F dos elementos distintos de cero cuyo producto es cero). En este caso F contiene una copia de $\mathbb{Z}/p\mathbb{Z}$, y se dice que **F es de característica p** .

Este último caso es el que nos interesa, pues los campos finitos tienen característica $p > 0$, específicamente cuando $p = 2$, se llaman **campos binarios** o de característica dos. Podemos percibir que un **campo finito** no es más que un campo con un número finito de elementos. Y como acabamos de apreciar, su característica es un número primo. Usaremos la notación \mathbb{F}_p para referirnos al campo $\mathbb{Z}/p\mathbb{Z}$. $\mathbb{F}_2, \mathbb{F}_3, \mathbb{F}_5, \dots$ y \mathbb{Q} son los llamados campos primos. Un campo de característica p se dice que tiene a \mathbb{F}_p como su subcampo primo. Para el caso que nos interesa, cuando la característica es dos, entonces se dice que tiene a \mathbb{F}_2 como su subcampo primo, siendo $\mathbb{F}_2 = \{0,1\}$.

1.1.2 Polinomios

Sea $F[x]$ el anillo de polinomios con coeficientes en el campo F .

Definición 1.3

Un polinomio $f \in F[x]$ se dice **irreducible sobre F** si f tiene grado positivo y no puede descomponerse como el producto de dos polinomios de $F[x]$, ambos de grado positivo.

Es evidente que los polinomios lineales (de grado uno) son irreducibles.

Una propiedad fundamental del anillo $R[x]$ es que es un dominio de integridad si R lo es. Así que $F[x]$ es un dominio de integridad, con la propiedad adicional de que se cumple la división con resto. Esto es, dados cualesquiera $f, g \in F[x]$, existen $q, r \in F[x]$ tales

Capítulo I

que $f = gq + r$, donde $\text{grd}(r) \leq \text{grd}(g)$, ($\text{grd}(f)$ es el grado del polinomio f). Se dice que g divide a f y se denota $g|f$ si existe q tal que $f = gq$. La división con resto permite probar que $F[x]$ es un dominio de factorización única.

Cada polinomio no nulo f sobre un campo finito además de su grado $\text{grd}(f)$ tiene otra característica numérica entera su orden.

Lema 1.4

Si el polinomio $f \in F_q[x]$ es un polinomio de grado $k \geq 1$ que satisface la condición $f(0) \neq 0$, entonces existe un número natural $e \leq q^k - 1$, para el cual el binomio $x^e - 1$ se divide por el polinomio $f(x)$.

Definición 1.5

Sea $f \in F_q[x]$ un polinomio no nulo. Si $f(0) \neq 0$, entonces el menor número natural e para el cual el polinomio $f(x)$ divide a $x^e - 1$ se llama **orden del polinomio $f(x)$** y se denota por $\text{ord}(f) = \text{ord}(f(x))$. Pero si $f(0) = 0$, entonces el polinomio $f(x)$ se puede representar de forma única como $f(x) = x^h g(x)$, donde $h \in \mathbb{N}$ y $g \in F_q[x]$ y $g(0) \neq 0$ y en este caso el orden del polinomio f se define como $\text{ord}(g)$.

Teorema 1.6

Si $f(x) \in F_q[x]$ es un polinomio irreducible sobre el campo F_q y $\text{grd}(f(x)) = k$, entonces $\text{ord}(f(x))$ divide a q^{k-1} .

Teorema 1.7

Todo polinomio $f \in F[x]$ se puede descomponer de manera única, salvo el orden de los factores, como producto de polinomios irreducibles.

Los polinomios irreducibles en $F[x]$ juegan el mismo papel que los números primos en \mathbb{Z} , así podemos decir que si un polinomio irreducible sobre F divide un producto de polinomios en $F[x]$ entonces divide al menos a uno de los factores de este producto.

Definición 1.8

Un elemento $\alpha \in F$ se dice que es raíz de $f \in F[x]$ si se cumple que $f(\alpha) = 0$.

De la definición anterior y la división con resto se deduce el siguiente teorema.

Teorema 1.9

Sea $f \in F[x]$ irreducible y α una raíz de f , $g(\alpha) = 0$ para algún $g \in F[x]$ si y solo si f divide a g .

En particular, si consideramos $f(x) = x - \alpha$, se tiene $g(\alpha) = 0$ si y solo si $x - \alpha \mid g(x)$. Aplicando este resultado un número finito de veces obtenemos el siguiente teorema.

Teorema 1.10

Un polinomio $f \in F[x]$ de grado k tiene a lo sumo k raíces en F .

Una consecuencia del resultado anterior es que los polinomios de grado 2 y 3 son irreducibles sobre F si y solo si no tienen raíces en F .

Para ilustrar la utilidad de algunos conceptos y propiedades enunciados hasta el momento, veamos el siguiente ejemplo: hallar los polinomios mónicos (con coeficiente principal igual a 1) irreducibles sobre \mathbb{F}_2 de grado 4.

Notemos que un polinomio $f \in \mathbb{F}_2[x]$, de cuarto grado, es irreducible si no tiene divisores de grado 1 o 2 en $\mathbb{F}_2[x]$. Por tanto podemos calcular todos los productos de las formas $(x+a)(x^3+bx+c)$ y $(x^2+ax+b)(x^2+cx+d)$, y compararlos con la lista de los $2^4 = 16$ polinomios mónicos de grado 4 en $\mathbb{F}_2[x]$. Encontramos entonces que $x^4 + x^3 + x^2 + x + 1$, $x^4 + x^3 + 1$ y $x^4 + x + 1$ son los polinomios irreducibles que buscamos.

1.1.3 Caracterización de los campos finitos

Por el momento sólo tenemos como ejemplo de campo finito a \mathbb{F}_p (p primo). A continuación denotaremos por \mathbb{F}_q al campo de q elementos (no decimos “**un** campo de q elementos” porque un campo finito de un orden determinado es único salvo isomorfismo).

Teorema 1.11

El anillo de restos $\mathbb{F}_q[x]/\langle f \rangle$ donde $f \in \mathbb{F}_q[x]$ es un polinomio mónico irreducible de grado k , es un campo. Este será el campo \mathbb{F}_{q^k} , que se llama **extensión algebraica** de \mathbb{F}_q de grado k , (y se obtiene al adjuntarle a \mathbb{F}_q una raíz del polinomio irreducible f).

Capítulo I

Este campo está conformado por los polinomios de $\mathbb{F}_q[x]$ de grado menor que k , por tanto tiene q^k elementos. Sea α una raíz de f , se puede representar \mathbb{F}_{q^k} como el conjunto de los polinomios en α de grado $\leq k-1$ con coeficientes en \mathbb{F}_q , en este caso α se llama **elemento definitorio** de \mathbb{F}_{q^k} . Es decir

$$\mathbb{F}_{q^k} = \{c_{k-1}\alpha^{k-1} + \dots + c_1\alpha + c_0 \mid c_i \in \mathbb{F}_q\}$$

Este teorema da una forma de representar los elementos del campo \mathbb{F}_{q^k} mediante la raíz de un polinomio f irreducible sobre \mathbb{F}_q , a este f se le llama **polinomio característico de la extensión \mathbb{F}_{q^k}** .

Ejemplo 1.12

Siendo α raíz de $f(x) = x^4 + x^3 + 1$, que es irreducible sobre \mathbb{F}_2 . Entonces \mathbb{F}_{2^4} puede representarse por el conjunto $\{0, 1, \alpha, \alpha^2, \alpha^3, \alpha^3 + 1, \alpha^3 + \alpha + 1, \alpha^3 + \alpha^2 + \alpha + 1, \alpha^2 + \alpha + 1, \alpha^3 + \alpha^2 + \alpha, \alpha^2 + 1, \alpha^3 + 1, \alpha^3 + \alpha^2 + 1, \alpha + 1, \alpha^2 + \alpha, \alpha^3 + \alpha^2\}$ con la suma y la multiplicación usuales en $\mathbb{F}_2[\alpha]$ y reduciendo los elementos de grado mayor que uno mediante la relación $\alpha^4 + \alpha^3 + 1 = 0$. Si queremos calcular por ejemplo α^{16} , se tendría $\alpha^{16} = \alpha \alpha^{15} = \alpha(\alpha^3 + \alpha^2) = \alpha^4 + \alpha^3 = \alpha^3 + 1 + \alpha^3 = 1$.

Otra forma de ver la extensión \mathbb{F}_{q^k} es como espacio vectorial de dimensión k sobre \mathbb{F}_q . La representación que acabamos de dar nos permite tomar al conjunto $\{1, \alpha, \alpha^2, \dots, \alpha^{k-1}\}$ (donde α es el elemento definitorio de \mathbb{F}_{q^k}) como una base de \mathbb{F}_{q^k} , a esta base se le llama **base polinomial**. Los elementos de \mathbb{F}_{q^k} quedarán representados entonces en la forma $c_{k-1}\alpha^{k-1} + \dots + c_1\alpha + c_0$ donde $c_i \in \mathbb{F}_q \forall i \in \{0, 1, \dots, k-1\}$.

Vimos cómo se extiende el campo \mathbb{F}_q adjuntando la raíz de un polinomio irreducible de grado k para obtener el campo \mathbb{F}_{q^k} . ¿Pero qué podemos decir de un campo F que contiene a \mathbb{F}_q ?

Teorema 1.13

Sea F un campo finito que contiene a \mathbb{F}_q , entonces F tiene q^k elementos, para algún $k \in \mathbb{N}$.

Capítulo I

La demostración se obtiene considerando a F como espacio vectorial finito dimensional sobre \mathbb{F}_q (de dimensión k).

Del teorema anterior se deduce una característica esencial de los campos finitos.

Teorema 1.14

Sea F un campo finito de característica p , entonces F tiene p^n elementos, para algún $n \in \mathbb{N}$.

Teorema 1.15

Dado el campo finito \mathbb{F}_q con $q = p^k$ elementos, todo subcampo de \mathbb{F}_q tendrá entonces p^n elementos, donde n es un divisor de k .

La demostración se obtiene al aplicar el teorema 1.11 considerando a F como subcampo de \mathbb{F}_{p^k} , por tanto F tiene característica p y p^k es una potencia del orden de F .

Definición 1.16

Sean los campos F y K , donde F es una extensión de K . Si un polinomio $f \in K[x]$ tiene todas sus raíces en F , y F es la menor extensión de K con esta característica, se dice que F es el **campo de descomposición de f sobre K** , o que f se descompone en F .

Teorema 1.17

Sea K un campo y f un polinomio de grado positivo en $K[x]$, entonces existe un campo de descomposición de f sobre K . Dos campos de descomposición de f sobre K son isomorfos bajo un isomorfismo que deja fijos los elementos de K y deja invariante el conjunto de las raíces de f .

Es evidente que el campo de descomposición de un polinomio $f \in K[x]$ es el menor campo que contiene todas sus raíces, así que el teorema anterior se deduce del proceso de adjuntar a K las raíces de f y la segunda parte de la unicidad de los campos finitos.

Capítulo I

De lo visto sobre polinomios irreducibles y su relación con las extensiones de campos podemos deducir que un polinomio cualquiera f sobre un campo \mathbb{F}_q se descompone en factores lineales $x - a$ con $a \in \mathbb{F}_q$ y factores irreducibles (de grado > 1) sobre \mathbb{F}_q . Está claro que si se adjuntan todas las raíces de f se obtiene su campo de descomposición. Una pregunta interesante es la siguiente: ¿Se obtendrá el campo de descomposición de f si se extiende \mathbb{F}_q adjuntándole un subconjunto de las raíces de f ? La respuesta yace en el siguiente teorema.

Teorema 1.18

Si $f \in \mathbb{F}_q[x]$ es un polinomio irreducible sobre \mathbb{F}_q de grado k , entonces f tiene una raíz α en \mathbb{F}_{q^k} . Es más, todas las raíces de f se hallan en \mathbb{F}_{q^k} y están dadas por los k elementos $\alpha, \alpha^q, \dots, \alpha^{q^{k-1}}$ de \mathbb{F}_{q^k} .

Corolario 1.19

Si $f \in \mathbb{F}_q[x]$ es irreducible sobre \mathbb{F}_q , de grado k , entonces \mathbb{F}_{q^k} es su campo de descomposición. Si f no es irreducible sobre \mathbb{F}_q , su campo de descomposición es el menor campo en que se descomponen todos los factores irreducibles de f .

Definición 1.20

Los elementos $\alpha, \alpha^q, \dots, \alpha^{q^{k-1}}$ de una extensión \mathbb{F}_{q^k} de \mathbb{F}_q se llaman **conjugados de α con respecto a \mathbb{F}_q** .

En el siguiente teorema veremos una propiedad útil sobre los elementos de \mathbb{F}_q , resultado de que \mathbb{F}_q^* sea un grupo (de orden finito) bajo la operación de multiplicación.

Teorema 1.21

Todo elemento $a \in \mathbb{F}_q$ cumple la propiedad $a^q = a$.

Del teorema anterior se deduce una característica del polinomio $x^q - x$, de particular importancia en la teoría de campos finitos.

Lema 1.22

El polinomio $x^q - x$ se descompone en \mathbb{F}_q como $\prod_{\alpha \in \mathbb{F}_q} (x - \alpha)$ y \mathbb{F}_q es su campo de descomposición.

Del lema anterior se deduce que todo elemento de un campo finito \mathbb{F}_{q^k} es raíz de un polinomio en $\mathbb{F}_q[x]$ (considerar por ejemplo $x^{q^k} - x$) al polinomio mónico de menor grado con esta propiedad para un elemento determinado $\alpha \in \mathbb{F}_{q^k}$ se le llama **polinomio mínimo de α sobre \mathbb{F}_q** y se demuestra fácilmente que dicho polinomio es irreducible.

Los teoremas 1.13, 1.14 y 1.15 ofrecen una visión más clara sobre el número de elementos en un campo finito, la que en cierto sentido se refuerza con el siguiente teorema.

Teorema 1.23

Para todo primo p y natural n existe un campo finito con p^n elementos (\mathbb{F}_{p^n}).

Para la demostración se considera el campo de descomposición del polinomio $f(x) = x^{p^n} - x$ sobre el campo primo \mathbb{F}_p . Siendo F dicho campo de descomposición, se considera entonces el conjunto $S = \{a \in F \mid a^{p^n} - a = 0\}$ o sea, el conjunto de raíces de f en F , se demuestra entonces que S es un subcampo de F y al contener todas las raíces de f , por la definición 1.14 $S = F$. Así que F es un campo con p^n elementos.

Existen además otras formas de representar un campo \mathbb{F}_q , una muy común es como potencias de un elemento fijo. Para verlo, primero es necesario enunciar el siguiente teorema.

Teorema 1.24

El grupo multiplicativo de un campo \mathbb{F}_q (denotado \mathbb{F}_q^*) es cíclico. Un generador de \mathbb{F}_q^* se llama elemento primitivo de \mathbb{F}_q .

De este teorema se deducen conclusiones importantes.

Teorema 1.25

Toda extensión \mathbb{F}_{q^k} de un campo \mathbb{F}_q se puede considerar como una extensión de \mathbb{F}_q al adjuntarle un solo elemento (a este tipo de extensiones se les denomina **simples**).

Para la demostración se considera extender \mathbb{F}_q al adjuntarle un elemento primitivo ξ de \mathbb{F}_{q^k} . De este razonamiento se deduce también que para cualquier m natural existe un polinomio irreducible en $\mathbb{F}_q[x]$ de grado k , este será el polinomio mínimo de un elemento primitivo de \mathbb{F}_{q^k} .

Teorema 1.26

Los elementos conjugados de un $\alpha \in \mathbb{F}_q$ con respecto a cualquier subcampo de \mathbb{F}_q tienen un mismo orden en el grupo multiplicativo \mathbb{F}_q^* .

Se demuestra a partir de la relación entre el orden de un elemento a en un grupo cíclico y el orden de a^m , para lo que se tiene en cuenta que $\text{mcd}(q-1, q^i) = 1$ para cualquier $i \in \mathbb{N}$.

El polinomio mínimo de un elemento $\alpha \in \mathbb{F}_{q^k}$ está dado por $\prod_{i=0}^{d-1} (x - \alpha^{q^i})$ y su grado d es un divisor de k .

Definición 1.27

Sea \mathbb{F}_{q^k} una extensión de \mathbb{F}_q , cuyo elemento definitorio α es raíz de un polinomio irreducible f de grado k . Si todo elemento de $\mathbb{F}_{q^k}^*$ se puede expresar como una potencia de α (equivalentemente, α es un elemento primitivo de \mathbb{F}_{q^k}) se dice entonces que f es un **polinomio primitivo**.

Al ser $\mathbb{F}_{q^k}^*$ un grupo cíclico, siempre existe en él un elemento (y un polinomio) primitivo.

Esto nos permite plantear $\mathbb{F}_{q^k} = \{ \alpha^m \mid 0 \leq m \leq q^k - 1 \}$ siempre que α sea raíz de un polinomio primitivo sobre \mathbb{F}_q .

La definición anterior se puede transcribir como sigue:

Capítulo I

Definición 1.28

El polinomio $f \in \mathbb{F}_q[x]$ de grado $k \geq 1$ se llama polinomio primitivo sobre el campo \mathbb{F}_q si es el polinomio mínimo sobre el campo \mathbb{F}_q de cierto elemento primitivo de la extensión \mathbb{F}_{q^k} del campo \mathbb{F}_q .

De esta manera, el polinomio primitivo sobre \mathbb{F}_q de grado k es un polinomio mónico, el cual es irreducible sobre \mathbb{F}_q y tiene una raíz $\alpha \in \mathbb{F}_{q^k}$ que es un elemento generador del grupo multiplicativo $\mathbb{F}_{q^k}^*$ del campo \mathbb{F}_{q^k} . Los polinomios primitivos se pueden caracterizar también así:

Teorema 1.29

El polinomio $f \in \mathbb{F}_q[x]$ de grado k es un polinomio primitivo sobre \mathbb{F}_q si y solo si, él es un polinomio mónico tal que $f(x) \neq 0$ y $\text{ord}(f) = q^k - 1$.

De lo visto anteriormente podemos sacar algunas conclusiones.

Lema 1.30

Un elemento α (diferente de 0) de \mathbb{F}_{q^k} tiene como orden multiplicativo un divisor de $q^k - 1$, si este divisor es el propio $q^k - 1$ entonces α es un elemento primitivo de \mathbb{F}_{q^k} .

Lema 1.31

Sea $\alpha \in \mathbb{F}_{p^k}$ se cumple que $\alpha^n = \alpha$ si y solo si $\alpha \in \mathbb{F}_{p^n}$ donde n es un divisor de k .

Lema 1.32

De la teoría de números conocemos que $\text{mcd}(a^n - 1, a^k - 1) = a^{\text{mcd}(k,n)} - 1$, así que el mayor campo contenido en \mathbb{F}_{q^k} y \mathbb{F}_{q^n} es $\mathbb{F}_{q^{\text{mcd}(n,k)}}$.

Para ilustrar algo de lo visto sobre la caracterización de los campos finitos podemos afirmar por ejemplo que existe un campo con 1024 elementos ($\mathbb{F}_{2^{10}}$), que sus subcampos propios son \mathbb{F}_2 , \mathbb{F}_{2^2} y \mathbb{F}_{2^5} , que un elemento a de $\mathbb{F}_{2^{10}}$ cumple $a^n = a$ si y solo si $n = 1, 2$ ó 5 en cuyo caso $a \in \mathbb{F}_{2^{10}}, \mathbb{F}_{2^2}$ ó \mathbb{F}_{2^5} respectivamente. Otra conclusión es

que para obtener los elementos de $\mathbb{F}_{2^{10}}$ como polinomios con coeficientes en \mathbb{F}_2 se le debe adjuntar a este último la raíz α de un polinomio irreducible de grado 10, si este polinomio es primitivo todos los elementos de $\mathbb{F}_{2^{10}}$ se pueden expresar como potencias de α .

1.2 Sucesiones recurrentes lineales sobre un campo finito

1.2.1 Definición de sucesión recurrente lineal

Definición 1.33

Sea k -número natural, $a, a_0, a_1, \dots, a_{k-1}$, elementos dados del campo finito \mathbb{F}_q . La sucesión s_0, s_1, \dots , de elementos del campo \mathbb{F}_q , que satisface la relación $s_{n+k} = a_{k-1}s_{n+k-1} + a_{k-2}s_{n+k-2} + \dots + a_0s_n + a$ $n = 0, 1, \dots$ (1.1) donde los primeros términos s_0, s_1, \dots, s_{k-1} unívocamente determinan toda la sucesión y se llaman valores iniciales.

Dicha relación se llama **relación recurrente lineal (de orden k)**. En la antigua literatura se puede también encontrar el término «ecuación en diferencias». El caso en que $a = 0$, se denomina relación recurrente lineal homogénea, en caso contrario relación recurrente lineal no homogénea. La correspondiente sucesión recurrente se llama **sucesión recurrente lineal homogénea (no homogénea)** sobre el campo \mathbb{F}_q .

Sea s_0, s_1, \dots una sucesión recurrente lineal homogénea de orden k sobre el campo \mathbb{F}_q , que satisface la relación recurrente lineal $s_{n+k} = a_{k-1}s_{n+k-1} + a_{k-2}s_{n+k-2} + \dots + a_0s_n$ $n = 0, 1, \dots$ (1.2) donde $a_j \in \mathbb{F}_q$, $0 \leq j \leq k-1$. El polinomio $f(x) = x^k - a_{k-1}x^{k-1} - a_{k-2}x^{k-2} - \dots - a_0 \in \mathbb{F}_q[x]$ se llama **polinomio característico** de la sucesión recurrente lineal dada. Está claro que él depende de la relación recurrente lineal (1.2).

En calidad de primera aplicación de la noción de polinomio característico de la sucesión recurrente lineal mostramos como en un caso particular importante los términos de la sucesión recurrente lineal pueden ser expresados de manera clara a través de los coeficientes del polinomio $f(x)$.

Teorema 1.34

Sea s_0, s_1, \dots una sucesión recurrente lineal homogénea de orden k sobre el campo \mathbb{F}_q y $f(x)$ su polinomio característico. Si las raíces a_1, \dots, a_k del polinomio $f(x)$ son todas diferentes, entonces $s_n = \sum_{j=1}^k \beta_j a_j^n$ $n = 0, 1, \dots$ (1.3) donde β_1, \dots, β_k diferentes elementos del campo de descomposición del polinomio $f(x)$ sobre el campo \mathbb{F}_q , los cuales unívocamente se determinan por los términos iniciales de la sucesión recurrente s_0, s_1, \dots .

Teorema 1.35

Si s_0, s_1, \dots es una sucesión recurrente lineal homogénea sobre el campo \mathbb{F}_q entonces existe un polinomio mónico determinado unívocamente $m(x) \in \mathbb{F}_q[x]$, poseedor de la siguiente propiedad, el polinomio mónico de grado positivo $f(x) \in \mathbb{F}_q[x]$ es el polinomio característico de la sucesión dada s_0, s_1, \dots si y solo si $f(x)$ se divide por $m(x)$.

Teorema 1.36

Sea $f(x) \in \mathbb{F}_q[x]$ el polinomio mónico irreducible sobre el campo \mathbb{F}_q y sea s_0, s_1, \dots una sucesión recurrente lineal homogénea sobre el campo \mathbb{F}_q , que no es una sucesión nula, si $f(x)$ es el polinomio característico de la sucesión s_0, s_1, \dots entonces él es igual a su polinomio mínimo $f(x)$.

Teorema 1.37

Sea s_0, s_1, \dots una sucesión de elementos del campo \mathbb{F}_q que satisface la relación recurrente lineal de orden k con polinomio característico $f(x) \in \mathbb{F}_q[x]$, entonces el polinomio $f(x)$ coincide con el polinomio mínimo de esta sucesión si y solo si los vectores de estado s_0, s_1, \dots, s_{k-1} son linealmente independientes sobre el campo \mathbb{F}_q .

Consecuencia 1.38

Si la sucesión s_0, s_1, \dots es la función de impulso correspondiente a cierta relación recurrente lineal homogénea sobre el campo \mathbb{F}_q , entonces el polinomio mínimo de esta sucesión es igual al polinomio característico de esta relación recurrente lineal.

1.2.3 Métodos básicos de representación de las SRL

1.2.3.1 Matriz Acompañante

Uno de los métodos básicos de representación de las SRL lo constituye el método de la matriz acompañante, esto es:

Sea s_0, s_1, \dots, s_{k-1} una sucesión homogénea de orden k en \mathbb{F}_q la cual satisface la siguiente relación

$$s_{n+k} = a_{k-1}s_{n+k-1} + a_{k-2}s_{n+k-2} + \dots + a_0s_n \quad n = 0, 1, \dots \quad (1.2)$$

y $a_j \in \mathbb{F}_q$ para $0 \leq j \leq k-1$. A esta sucesión le podemos asignar la siguiente matriz de tamaño $k \times k$ sobre \mathbb{F}_q

$$A = \begin{pmatrix} 0 & 0 & \dots & 0 & a_0 \\ 1 & 0 & \dots & 0 & a_1 \\ 0 & 1 & \dots & 0 & a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & a_{k-1} \end{pmatrix} \quad (1.4)$$

La cual llamaremos **matriz acompañante** a la sucesión recurrente lineal.

Hay otras formas equivalentes de representar esta matriz. En el presente trabajo usaremos la representación de (Menezes, VanOorschot, & Vanstone, 1996).

Es fácil notar que $f(x)$ coincide con el polinomio característico de la matriz A como él se determina en el álgebra lineal, es decir $f(x) = \det(A - xI)$, donde I es la matriz identidad de orden $k \times k$ sobre el campo \mathbb{F}_q . Por otro lado la matriz A se puede considerar como la matriz acompañante del polinomio mónico $f(x)$.

Lema 1.39

Sea s_0, s_1, \dots una sucesión recurrente lineal homogénea de orden k sobre el campo \mathbb{F}_q tal que se cumple la relación (1.2) y A es la matriz acompañante a esta sucesión definida por la igualdad (1.4), entonces para los vectores de estado de la sucesión s_0, s_1, \dots es válida la igualdad.

$$s_n = s_0 A^n \quad (1.5)$$

Lema 1.40

Si $f(x) = x^k - a_{k-1}x^{k-1} - a_{k-2}x^{k-2} - \dots - a_0 \in \mathbb{F}_q[x]$ $k \geq 1$, $a_0 \neq 0$. Entonces $\text{ord}(f(x))$ es igual al orden de la matriz A definida por la fórmula (1.4) y considerada como elemento del grupo lineal general $GL(k, \mathbb{F}_q)$ (grupo de las matrices cuadradas inversibles (determinante distinto de cero), de orden k con coeficientes sobre \mathbb{F}_q).

1.2.3.2 Función Generatriz

Hasta el momento en el estudio de las sucesiones recurrentes lineales hemos utilizado los conceptos del álgebra lineal, el álgebra de los polinomios y la teoría de los campos finitos. La utilización del funcionamiento algebraico de las series de potencias formales nos permite obtener otros resultados notables relacionados con las sucesiones recurrentes lineales.

Sea una sucesión arbitraria s_0, s_1, \dots de elementos del campo \mathbb{F}_q , a esta sucesión se le puede asociar su **función generatriz** de la variable x , la cual es sencillamente una expresión formal del tipo $G(x) = s_0 + s_1x + s_2x^2 + \dots + s_nx^n = \sum_{n=0}^{\infty} s_nx^n$ (1.6) donde x es la variable formal. Sobre la base de este enfoque está la idea de que en la función $G(x)$ están recogidos, en determinado orden, todos los términos de la sucesión s_0, s_1, \dots así que la función $G(x)$ puede, de cierta manera, reflejar las propiedades de esta sucesión.

Para la aplicación de la teoría de las series formales de potencia examinaremos ahora una sucesión recurrente lineal de orden k , s_0, s_1, \dots sobre el campo \mathbb{F}_q , que satisface la relación recurrente lineal (1.2). Llamemos al polinomio $f^*(x) = 1 - a_{k-1}x - a_{k-2}x^2 - \dots - a_0x^k \in \mathbb{F}_q[x]$ (1.7) **polinomio característico reverso** de esta sucesión. El polinomio característico $f(x)$ y su polinomio característico reverso $f^*(x)$ están ligados entre sí por la relación $f^*(x) = x^k f(1/x)$. Si el polinomio característico es primitivo entonces su reverso también lo es.

Teorema 1.41

Si s_0, s_1, \dots sucesión recurrente lineal homogénea de orden k sobre el campo \mathbb{F}_q que satisface la relación recurrente lineal (1.2). Sea $f^*(x) \in \mathbb{F}_q[x]$ el polinomio característico reverso de esta sucesión definida en (1.6), entonces tiene lugar la igualdad

$$G(x) = \frac{g(x)}{f^*(x)} \quad (1.8)$$

donde $g(x) = -\sum_{j=0}^{k-1} \sum_{i=0}^j a_{i+k-j} s_i x^j \in \mathbb{F}_q[x]$ y $a_k = -1$ (1.9)

El recíproco, si $g(x)$ es un polinomio generador sobre el campo \mathbb{F}_q , $\text{grad}(g(x)) < k$ y $f^*(x) \in \mathbb{F}_q[x]$ se define por la igualdad (1.7), entonces la serie formal de potencia $G(x) \in \mathbb{F}_q[[x]]$ definida por la igualdad (1.6) es una función generatriz de la sucesión recurrente lineal homogénea de orden k sobre el campo \mathbb{F}_q que satisface la relación recurrente lineal (1.2).

1.2.2 Período de una sucesión recurrente lineal.

Una particularidad típica de las sucesiones recurrentes lineales sobre un campo finito es que a partir de algún momento muestran su naturaleza periódica, es decir:

Definición 1.42

Sea S un conjunto arbitrario no vacío y sea s_0, s_1, \dots una sucesión de elementos del conjunto S . Si existen los números enteros $r > 0$ y $n_0 > 0$ tales que $s_{n+r} = s_n$ para todos los $n \geq n_0$, entonces la sucesión s_0, s_1, \dots , se llama **sucesión periódica**, a r se le llama período de esta sucesión. El menor de todos los posibles períodos de la sucesión periódica se llama período mínimo de la sucesión.

Antes de pasar al estudio detallado de la periodicidad, introducimos la terminología correspondiente y damos algunas afirmaciones generales concernientes a las sucesiones periódicas.

Lema 1.43

Cada período de la sucesión periódica se divide por su período mínimo.

Definición 1.44

La sucesión periódica s_0, s_1, \dots con período mínimo r se llama **puramente periódica** si la igualdad $s_{n+r} = s_n$ se cumple para todos los $n = 0, 1, \dots$

La siguiente condición, que a veces se encuentra en la literatura es equivalente a la definición de sucesión puramente periódica.

Lema 1.45

La sucesión s_0, s_1, \dots es puramente periódica si y solo si existen los números enteros $r > 0$, tal que $s_{n+r} = s_n$ para todos los $n = 0, 1, \dots$

Teorema 1.46

Sea \mathbb{F}_q – un campo finito arbitrario, y k cierto número natural. Entonces cada sucesión recurrente lineal de orden k sobre el campo \mathbb{F}_q es periódica. Con esto su período mínimo r satisface la desigualdad $r \leq q^k$, en el caso de una sucesión homogénea la desigualdad $r \leq q^{k-1}$.

Teorema 1.47

Sea s_0, s_1, \dots una sucesión recurrente lineal sobre un campo finito que satisface la relación recurrente lineal (1.1). Si el coeficiente a_0 en (1.1) no es igual a 0, entonces la sucesión s_0, s_1, \dots es puramente periódica.

Teorema 1.48

Sea s_0, s_1, \dots una sucesión recurrente lineal homogénea de orden k sobre el campo \mathbb{F}_q , tal que se cumple la relación (1.2) y $a_0 \neq 0$. Entonces el período mínimo de la sucesión dada divide al orden de la matriz acompañante a ella definida por la fórmula (1.4) y considerada como elemento del grupo lineal general $GL(k, \mathbb{F}_q)$.

De todas las sucesiones recurrentes lineales homogéneas sobre el campo \mathbb{F}_q que satisfacen la relación recurrente lineal de orden k dada del tipo (1.2) se puede separar una sucesión con valor máximo de período mínimo, llamada función impulso. Esta

Capítulo I

sucesión se denota por d_0, d_1, \dots y se determina unívocamente por los valores iniciales $d_0 = \dots = d_{k-2} = 0, d_{k-1} = 1$ ($d_0 = 1$ para $k = 1$) y la relación recurrente

$$D_{n+k} = a_{k-1}d_{n+k-1} + a_{k-2}d_{n+k-2} + \dots + a_0d_n \quad n = 0, 1, \dots \quad (1.10)$$

Lema 1.49

Sea d_0, d_1, \dots una sucesión sobre el campo \mathbb{F}_q que es una función de impulso que satisface la relación recurrente (1.10), y sea A la matriz acompañante a ella del tipo (1.4). Entonces dos vectores de estado d_m y d_n de la sucesión recurrente lineal d_0, d_1, \dots coinciden si y solo si $A^m = A^n$.

Teorema 1.50

El período mínimo de la sucesión recurrente lineal homogénea sobre el campo \mathbb{F}_q divide al período mínimo de la correspondiente función de impulso.

Teorema 1.51

Si la función d_0, d_1, \dots es una función de impulso de orden k sobre el campo \mathbb{F}_q y satisface la relación (1.10) para $a_0 \neq 0$ y A la correspondiente matriz del tipo (1.4), entonces el período mínimo de esta sucesión es igual al orden de la matriz A como elemento del grupo lineal general $GL(k, \mathbb{F}_q)$.

Teorema 1.52

Sea s_0, s_1, \dots una sucesión recurrente lineal homogénea de orden k sobre el campo \mathbb{F}_q , y n_0 es el pre período de esta sucesión. Si existen k vectores de estado $s_{m_1}, s_{m_2}, \dots, s_{m_k}, m_j \geq n_0$ ($1 \leq j \leq k$) los cuales son linealmente independientes sobre \mathbb{F}_q , entonces la propia sucesión s_0, s_1, \dots y su correspondiente función de impulso son puramente periódica y tienen el mismo período mínimo.

Teorema 1.53

Sea s_0, s_1, \dots una sucesión recurrente lineal de orden k sobre un campo \mathbb{F}_q , que satisface la relación recurrente (1.2) y es una sucesión puramente periódica con período

Capítulo I

r . Sea $f(x)$ el polinomio característico de esta sucesión. Entonces tiene lugar la igualdad $f(x)s(x) = (1 - x^r)h(x)$ (1.9) donde

$$s(x) = s_0x^{r-1} + s_1x^{r-2} + \dots + s_{r-2}x + s_{r-1} \in \mathbb{F}_q[x] \quad a_k = -1 \quad (1.11).$$

Teorema 1.54

Si s_0, s_1, \dots es una sucesión recurrente lineal homogénea sobre el campo \mathbb{F}_q con un vector inicial de estado no nulo, sea su polinomio característico $f(x) \in \mathbb{F}_q[x]$ un polinomio irreducible sobre el campo \mathbb{F}_q y que satisface la condición $f(0) \neq 0$. Entonces la sucesión s_0, s_1, \dots es una sucesión puramente periódica y su período mínimo r es igual al $\text{ord}(f(x))$.

Por el Teorema 1.6 $\text{ord}(f(x))$ divide a q^{k-1} .

Para las aplicaciones, las sucesiones recurrentes lineales que tienen período mínimo bastante grande presentan gran interés. Del teorema 1.51 se conoce que para la sucesión recurrente lineal homogénea de orden k sobre el campo \mathbb{F}_q , el período mínimo no puede superar a q^{k-1} . Para construir sucesiones recurrentes con período mínimo exactamente igual a q^{k-1} , utilizamos el concepto de polinomio primitivo (Definición 1.27).

Definición 1.55

La sucesión recurrente lineal homogénea sobre el campo \mathbb{F}_q cuyo polinomio característico es un polinomio primitivo sobre el campo \mathbb{F}_q y su vector de estado inicial es un vector no nulo se llama **sucesión de período máximo** sobre el campo \mathbb{F}_q .

Teorema 1.56

Cada sucesión de orden k y de período máximo sobre el campo \mathbb{F}_q es puramente periódica y su período mínimo es igual a q^{k-1} , el cual es el mayor de los posibles valores que puede tomar el período mínimo de la sucesión recurrente lineal homogénea de orden k sobre el campo \mathbb{F}_q .

Se puede mostrar que para las funciones generatrices es válida la igualdad fundamental siguiente:

Aunque no se había hecho referencia a eso, es evidente que la relación recurrente lineal satisface un conjunto de otras relaciones recurrentes lineales además de aquella que define esta sucesión. Así si la sucesión s_0, s_1, \dots es puramente periódica con período r entonces ella satisface las relaciones recurrentes lineales, $s_{n+r} = s_n$ ($n = 0, 1, \dots$) $s_{n+2r} = s_n$ ($n = 0, 1, \dots$) etc. El caso extremo lo representa la sucesión $0, 0, 0, \dots$ la cual satisface cualquier relación recurrente lineal dada.

El polinomio mínimo juega un papel rector en la definición de período mínimo de la sucesión recurrente lineal. Esto se ve por ejemplo en el siguiente resultado.

Teorema 1.57

Sea s_0, s_1, \dots una sucesión recurrente lineal homogénea sobre el campo \mathbb{F}_q con **polinomio mínimo** $m(x) \in \mathbb{F}_q[x]$ entonces el período mínimo de esta sucesión es igual al $ord(m(x))$.

1.2.4 Sucesiones Recurrentes Lineales Binarias

Es de interés para el presente trabajo las sucesiones recurrentes lineales homogéneas. Además, como se mencionó anteriormente, los campos de importancia en este trabajo, son los campos de característica dos, o sea, \mathbb{F}_{2^k} , puesto que son los de mayor interés criptográfico (Glen, 2002).

Llamaremos **sucesión recurrente lineal binaria de orden k** a una sucesión recurrente lineal del tipo (1.1) donde los elementos pertenecen a \mathbb{F}_2 , o sea,

$$s_{n+k} = a_{k-1}s_{n+k-1} + a_{k-2}s_{n+k-2} + \dots + a_0s_n + a \quad n = 0, 1, \dots$$

donde k es un número natural y $a, a_0, a_1, \dots, a_{k-1}$ son ceros y unos.

Se dice **sucesión recurrente lineal homogénea binaria** de orden k si el término independiente $a = 0$ y **sucesión recurrente lineal no homogénea binaria** de orden k en caso $a = 1$.

Los registros de desplazamiento con retroalimentación lineal constituyen una de las aplicaciones de las sucesiones recurrentes lineales binarias, los cuales se estudian en el próximo capítulo. Estos pueden generar sucesiones recurrentes lineales binarias de

Capítulo I

período máximo, es decir, con período mínimo igual a q^{k-1} . Para construir dichas sucesiones, utilizamos el concepto de polinomio primitivo (Definición 1.27). Luego según la Definición 1.55 el **polinomio característico** $f(x) = x^k - a_{k-1}x^{k-1} - a_{k-2}x^{k-2} - \dots - a_0 \in \mathbb{F}_q[x]$, que se puede escribir sobre el campo $\mathbb{F}_2[x]$: $f(x) = x^k + a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + \dots + a_0$, tiene que ser primitivo, lo cual implica que es irreducible, y por consiguiente $a_0 = 1$.

Según el Teorema 1.47 la sucesión recurrente lineal homogénea sobre este campo es puramente periódica.

Luego la **matriz acompañante** que representa este tipo de sucesión es:

$$A = \begin{pmatrix} 0 & 0 & \dots & 0 & a_0 \\ 1 & 0 & \dots & 0 & a_1 \\ 0 & 1 & \dots & 0 & a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & a_{k-1} \end{pmatrix}$$

Si A es la matriz definida anteriormente, entonces es fácil notar que $f(x)$ coincide con el polinomio característico de la matriz A como él se determina en el álgebra lineal, es decir $f(x) = \det(A - xI)$, donde I es la matriz identidad de orden $k \times k$ sobre el campo \mathbb{F}_2 . Además en \mathbb{F}_2 $f(x) = f(-x)$.

Llamemos al polinomio $f^*(x) = 1 + a_{k-1}x + a_{k-2}x^2 + \dots + x^k \in \mathbb{F}_2[x]$ (1.12) polinomio característico reverso de la sucesión recurrente lineal homogénea binaria. El cual se relaciona con el polinomio característico por la relación $f^*(x) = x^k f(1/x)$.

Por el teorema 1.54 el polinomio característico de la sucesión recurrente lineal homogénea $f(x)$ sobre el campo binario coincide con su polinomio mínimo $m(x)$. Por lo que $\text{ord}(f(x)) = \text{ord}(m(x)) = k$.

En este primer capítulo se realizó un estudio de las sucesiones recurrentes lineales sobre campos finitos. Para ello fue necesario presentar algunos conceptos básicos sobre la teoría de estos tipos de campos, la cual es de gran utilidad para la comprensión de las SRL, particularmente las SRL homogéneas binarias que se utilizan en el siguiente capítulo, puesto que estas son generadas a partir de los LFSRs.

CAPÍTULO II. REGISTROS DE DESPLAZAMIENTO CON RETROALIMENTACIÓN LINEAL

Los registros de desplazamiento, en particular, los registros de desplazamiento con realimentación lineal, son los componentes básicos de muchos generadores de sucesiones binarias pseudoaleatorias. En este capítulo se exponen los principales conceptos sobre estos mecanismos (Menezes, VanOorschot, & Vanstone, 1996).

Este capítulo está compuesto por 5 epígrafes. El primero se dedica a definir los registros de desplazamiento con retroalimentación lineal. El segundo, al período de las sucesiones producidas por los registros de desplazamiento con retroalimentación lineal, haciendo énfasis en el período máximo. En el tercero se describe la relación entre los registros de desplazamiento con retroalimentación lineal y las sucesiones recurrentes lineales. En el cuarto epígrafe se exponen las propiedades de aleatoriedad de las sucesiones de salida de los registros de desplazamiento con retroalimentación lineal, basadas en los postulados de Golomb. El quinto y último epígrafe aborda la complejidad lineal de los LSFRs. Las definiciones y lemas que se presentan se pueden encontrar en (Menezes, VanOorschot, & Vanstone, 1996) y (Golomb, 1982). Se puede complementar el tema utilizando (Bruen & Mollin, 2009) y (Bruen & Mollin, 2009) .

2.1 Registros de desplazamiento con retroalimentación lineal

Los registros de desplazamiento con realimentación lineal (LFSRs) se utilizan en muchos de los generadores de sucesiones binarias que se han propuesto en la literatura. Existen varias razones para esto, entre ellas:

- LFSRs son muy adecuados para la aplicación de hardware;
- Pueden producir sucesiones de período largo;
- Pueden producir sucesiones con buenas propiedades estadísticas;
- Debido a su estructura, pueden ser analizados fácilmente usando técnicas algebraicas.

Capítulo II

Definición 2.2

El LFSR se denota $(L, f(x))$, donde $f(x) = x^L + a_{L-1}x^{L-1} + a_{L-2}x^{L-2} + \dots + a_0 \in \mathbb{Z}_2[x]$ es el **polinomio de conexión (o retroalimentación)**. EL LFSR se dice que es no singular si el grado de $f(x)$ es L .

Donde los exponentes del polinomio, menores que el grado, se corresponden con las etapas que intervienen en el cálculo del valor de retroalimentación. Si el contenido inicial de la etapa j es s_j para cada j , $0 \leq j \leq L - 1$, entonces $[s_0, s_1, \dots, s_{L-1}]$ es llamado estado inicial del LFSR (Menezes, VanOorschot, & Vanstone, 1996).

Lema 2.3

Si el estado inicial del LFSR en la Figura 2.1 es $[s_0, s_1, \dots, s_{L-1}]$, entonces la sucesión de salida $s = s_0, s_1, s_2, \dots$ viene determinada únicamente por la siguiente recurrencia:

$$s_j = (a_1s_{j-1} + a_2s_{j-2} + \dots + a_k s_{j-L}) \text{ mod } 2 \text{ para } j \geq L.$$

Ejemplo 2.4 (Sucesión de salida de un LFSR)

Considere el LFSR $(4, x^4 + x + 1)$ o sea, $f(x) = x^4 + x + 1$ representado en la Figura 2.2. Si el estado inicial del LFSR es $[0, 0, 0, 0]$, la sucesión de salida es la sucesión de ceros. Las siguientes tablas muestran el contenido de los estados x_0, x_1, x_2, x_3 al final de cada unidad de tiempo t cuando el estado inicial es $[0, 1, 1, 0]$.

t	x_3	x_2	x_1	x_0
0	0	1	1	0
1	0	0	1	1
2	1	0	0	1
3	0	1	0	0

t	x_3	x_2	x_1	x_0

Capítulo II

4	0	0	1	0
5	0	0	0	1
6	1	0	0	0
7	1	1	0	0

8	1	1	1	0
9	1	1	1	1
10	0	1	1	1
11	1	0	1	1
12	0	1	0	1
13	1	0	1	0
14	1	1	0	1
15	0	1	1	0

La sucesión de salida es $s = 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, \dots$, y es periódica con período 15 (Teorema 1.55).

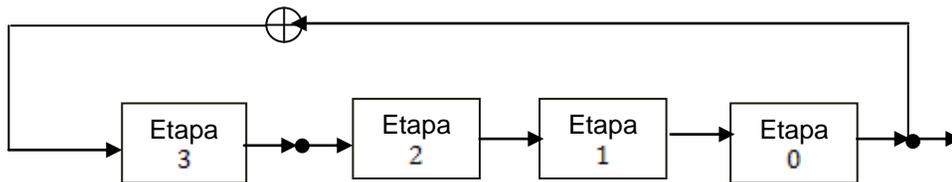


Figura 2.2 LFSR $(4, x^4 + x + 1)$ del Ejemplo 2.4

La importancia de ser un LFSR no singular se explica a través del siguiente lema:

Lema 2.5

Cada sucesión de salida de un LFSR $(L, f(x))$ es periódica si y sólo si el polinomio de conexión $f(x)$ tiene grado L .

Si un LFSR $(L, f(x))$ es singular, (es decir, $f(x)$ tiene grado menor que L), entonces no todas las sucesiones de salida son periódicas. Sin embargo, las sucesiones de salida son periódicas, obviando un cierto número finito de términos al principio. Para el resto de este capítulo, se utilizarán LFSRs no singulares.

2.2 Período de los LFSRs

Definición 2.6

Capítulo II

Si el polinomio característico de una sucesión es irreducible de grado L , el período de la sucesión es un factor de $2^L - 1$ (Golomb, 1982).

Teorema 2.7

La sucesión de estados en un registro de desplazamiento es periódica, con un período $p \leq 2^L - 1$, donde L es el número de estados.

Lema 2.8

Sea $f(x) \in \mathbb{Z}_2[x]$ un polinomio de conexión de grado L .

- i. Si $f(x)$ es irreducible sobre \mathbb{Z}_2 (véase la Definición 1.3), entonces cada uno de los $2^L - 1$ estados iniciales diferentes de cero del LFSR no singular $(L, f(x))$; produce una sucesión de salida con período igual al menor número entero positivo n , tal que, $f(x)$ divide a $1 + x^n$ en $\mathbb{Z}_2[x]$.
- ii. Si $f(x)$ es un polinomio primitivo (véase la Definición 1.27), entonces cada uno de los $2^L - 1$ estados iniciales distintos de cero del LFSR no singular $(L, f(x))$ produce una sucesión de salida con el máximo período posible $2^L - 1$.
- iii. Si $2^L - 1$ es primo, todo polinomio irreducible de grado L se corresponde a una sucesión de período máximo, de un LFSR. En este caso, el único factor de $2^L - 1$ es el propio $2^L - 1$. Cuando $2^L - 1$ es primo, es conocido en la literatura como primo de Mersenne (Golomb, 1982).

Un método para generar polinomios primitivos sobre \mathbb{Z}_2 uniformemente al azar se da en el algoritmo del Anexo 1. La tabla del Anexo 2 lista polinomios primitivos de grado L sobre \mathbb{Z}_2 para cada L , $1 \leq L \leq 229$. El Lema 2.6 (ii) motiva la siguiente definición.

Definición 2.9

Si $f(x) \in \mathbb{Z}_2[x]$ es un polinomio primitivo de grado L , entonces $(L, f(x))$ es llamado un LFSR de longitud máxima. La salida de un LFSR de longitud máxima con estado inicial distinto de cero se denomina una m -sucesión.

2.3 Relación entre los LFSR y las sucesiones recurrentes lineales

En (Menezes, VanOorschot, & Vanstone, 1996) se denota al polinomio cuyos coeficientes coinciden con los coeficientes de retroalimentación, como polinomio de conexión. Mientras que en (Golomb, 1982) a este polinomio se le denota polinomio característico.

La expresión utilizada por cada autor, radica en la forma de representar este polinomio. En (Menezes, VanOorschot, & Vanstone, 1996) se interpretan los coeficientes de retroalimentación como los coeficientes del polinomio de conexión, sin tener en cuenta el coeficiente del término cuyo exponente coincide con el grado polinomio. Mientras que en (Golomb, 1982) se adoptan como coeficientes de retroalimentación los coeficientes del polinomio característico, pero en este caso sin tener en cuenta el coeficiente del término independiente.

En ambas situaciones, se representan los coeficientes de retroalimentación correctamente. Puesto que, al tomar cualquiera de estos dos polinomios, teniendo en cuenta las formas de interpretación de cada uno, se obtienen los mismos coeficientes de retroalimentación. Esto es debido a que el polinomio característico constituye el polinomio reverso del polinomio de conexión.

Un método simple para generar sucesiones binarias es utilizar los registros de desplazamiento con retroalimentación lineal. Las sucesiones generadas son periódicas, con un período que no excede a $2^L - 1$, donde L es el número de etapas del LFSR.

Toda sucesión $\{s_i\}$ generada por un LFSR satisface la relación de recurrencia lineal donde a_i es 1 o 0 de acuerdo con si el valor de la $i - \text{ésima}$ etapa está o no incluido en la retroalimentación.

Si en el análisis de un LFSR es considerada una sola etapa, el método de la función generatriz puede conducir a rápidos resultados.

Función Generatriz en LFSRs

Capítulo II

Sea $\{s_n\} = \{s_0, s_1, s_2, \dots\}$ la sucesión que describe la sucesión de valores que toma la primera etapa, se puede asociar a esta la función generatriz

$$G(x) = \sum_{n=0}^{\infty} s_n x^n$$

Si $\{s_n\}$ satisfice la relación de recurrencia

$$s_n = \sum_{i=1}^L a_i s_{n-i}$$

Denotando los valores iniciales del LFSR como

$$s_{-1}, s_{-2}, \dots, s_{-L}$$

Entonces

$$\begin{aligned} G(x) &= \sum_{n=0}^{\infty} \sum_{i=1}^L a_i s_{n-i} x^n = \sum_{i=1}^L a_i x^i \sum_{n=0}^{\infty} s_{n-i} x^{n-i} \\ &= \sum_{i=1}^L a_i x^i [s_{-i} x^{-i} + \dots + s_{-1} x^{-1} + \sum_{n=0}^{\infty} s_n x^n] \end{aligned}$$

Luego

$$G(x) = \sum_{i=1}^L a_i x^i [s_{-i} x^{-i} + \dots + s_{-1} x^{-1} + G(x)]$$

y

$$G(x) - \sum_{i=1}^L a_i x^i G(x) = \sum_{i=1}^L a_i x^i (s_{-i} x^{-i} + \dots + s_{-1} x^{-1})$$

Más formalmente,

$$G(x) = \frac{\sum_{i=1}^L a_i x^i (x^{-i} + \dots + s_{-1} x^{-1})}{1 - \sum_{i=1}^L a_i x^i}$$

Esto expresa a $G(x)$ completamente en términos de las condiciones iniciales $s_{-1}, s_{-2}, \dots, s_{-L}$ y los coeficientes de retroalimentación. De hecho, el denominador es independiente de las condiciones iniciales donde el polinomio, $1 - \sum_{i=1}^L a_i x^i = x^L + a_{L-1} x^{L-1} + a_{L-2} x^{L-2} + \dots + 1$ se denomina polinomio característico

Capítulo II

de la sucesión recurrente lineal homogénea binaria $\{s_n\}$ como se mencionó en el primer capítulo y es equivalente al polinomio de conexión del LSFR.

De esta forma se obtiene por este método que

$$\sum_{n=0}^{\infty} a_n x^n = \frac{g(x)}{f(x)}$$

donde el numerador es un polinomio de grado menor que L .

Matriz Acompañante en LFSR

Cada estado de un registro desplazamiento de longitud L puede representado como un vector L -dimensional. Luego el registro de desplazamiento puede ser visto como un operador lineal, el cual transforma cada estado en el próximo. Es muy familiar el hecho de que es más conveniente representar un operador lineal, el cual opera sobre vectores L -dimensionales, por una matriz $L \times L$ Véase (Golomb, 1982), (Goresky M., 2012) y (Panario, 2013).

La **matriz acompañante en LSFR** es

$$A = \begin{pmatrix} 0 & 0 & \dots & 0 & a_0 \\ 1 & 0 & \dots & 0 & a_1 \\ 0 & 1 & \dots & 0 & a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & a_{L-1} \end{pmatrix}$$

siendo $f(x) = x^L + a_{L-1}x^{L-1} + a_{L-2}x^{L-2} + \dots + a_0 \in \mathbb{Z}_2[x]$ el **polinomio de conexión del LSFR**.

Con 1s a través de toda la diagonal anterior a la diagonal principal y los coeficientes presentes en la sucesión recurrente lineal en la última columna en orden hacia abajo.

De esta manera se pueden representar los estados del registro hacia atrás de la siguiente forma

$$(s_{n-1}, s_{n-2}, \dots, s_{n-L}) \begin{pmatrix} 0 & 0 & \dots & 0 & a_0 \\ 1 & 0 & \dots & 0 & a_1 \\ 0 & 1 & \dots & 0 & a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & a_{L-1} \end{pmatrix}$$

Capítulo II

$$= (s_{n-2}, s_{n-3}, \dots, s_{n-L}, a_0 s_{n-1} + a_1 s_{n-2} + \dots + a_{L-1} s_{n-L-1})$$

$$= (s_{n-2}, s_{n-3}, \dots, s_{n-L-1})$$

La ecuación característica de la matriz A es:

$$f(x) = \det |A - xI| = \begin{vmatrix} -x & 0 & \dots & 0 & a_0 \\ 1 & -x & \dots & 0 & a_1 \\ 0 & 1 & \dots & -x & a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & a_{L-1} - x \end{vmatrix}$$

Para calcularlo, desarrollando el determinante por la n -sima columna, veamos cual es el complemento algebraico de cada componente a_L , situado en el lugar $(L-1, n)$, para L desde 0 hasta $n-2$. En general, el determinante a calcular tiene la forma:

$$\begin{vmatrix} \begin{vmatrix} -x & 0 & 0 & \dots & 0 \\ 1 & -x & 0 & \dots & 0 \\ 0 & 1 & -x & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & -x \end{vmatrix} & \begin{vmatrix} 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 0 \end{vmatrix} & \begin{vmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_{L-1} \end{vmatrix} \\ \begin{vmatrix} 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 \end{vmatrix} & \begin{vmatrix} -x & 0 & 0 & \dots & 0 \\ 1 & -x & 0 & \dots & 0 \\ 0 & 1 & -x & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & -x \end{vmatrix} & \begin{vmatrix} a_L \\ a_{L+1} \\ a_{L+2} \\ \vdots \\ a_{n-2} \\ a_{n-1} - x \end{vmatrix} \end{vmatrix}$$

El complemento algebraico del elemento c_L , situado en el lugar $(L-1, n)$, es igual a $(-1)^{L+1+n}$ por el menor que resulta de suprimir la fila $L+1$ y la columna n . No es difícil notar que al suprimirse esa fila y esa columna los unos de la subdiagonal en la submatriz inferior derecha suben a la diagonal quedando el determinante

Capítulo II

$$\begin{vmatrix} -x & 0 & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\ 1 & -x & 0 & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\ 0 & 1 & -x & \dots & 0 & 0 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \dots & \dots & \dots & \dots & \dots & \vdots \\ 0 & 0 & 0 & \dots & -x & 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 & 1 & -x & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 & 0 & 1 & -x & 0 & 0 \\ 0 & 0 & 0 & \dots & 0 & 0 & 0 & 1 & -x & 0 \\ \vdots & \vdots & \vdots & \dots & 0 & 0 & 0 & 0 & 1 & -x \\ 0 & 0 & 0 & \dots & 0 & 0 & 0 & 0 & 0 & 1 \end{vmatrix}$$

cuyo valor es $(-x)^L = (-1)^L x^L$. De aquí resulta que el complemento algebraico de a_L es $(-1)^{L+1+n} (-1)^L x^L = (-1)^{n+1} x^L = (-1)^n (-x^L)$. Luego, el término correspondiente, en el desarrollo por la n -ésima columna, es $(-1)^n (-a_L x^L)$.

Por otra parte, el complemento algebraico del elemento $a_{n-1} - x$, situado en el lugar (n, n) , es igual a $(-1)^{n+n} (-x)^{n-1} = (-1)^{n-1} (x)^{n-1} = (-1)^n (-x^n)$. De aquí resulta que el término resultante en el desarrollo por la n -ésima columna es igual a $(a_{n-1} - x)(-1)^n (-x^{n-1}) = (-1)^n (-a_{n-1} x^{n-1} + x^n)$

De todo lo anterior resulta que el determinante de la matriz polinomial $A - xI$ es igual a $(-1)^n (-a_0 - a_1 x - a_2 x^2 - \dots - a_L x^L \dots - a_{n-2} x^{n-2} - a_{n-1} x^{n-1} + x^n)$

Es claro que, para n par este es ya el polinomio mónico buscado, mientras que si n es impar es el opuesto del mismo. Como estamos trabajando sobre campos binarios entonces $f(x) = f(-x)$ lo que implica que siempre obtenemos el polinomio primitivo buscado.

Se tiene pues que, en todos los casos, el polinomio característico de la matriz A es:

$$f(x) = x^n + a_{n-1} x^{n-1} + \dots + a_L x^L + \dots + a_1 x + a_0$$

Determinando el período del LSFR

Determinar el período del LFSR es equivalente, excepto en casos degenerados, a encontrar la menor potencia p de la matriz A , tal que, $A^p = I$, la matriz identidad.

Capítulo II

Un teorema bien conocido de la teoría de las matrices afirma que toda matriz formalmente satisface su ecuación característica (Golomb, 1982): así, $f(A) = 0$. Si $f(x)$ divide a $1 + x^p$, entonces A es una raíz de $I - X^p = 0$, puesto que es una raíz del factor $f(X) = 0$. Es decir, si $f(x)$ divide a $1 + x^p$, entonces $A^p = I$. Inversamente, si $f(x)$ es irreducible, divide a todo polinomio que posee a A como raíz en común con él y dividirá a $1 + x^p$, si $A^p = I$.

2.4 Propiedades de pseudoaleatoriedad en las sucesiones de los LFSRs

En este epígrafe estudiaremos los postulados de Golomb (Golomb, 1982) y (Tilborg, 2005).

Postulado R-1

Suponiendo un registro de L etapas, el cual posee $2^L - 1$ posibles estados antes de la repetición, estos estados constituyen los enteros desde 1 hasta $2^L - 1$, en notación binaria. La sucesión de salida $\{s_n\}$ del registro de desplazamiento puede ser vista como los *bits de paridad* de los números desde 1 hasta $2^L - 1$. Es decir, el bit de paridad es 1 si el número es impar y es 0 si el número es par. Desde 1 hasta $2^L - 1$ existen 2^{L-1} números impares y $2^{L-1} - 1$ números pares, de esta manera, en una sucesión de salida de máxima longitud de un registro de desplazamiento, existen 2^{L-1} unos y $2^{L-1} - 1$ ceros.

Teorema 2.10

El postulado R-1 se sostiene para toda sucesión de salida de máxima longitud de un registro de desplazamiento.

Transformando la sucesión de salida $\{s_n\}$ de 0s y 1s, en una sucesión $\{s\}$ de 1s y -1s, mediante la transformación $s = 1 - 2s_n$, en cualquier período p , el número de 1s es casi igual al número de -1s (Precisamente la disparidad no debe exceder en 1). Es decir,

$$\sum_{n=1}^p s_n \leq 1$$

Capítulo II

Postulado R-2

En una sucesión de salida de longitud máxima $\{s_n\}$ de un registro de desplazamiento de L etapas, existen $2^L - 1$ vías para escoger L términos consecutivos. Es decir, cada estado de L términos consecutivos ocurre exactamente una sola vez, excepto el estado con todas las etapas en 0.

En particular, L unos consecutivos ocurren una sola vez. Esta corrida de 1s debe estar precedida y seguida de un 0 o existirían otras corridas de L unos consecutivos. Un 0 seguido de $L - 1$ unos ocurre exactamente una vez, este caso está fuertemente ligado al caso anterior debido a que este ocurre cuando L unos son precedidos por un cero. Similarmente, $L - 1$ unos seguidos de un cero ocurren también una sola vez y está basado en el hecho de que L unos deben ser continuados por un cero.

Suponiendo $0 < k < L - 1$. Para encontrar el número de corridas de unos de longitud k , considerando L términos consecutivos comenzando por 0, entonces L unos, luego un cero y los restantes $L - k - 2$ términos arbitrarios. Estas ocurren 2^{L-k-2} veces, puesto que, cada completamiento $L - k - 2$ términos arbitrarios ocurre solo una vez.

Con un razonamiento análogo se puede determinar el número de corridas de ceros de longitud k , $0 < k < L - 1$. No existe una corrida de L ceros consecutivos, puesto que, esto “terminaría” el funcionamiento del registro. De esta manera, un 1 seguido de $L - 1$ ceros debe ocurrir, por lo que existe una corrida de $L - 1$ ceros.

De esta forma la estructura de una sucesión de longitud máxima de está completamente determinada como corridas de unos (llamados bloques) y corridas de unos (llamados huecos).

Si $0 < k < L - 1$, existen 2^{L-k-2} bloques e igual número de huecos de longitud k . Además, existe un hueco de longitud $L - 1$ y un bloque de longitud L .

En términos del período n de la sucesión ($n = 2^L - 1$), existen $(n + 1)/2$ corridas, la mitad de estas bloques y la otra huecos. De los bloques, la mitad es de longitud 1, $1/4$ es de longitud 2, $1/8$ es de longitud 3, etc. e igualmente para los huecos. Este

Capítulo II

procedimiento continúa hasta que existe un bloque y un hueco de longitud $L - 2$. A partir de aquí, existe un hueco de longitud $L - 1$ y un bloque de longitud L .

Teorema 2.11

El postulado R-2 se sostiene para toda sucesión de salida de máxima longitud de un registro de desplazamiento.

Sucesiones de salida de registros de desplazamiento como grupo abeliano

Sea $S_1 = \{s_1, s_2, s_3, \dots\}$ una sucesión de longitud máxima de un registro de desplazamiento con período $n = 2^L - 1$. Sea $S_2 = \{s_2, s_3, s_4, \dots\}$, $S_3 = \{s_3, s_4, s_5, \dots\}$, ..., $S_p = \{s_p, s_{p+1}, s_{p+2}, \dots\}$ y $S_0 = \{0, 0, 0, \dots\}$.

Definición 2.12

Un grupo abeliano G CITATION JAV09 \l 1033 | (Mendoza, 2009)} es un conjunto de elementos que satisfacen:

- La suma de cualquiera dos elementos de G se encuentra en G .
- Para cualquier a, b, c en G , $a + b = b + a$ y $(a + b) + c = a + (b + c)$.
- Existe un elemento 0 que satisface que $a + 0 = a$ para cualquier a en G .
- Todo elemento a tiene un negativo \bar{a} , tal que $a + \bar{a} = 0$.

Nota: Para el grupo abeliano multiplicativo, reemplazar la suma por el producto, el elemento 0 por el 1 y el negativo por el recíproco.

Teorema 2.13

Las sucesiones S_0, S_1, \dots, S_p , forman un grupo abeliano con respecto a la operación de adición de elementos sobre campos binarios (mod 2) a nivel de término (Esta adición módulo 2 a nivel de término significa que si $B = \{b_1, b_2, b_3, \dots\}$ y $A = \{a_1, a_2, a_3, \dots\}$ entonces $B + A = \{b_1 + a_1, b_2 + a_2, b_3 + a_3, \dots\}$).

Postulado R – 3

Sea $\{b_n\}$ la sucesión resultante de aplicar la transformación utilizada en el primer postulado a la sucesión $\{s_n\}$. Es decir, los 0s son reemplazados por 1s y los 1s por -1s. Otra transformación pudiera ser, $b_n = e^{i\pi s_n}$.

Sea S_0, S_1, \dots, S_n , definida anteriormente. Realizando el reemplazo de 0s por 1s y 1s por -1s para obtener las sucesiones B_0, B_1, \dots, B_n . Entonces la adición de elementos sobre el campo de las S_i es la misma que la multiplicación de las B_i . Esto queda claro a partir de las tablas de suma y multiplicación.

Puesto que $A_i + A_j = A_k$, se sigue que $B_i B_j = B_k$, donde el producto $B_i B_j$ es tomado término a término. Luego, menos para $B_k = B_0 = \{1, 1, 1, \dots\}$, lo cual sucede solo si $i = j$, B_k contiene $(n - 1)/2$, 1s y $(n + 1)/2$, (-1) s.

De esta forma la función de autocorrelación de $\{b_n\}$ es

$$A(\tau) = \frac{1}{p} \sum_{n=1}^p b_n b_{n+\tau} = \begin{cases} 1 & \text{si } \tau = 0 \\ -\frac{1}{p} & \text{si } 0 < \tau < p \end{cases}$$

porque $\{b_n b_{n+\tau}\}$ es una sucesión de tipo $B_i B_j$, el cual en es de tipo B_k , y el exceso de 1s y -1s es n para B_0 y -1 de lo contrario.

Teorema 2.14

Toda sucesión de salida de máxima longitud de un registro de desplazamiento satisface el postulado R-3.

Definición 2.15

Sea s una m -sucesión que se genera por un LFSR de longitud máxima de longitud L . La sucesión s satisface los postulados de aleatoriedad de Golomb (Golomb, 1982). Esto es, cada m -sucesión es también una PN – sucesión (Pseudo-Noise sequence).

Una PN – sucesión está definida como una sucesión recurrente lineal de longitud máxima sobre elementos de campos binarios. Es decir, $\{s_L\}$ es una PN – sucesión si y solo si es una sucesión binaria que satisface la recurrencia lineal

$$s_k = \sum_{i=1}^L a_i s_{k-i} \pmod{2}$$

y posee período $n = 2^L - 1$. El número L constituye el grado de la PN – sucesión.

El polinomio $f(x) = 1 + \sum a_i x^i \pmod{2}$ es llamado polinomio característico de la sucesión $\{s_L\}$. Una condición necesaria para que $\{s_L\}$ sea considerada una PN -sucesión es que $f(x)$ sea irreducible. Una condición necesaria y suficiente es que $f(x)$ divida a $1 - x^m$ para $m = n$, pero no para un entero positivo m menor que n .

2.5 Complejidad lineal y LFSR

En este trabajo todas las sucesiones se asumen que son sucesiones binarias. Podemos encontrar lo relacionado a este epígrafe en (Zenner, 2004) y (Jansen & Boeke, 1998).

Notación: s denota una sucesión infinita cuyos términos son s_0, s_1, s_2, \dots ;

Capítulo II

s^n indica una sucesión finita de longitud n cuyos términos son s_0, s_1, \dots, s_{n-1} .

Definición 2.16

Se dice que un LFSR para generar una sucesión s si hay algún estado inicial para el que la sucesión de salida del LFSR es s . De manera similar, se dice que un LFSR para generar una sucesión finita s^n si hay algún estado inicial para el que la sucesión de salida del LFSR tiene como su primera n a términos.

Definición 2.17

La complejidad lineal de una sucesión binaria infinita s , denotado $L(s)$, se define de la siguiente manera:

- I. Si s es la sucesión cero $s = 0,0,0, \dots$, entonces $L(s) = 0$.
- II. Si LFSR no genera s , entonces $L(s) = \infty$.
- III. De otro modo, $L(s)$ es la longitud del LFSR más pequeño que genera s .

Definición 2.18

La complejidad lineal de una sucesión binaria finita s^n , denotada $L(s^n)$, es la longitud del LFSR más pequeño que genera una sucesión que tiene s^n como sus primeros n términos.

A continuación se resumen algunos resultados básicos acerca de la complejidad lineal.

Propiedades de complejidad lineal

Sea s y t sucesión binarias:

- I. Para cualquier $n \geq 1$, la complejidad lineal de las subsucesión a s^n satisface $0 \leq L(s^n) \leq n$
- II. $L(s^n) = 0$ si y sólo si s^n es la sucesión cero de longitud n .
- III. $L(s^n) = n$ si y sólo si $s^n = 0,0,0, \dots, 0,1$.
- IV. Si s es periódica con período N , entonces $L(s) \leq N$.
- V. $L(s \oplus t) \leq L(s) + L(t)$, donde $s \oplus t$ denota la operación XOR de los bits de s y t .

Capítulo II

Si el polinomio $C(D) \in \mathbb{Z}_2[D]$ es irreducible sobre \mathbb{Z}_2 y tiene grado L , entonces cada $2^L - 1$ distintos de cero los estados iniciales del LFSR no singular; $\langle L, C(D) \rangle$ produce una sucesión de salida con una complejidad lineal L .

El perfil de la complejidad lineal de una sucesión binaria se enuncia a continuación.

Definición 2.19

Sea $s = s_0, s_1, \dots$ una sucesión binaria, y L_N denota la complejidad lineal de la subsucesión $s^N = s_0, s_1, \dots, s_{N-1}, N \geq 0$.

La sucesión L_1, L_2, \dots , se denomina **el perfil de complejidad lineal** de s . Del mismo modo, si $s^n = s_0, s_1, \dots, s_{n-1}$ es una sucesión binaria finita, la sucesión L_1, L_2, \dots, L_n se denomina el perfil complejidad lineal de s^n .

El perfil de la complejidad lineal de una sucesión puede ser calculada usando el algoritmo de Berlekamp-Massey.

Propiedades del perfil de complejidad lineal

Si L_1, L_2, \dots es el perfil de la complejidad lineal de una sucesión $s = s_0, s_1, \dots$.

- I. Si $j > i$, entonces $L_j \geq L_i$
- II. $L_{N+1} > L_N$, es posible sólo si $L_N \leq N/2$
- III. Si $L_{N+1} > L_N$, entonces, $L_{N+1} + L_N = N + 1$

El perfil de la complejidad lineal de una sucesión s se puede graficar mediante el trazado de los puntos $(N, L_N), N \geq 1$, en el plano $N \times L$ y que une los puntos sucesivos por una línea horizontal seguida por una línea vertical.

Las propiedades anteriores pueden ser interpretadas diciendo que la gráfica de un perfil de complejidad lineal es no decreciente. Por otra parte, un salto (vertical) en el gráfico sólo puede ocurrir por debajo de la línea de $L = N/2$; si se produce un salto, entonces es simétrica respecto a esta línea. La siguiente definición muestra que la complejidad lineal esperada de una sucesión aleatoria debe seguir de cerca la línea $L = N/2$.

Algoritmo de Berlekamp-Massey

El algoritmo de Berlekamp-Massey es un algoritmo eficiente para la determinación de la complejidad lineal de una sucesión binaria finita s de longitud n .

El algoritmo toma n iteraciones, con N iteración del cálculo de la complejidad lineal de la subsucesión s^N que consiste en los primeros N términos de s^N . Las bases teóricas para el algoritmo son:

Definición 2.20

Considere la sucesión binaria finita $S^{N+1} = s_0, s_1, \dots, s_{N-1}, s_N$.

Para $C(D) = 1 + c_1D + \dots + c_L D^L$, sea $\langle L, C(D) \rangle$ un LFSR que genera la subsucesión $s^N = s_0, s_1, \dots, s_{N-1}$

La siguiente discrepancia d_n es la diferencia entre s_N y los $(N + 1)$ términos generados por el LFSR: $d_n = (s_N + \sum_{i=1}^L a_i s_{N-i}) \text{ mod } 2$.

Sea $S^{N+1} = s_0, s_1, \dots, s_{N-1}, s_N$ una sucesión binaria finita de complejidad lineal $L = L(s^N)$, y sea $\langle L, C(D) \rangle$ un LFSR que genera s^N .

- I. El LFSR $\langle L, C(D) \rangle$ también genera $S^{N+1} = s_0, s_1, \dots, s_{N-1}, s_N$ si y sólo si la siguiente discrepancia $d_n = 0$.
- II. Si $d_n = 0$, entonces $L(s^N) = L$.
- III. Supongamos $d_n = 1$. Sea m el mayor entero $< N$ tal que $L(s^m) < L(s^N)$, y sea $\langle L(s^m), B(D) \rangle$ un LFSR de longitud $L(s^m)$ que genera s^m . Entonces $\langle L', C'(D) \rangle$ es un LFSR de longitud más pequeña que genera s^{N+1} , donde

$$L' = \left\{ \begin{array}{ll} L, & \text{si } L > \frac{N}{2} \\ N + 1, & \text{si } L \leq N/2 \end{array} \right\}$$

Algoritmo Berlekamp-Massey: (Menezes, VanOorschot, & Vanstone, 1996)

ENTRADA: Una sucesión binaria $s^n = s_0, s_1, s_2, \dots, s_{n-1}$, de longitud n .

SALIDA: La complejidad lineal $L(s^n)$ de s^n , $0 \leq L(s^n) \leq n$.

1. *Inicialización.* $C \leftarrow 1$, $L \leftarrow 0$, $m \leftarrow -1$, $B(D) \leftarrow 1$, $N \leftarrow 0$.

Capítulo II

2. **Mientras** $(N < n)$ **haga lo siguiente:**

2.1 *Calcule la siguiente discrepancia* d . $d \leftarrow (s_N + \sum_{i=1}^L c_i s_{N-i}) \bmod 2$.

2.2 **Si** $d = 1$ **luego haz lo siguiente:**

$T(D) \leftarrow C(D), C(D) \leftarrow C(D) + B(D) \cdot D^{N-m}$.

Si $L \leq N/2$ **entonces** $L \leftarrow N + 1 - L, m \leftarrow N, B(D) \leftarrow T(D)$.

2.3 $N \leftarrow N + 1$.

3. **Retornar** (L) .

En el presente capítulo hemos estudiado una herramienta para construir criptosistemas de cifrado en flujo: los LSFRs, algunas propiedades importantes y su relación con las SRL que nos lleva a hacer un análisis criptográfico de los LSFRs, en el siguiente Capítulo tres.

CAPÍTULO III. ANÁLISIS CRIPTOGRÁFICO DE LOS LFSR

El presente capítulo está conformado por 4 epígrafes. En el primero se exponen los conceptos básicos de cifrado en flujo. El segundo, se dedica a los ataques de texto claro conocido. El tercero, plantea cómo obtener los polinomios primitivos de los registros de desplazamiento con retroalimentación lineal a partir del conocimiento de parte de la salida. El cuarto, y último epígrafe, de este capítulo plantea un procedimiento para la recuperación del estado inicial del registro.

3.1 Cifrado en flujo

Como se mencionó anteriormente, el cifrado en flujo se realiza bit a bit, mediante el texto claro y la sucesión aleatoria generada.

Véase (López, 2009), (Schneier, 1) y (Brien & Mollin, 2009)

Definición 3.1

Sea $x_i, y_i, s_i \in \{0,1\}$ los bits de texto claro, texto cifrado y la sucesión aleatoria generada, respectivamente. El cifrado y descifrado en flujo consiste en:

$$\text{Cifrado: } y_i = C_{s_i}(x_i) \equiv x_i + s_i \text{ mod } 2$$

$$\text{Descifrado: } x_i = D_{s_i}(y_i) \equiv y_i + s_i \text{ mod } 2$$

Las función fueron denotadas de manera diferente pero, como se puede observar existe una similitud entre estas. La razón de la similitud de la función de cifrado y descifrado se puede mostrar fácilmente. Debemos demostrar que la función de descifrado realmente produce el bit de texto en claro x_i . Se sabe que el bit y_i de texto cifrado fue obtenido utilizando la función de cifrado $y_i \equiv x_i + s_i \text{ mod } 2$. Insertamos la expresión de cifrado en la función de descifrado:

$$\begin{aligned} D_{s_i}(y_i) &\equiv y_i + s_i \text{ mod } 2 \\ &\equiv (x_i + s_i) + s_i \text{ mod } 2 \\ &\equiv x_i + s_i + s_i \text{ mod } 2 \\ &\equiv x_i + 2s_i \text{ mod } 2 \end{aligned}$$

Capítulo III

$$\equiv x_i + 0 \text{ mod } 2$$

$$\equiv x_i \text{ mod } 2$$

de esta forma queda demostrado.

Los cifrados de flujo actuales utilizan una sucesión de bits de clave s_1, s_2, \dots generada por un generador de sucesiones pseudoaleatorias que debe tener ciertas propiedades (Como los postulados mencionados en el capítulo anterior). Una manera sencilla de producir sucesiones pseudoaleatorias grandes es utilizar los LFSRs. Los LFSRs se implementan fácilmente en hardware y muchos, pero no todos, de los cifrados de flujo, hoy por hoy, hacen uso de estos. Un ejemplo destacado es el sistema de cifrado A5 / 1 (Biham & Dunkelman, 2000), que está estandarizado para el cifrado de voz en las redes del Sistema Global de la Comunicaciones Móviles (GSM) (Siegmund M. Redl, 1995). Como veremos en este capítulo, a pesar de que un LFSR produce sucesiones con buenas propiedades estadísticas, estos son criptográficamente débiles.

En la actualidad la mayoría de los algoritmos son públicos, por lo que se pueden conocer las características de los mismos y sus vulnerabilidades. Por esta razón, es posible conocer la longitud de los registros de desplazamiento con retroalimentación lineal.

No obstante, si el algoritmo es secreto es posible conocer este dato, mediante la utilización de la ingeniería inversa, si este está implementado en hardware, lo cual es muy frecuente en la utilización de los LFSRs. Tal es el caso del algoritmo mencionado, A5/1. Mientras que, si está implementado en software es posible conocer este parámetro teniendo en cuenta el almacenamiento requerido.

Incluso los propios polinomios utilizados para retroalimentación pueden ser públicos, pero es recomendado que se mantenga como parámetros secretos.

3.2 Ataques de texto claro conocido

Como lo indica su nombre, los LFSRs son lineales. Los sistemas lineales se rigen por relaciones lineales entre sus entradas y salidas. Puesto que, las dependencias lineales pueden ser relativamente fáciles de analizar, esto puede ser una gran ventaja, por

ejemplo, en sistemas de comunicación. Sin embargo, un criptosistema donde los bits de la llave sólo intervienen en relaciones lineales hace a un cifrado altamente inseguro. Ahora vamos a investigar cómo el comportamiento lineal de un LFSR conduce a un ataque poderoso (Guarino, 2010) y (Kholosha, 2003).

Si utilizamos un LFSR para cifrado de flujo, la llave secreta S es el estado inicial de registro, es decir, el vector $(s_{L-1}, \dots, s_1, s_0)$. Un ataque posible, es el ataque de texto claro conocido donde un atacante conoce algunos pares de texto claro y su texto cifrado correspondiente. Se puede suponer, además, que el atacante conoce la longitud L del LFSR. El ataque es tan eficiente que se puede tratar fácilmente un gran número de valores posibles L , de manera que esta suposición no es una restricción importante. Sea $x_0, x_1, \dots, x_{2L-1}$ el texto claro conocido y $y_0, y_1, \dots, y_{2L-1}$ el texto cifrado correspondiente. Con estos pares de $2L$ bits de texto claro y texto cifrado, un atacante puede reconstruir $2n$ bits de la sucesión aleatoria generada para el cifrado en flujo:

$$s_i \equiv x_i + y_i \pmod{2}; \quad i = 0, 1, \dots, 2L - 1.$$

Para el desarrollo de este epígrafe nos plantearemos la siguiente problemática, un criptoanalista está trabajando para descifrar determinada información, para ello realiza el ataque del texto claro conocido, interceptando los caracteres que se pueden inferir fácilmente de acuerdo al momento y las circunstancias en que esta operación se realice.

Ejemplo 3.2

- a. Si el mensaje a cifrar posee referencia a direcciones web es muy común la presencia de los caracteres `http:\`, `ftp:\`, `https:\`, u otras directivas de comunicación, lo cual puede ser utilizado para realizar estos ataques.

Para llegar al estado inicial necesitamos conocer $2L$ salidas sucesivas, siendo L la longitud del registro de desplazamiento con retroalimentación lineal, que se conoce por ser la mayoría de los algoritmos públicos.

De esta manera, la sucesión obtenida mediante este ataque, como subsucesión de una SRL homogénea binaria producida por un LFSR, la denotaremos por

$$s = s_i, s_{i+1}, s_{i+2}, s_{i+3}, \dots, s_{i+L}, s_{i+L+1}, \dots, s_{(i+L)+L-1}$$

siendo i el instante de tiempo en que se obtuvo dicha salida $i \in [0, 2^L - 2]$ y L el grado del polinomio de conexión

$$f(x) = x^L + a_{L-1}x^{L-1} + a_{L-2}x^{L-2} + \dots + 1$$

del registro, que coincide con la longitud del mismo por la Definición 2.6, que como se dijo al inicio del capítulo se conoce por ser la mayoría de los algoritmos de llave pública. A través de esta subsucesión se puede obtener el estado inicial, obteniendo la llave secreta, y de esta forma reconstruir la sucesión completa determinando todo el texto claro.

3.3 Obtención del polinomio primitivo de los LFSRs

En la búsqueda del estado inicial $[s_0, s_1, \dots, s_{L-1}]$ necesitamos obtener, utilizando el ataque de texto claro conocido, el polinomio de conexión del registro de desplazamiento con retroalimentación lineal. Los coeficientes de dicho polinomio coinciden con los de la sucesión recurrente lineal que representa. Para hallarlo es necesario una parte de la sucesión de salida de $2L$ elementos consecutivos, siendo L el grado del polinomio de conexión. Para la aplicación de este método no es necesario conocer el instante de tiempo donde comienza la sucesión de $2L$ elementos consecutivos, o sea, i .

Por la definición (1.33) de recurrencia lineal podemos obtener el siguiente sistema de ecuaciones expresado en función de términos conocidos por el epígrafe anterior, siendo $a_j, 0 \leq j \leq L - 1$ las incógnitas:

$$s_{i+L} = a_{L-1}s_{i+L-1} + a_{L-2}s_{i+L-2} + a_{L-3}s_{i+L-3} + \dots + a_0s_i$$

$$s_{i+L+1} = a_{L-1}s_{i+L} + a_{L-2}s_{i+L-1} + a_{L-3}s_{i+L-2} + \dots + a_0s_{i+1}$$

$$s_{i+L+2} = a_{L-1}s_{i+L+1} + a_{L-2}s_{i+L} + a_{L-3}s_{i+L-1} + \dots + a_0s_{i+2}$$

⋮

$$s_{(i+L)+L-1} = a_{L-1}s_{(i+L)+L-2} + a_{L-2}s_{(i+L)+L-3} + a_{L-3}s_{(i+L)+L-4} + \dots + a_0s_{i+L-1}$$

Capítulo III

Como podemos ver, siempre es posible expresar el estado actual en función de los anteriores. Si la longitud del registro no es muy grande, los cálculos se pueden hacer fácilmente a mano, resolviendo un reducido sistema de ecuaciones por alguno de los métodos clásicos conocidos, como sustitución o reducción y en ocasiones hasta por tanteo. Esto se complica a medida que la longitud aumente. Cuando esto ocurre dicho sistema se puede resolver fácilmente por el método de Gauss (véase (Arachchige, 1991) y (Yoshiyasu Takefusi, 1983)) el cual está implementado por el LCA de nuestra universidad. Este nos elimina todo tipo de complicación, se ponen ceros o unos en dependencia de si se encuentran o no los términos de la sucesión recurrente lineal homogénea que le anteceden a la subsucesión obtenida, como ya hemos mencionado, por un ataque de texto claro conocido y se aplica el método de Gauss. De esta forma se obtienen los coeficientes a_0, a_1, \dots, a_{L-1} , del polinomio de conexión del registro de desplazamiento con retroalimentación lineal y con esto el polinomio característico asociado a la relación recurrente lineal (1.2), que según lo planteado en la cuarta sección del epígrafe dos correspondiente al primer capítulo, $f(x) = \det(A - xI)$, donde I es la matriz identidad de orden $L \times L$ sobre el campo \mathbb{F}_2 y la matriz A se puede considerar como la matriz acompañante del polinomio mónico $f(x)$, la cual, según la sección cuatro del epígrafe dos del capítulo 1, se representa como sigue:

$$A = \begin{pmatrix} 0 & 0 & \dots & 0 & 1 \\ 1 & 0 & \dots & 0 & a_1 \\ 0 & 1 & \dots & 0 & a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & a_{L-1} \end{pmatrix}$$

Donde los $a_j \in \mathbb{F}_2$, por tanto son ceros y unos.

Ejemplo 3.3

Tenemos el siguiente registro de desplazamiento con retroalimentación lineal $(5, f(x))$

Para encontrar el polinomio de conexión, como habíamos dicho, necesitamos una subsucesión de salida de $2L$ elementos obtenidas por el ataque de texto claro conocido.

Capítulo III

Sea $s = 1,0,0,0,1,1,0,1,1,1$ dicha subsucesión. Luego se tiene,

$$\begin{array}{cccccc|ccccc} 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ s_i & s_{i+1} & s_{i+2} & s_{i+3} & s_{i+4} & s_{i+5} & s_{i+6} & s_{i+7} & s_{i+8} & s_{i+9} \end{array}$$

Planteando el sistema de ecuaciones dado en el epígrafe anterior tendríamos:

$$s_{i+5} = a_4 s_{i+4} + a_3 s_{i+3} + a_2 s_{i+2} + a_1 s_{i+1} + a_0 s_i$$

$$s_{i+6} = a_4 s_{i+5} + a_3 s_{i+4} + a_2 s_{i+3} + a_1 s_{i+2} + a_0 s_{i+1}$$

$$s_{i+7} = a_4 s_{i+6} + a_3 s_{i+5} + a_2 s_{i+4} + a_1 s_{i+3} + a_0 s_{i+2}$$

$$s_{i+8} = a_4 s_{i+7} + a_3 s_{i+6} + a_2 s_{i+5} + a_1 s_{i+4} + a_0 s_{i+3}$$

$$s_{i+9} = a_4 s_{i+8} + a_3 s_{i+7} + a_2 s_{i+6} + a_1 s_{i+5} + a_0 s_{i+4}$$

Sustituyendo nos queda el reducido sistema:

$$1 = a_4 + a_0$$

$$0 = a_4 + a_3$$

$$1 = a_2 + a_1$$

$$1 = a_4 + a_2 + a_1$$

$$1 = a_4 + a_3 + a_1 + a_0$$

Resolviendo el mismo se obtiene

$$a_4 = 0$$

$$a_3 = 0$$

$$a_2 = 1$$

$$a_1 = 0$$

$$a_0 = 1$$

Y calculando

$$f(x) = \det(A - xI)$$

Siendo

$$I = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}_{5 \times 5}$$

Y

$$A = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}_{5 \times 5}$$

Obtenemos el polinomio de conexión

$$f(x) = x^5 + x^2 + 1$$

3.4 Procedimientos para la recuperación del estado inicial de los LFSR

Luego de haber obtenido el polinomio de conexión podemos hacer uso de estudios realizados en los capítulos anteriores. En el primer capítulo hablamos de matriz acompañante, la misma nos es de gran utilidad para recuperar el estado inicial del registro de desplazamiento con retroalimentación lineal.

$$\text{Sea } A = \begin{pmatrix} 0 & 0 & \dots & 0 & 1 \\ 1 & 0 & \dots & 0 & a_1 \\ 0 & 1 & \dots & 0 & a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & a_{L-1} \end{pmatrix}$$

la matriz acompañante a la sucesión recurrente lineal homogénea binaria.

Para todo vector de estado se verifica en la SRL homogénea que $s_i = s_0 A^i$ (Lema 1.39), entonces despejando s_0 obtenemos

$$s_0 = s_i(A^i)^{-1}$$

De esta manera obtenemos el vector de estado inicial, siendo i el instante de tiempo que se obtuvo la sucesión, $0 \leq i \leq 2^L - 1$.

Ejemplo 3.4

Utilizando el resultado del ejemplo anterior y conociendo el instante de tiempo en que se comenzó a generar dicha subsucesión ($i = 10$) podemos recuperar el estado inicial $[s_0, s_1, \dots, s_{L-1}]$. El registro de desplazamiento con retroalimentación lineal ($5, x^5 + x^2 + 1$) que mostramos es no singular. Cada uno de los posibles estados iniciales del registro no singular produce una sucesión recurrente lineal homogénea sobre el campo binario (sucesión de salida) de posible período máximo por el Lema 2.6 ya que $f(x) = x^5 + x^2 + 1$ es un polinomio primitivo, por lo tanto su período sería:

$$n = 2^5 - 1 = 31.$$

Además 5 y 31 son primos de Mersenne, entonces la sucesión recurrente lineal es de período máximo.

Como todo vector de estado verifica que $s_i = S_0 A^i$ (Lema 1.39), entonces se cumple para el estado inicial $S_0 = [s_0, s_1, \dots, s_{L-1}]$.

Despejando la incógnita se obtiene

$$S_0 = s_{10}(A^{10})^{-1}$$

Luego necesitamos el cálculo de:

$$A^{10} = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}^{10} = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 \end{pmatrix}$$

Capítulo III

Y de su matriz inversa, la cual se puede obtener por el método de Gauss o utilizando la traspuesta de la adjunta dividida por el determinante de dicha matriz, o sea $\frac{(A^{10})^t}{\det(A^{10})}$, o también utilizando el software El Matemática:

$$A^{10^{-1}} = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 \end{pmatrix}$$

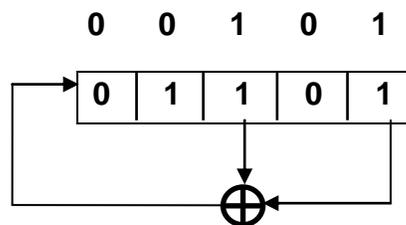
Realizando entonces el producto de matrices obtenemos:

$$S_0 = (1 \ 0 \ 0 \ 0 \ 1) \begin{pmatrix} 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 \end{pmatrix} = (0 \ 1 \ 1 \ 0 \ 1)$$

El cual podemos verificar que es el estado inicial a partir del cual se generó la sucesión recurrente lineal homogénea.

Sea el registro de desplazamiento con retroalimentación lineal $(5, x^5 + x^2 + 1)$ y el estado inicial $S_0 = (0 \ 1 \ 1 \ 0 \ 1)$ a partir del cual se generó la subsucesión $s = 1,0,0,0,1,1,0,1,1,1$.

Las conexiones están dadas según la Definición 2.2.



Aplicando un correcto funcionamiento del registro obtenemos los 31 estados del registro y justo en el instante de tiempo $i = 10$, obtenemos el estado a partir del cual se generó la sucesión de salida obtenida por el ataque de texto claro conocido.

Capítulo III

00110 0	11111 1	11000 0	01110 0	00101 1	00100 0
10011 1	01111 1	01100 0	10111 1	00010 0	10010 0
11001 1	00111 1	10110 0	01011 1	00001 1	01001 1
11100 0	00011 1	11011 1	10101 1	10000 0	10100 0
11110 0	<u>10001</u> 1	11101 1	01010 0	01000 0	11010 1

La sucesión de salida que se obtiene es:

$$S = 1,0,1,1,0,0,1,1,1,1,0,0,0,1,1,0,1,1,1,0,1,0,1,0,0,0,0,1,0,1$$

Observación: El estado a partir del cual se obtuvieron los elementos de dicha subsucesión y dichos elementos coinciden (rojo subrayado).

Bajo el mismo supuesto y la misma hipótesis plantearemos otro procedimiento para la recuperación del estado inicial. Utilizaremos la definición de recurrencia propuesta en el segundo epígrafe del primer capítulo.

Sea $f(x) = x^L + a_{L-1}x^{L-1} + a_{L-2}x^{L-2} + \dots + a_0$, el polinomio de conexión del registro de desplazamiento obtenido en el epígrafe anterior, $S = s_i, s_{i+1}, s_{i+2}, s_{i+3}, \dots, s_{i+L}, s_{i+L+1}, \dots, s_{(i+L)+L-1}$ la subsucesión de salida que se obtuvo por el ataque de texto claro expuesto en el epígrafe 3.1. Entonces por la Definición 1.29 de sucesión recurrente lineal homogénea, siempre es posible expresar cualquier término de la sucesión recurrente lineal homogénea en función de los términos anteriores. De esta manera, podemos representar la ecuación de cualquier término de la recurrencia a partir de s_L en función de los estados anteriores y por consiguiente, del estado inicial $S_0 = [s_0, s_1, \dots, s_{L-1}]$ realizando la recurrencia hacia atrás utilizando la suma *mod 2*.

En función de las etapas iniciales sería

Capítulo III

$$s_L = a_{L-1}s_{L-1} + a_{L-2}s_{L-2} + a_{L-3}s_{L-3} + \dots + a_0s_0$$

Y así sucesivamente

$$s_{L+1} = a_{L-1}s_L + a_{L-2}s_{L-1} + a_{L-3}s_{L-2} + \dots + a_0s_1$$

$$s_{L+2} = a_{L-1}s_{L+1} + a_{L-2}s_L + a_{L-3}s_{L-1} + \dots + a_0s_2$$

⋮

$$s_{L+n} = a_{L-1}s_{L+n-1} + a_{L-2}s_{L+n-2} + a_{L-3}s_{L+n-3} + \dots + a_0s_n$$

donde $0 \leq n \leq 2^L - 2 - L$.

Formaríamos entonces un sistema solo en función de las etapas iniciales utilizando la suma *mod 2*

$$s_L = a_{L-1}s_{L-1} + a_{L-2}s_{L-2} + a_{L-3}s_{L-3} + \dots + a_0s_0$$

$$s_{L+1} = a_{L-1}(a_{L-1}s_{L-1} + a_{L-2}s_{L-2} + a_{L-3}s_{L-3} + \dots + a_0s_0) + a_{L-2}s_{L-1} + a_{L-3}s_{L-2} + \dots + a_0s_1$$

⋮

El sistema de ecuaciones anterior siempre se puede resolver, solo que sería costoso computacionalmente en los casos donde el instante de tiempo i sea muy grande. La cantidad de ecuaciones a formular es L , que es la cantidad de etapas desconocidas del estado inicial y, como se había mencionado, el grado del polinomio de conexión. El planteamiento de las ecuaciones cesa cuando obtengamos las primeras L ecuaciones a partir del instante de tiempo supuesto conocido. Con este sistema recuperaríamos el estado inicial.

Ejemplo 3.5

Sea $f(x) = x^5 + x^2 + 1$, el polinomio de conexión del registro de desplazamiento con retroalimentación lineal encontrado en el Ejemplo 3.2, $s = 1,0,0,0,1,1,0,1,1,1$ la subsucesión de salida obtenida por el ataque a partir del tiempo $i = 10$ y $S_0 = [s_0, s_1, \dots, s_{L-1}]$ constituyen las incógnitas.

Capítulo III

El sistema se formularía

$$s_5 = a_4 s_4 + a_3 s_3 + a_2 s_2 + a_0 s_0$$

$$s_6 = a_4 s_5 + a_3 s_4 + a_2 s_3 + a_0 s_1$$

$$s_7 = a_4 s_6 + a_3 s_5 + a_2 s_4 + a_0 s_3$$

$$s_8 = a_4 s_7 + a_3 s_6 + a_2 s_5 + a_0 s_4$$

$$s_9 = a_4 s_8 + a_3 s_7 + a_2 s_6 + a_0 s_5$$

$$s_{10} = a_4 s_9 + a_3 s_8 + a_2 s_7 + a_0 s_6$$

$$s_{11} = a_4 s_{10} + a_3 s_9 + a_2 s_8 + a_0 s_7$$

$$s_{12} = a_4 s_{11} + a_3 s_{10} + a_2 s_9 + a_0 s_8$$

$$s_{13} = a_4 s_{12} + a_3 s_{11} + a_2 s_{10} + a_0 s_9$$

$$s_{14} = a_4 s_{13} + a_3 s_{12} + a_2 s_{11} + a_0 s_{10}$$

Sustituyendo los valores de

$a_4 = 0, a_3 = 0, a_2 = 1, a_1 = 0, a_0 = 1, s_{10} = 1, s_{11} = 0, s_{12} = 0, s_{13} = 0, s_{14} = 1$ en el sistema y realizando la recurrencia hacia atrás se obtiene

$$s_5 = s_2 + s_0$$

$$s_6 = s_3 + s_1$$

$$s_7 = s_4 + s_2$$

$$s_8 = s_2 + s_0 + s_3$$

$$s_9 = s_3 + s_1 + s_4$$

$$1 = s_4 + s_0$$

$$0 = s_0 + s_1 + s_2$$

$$0 = s_1 + s_2 + s_3$$

$$0 = s_2 + s_3 + s_4$$

Capítulo III

$$1 = s_0 + s_2 + s_3 + s_4$$

Resolviendo este utilizando algún método de los dichos anteriormente obtendríamos

$$s_0 = 0, s_1 = 1, s_2 = 1, s_3 = 0, s_4 = 1$$

$$S_0 = (0 \ 1 \ 1 \ 0 \ 1)$$

Mediante el análisis criptográfico de los registros de desplazamiento con retroalimentación lineal pudimos obtener, bajo ciertos supuestos, el polinomio de conexión del registro y con este hallar, por dos vías, el estado inicial a partir del cual se generó la SRL homogénea binaria del primer capítulo. Esto no prueba que los registros son vulnerables a ataques por lo que hay que utilizar otros mecanismos para potenciarlos.

Conclusiones

CONCLUSIONES

- A través de este trabajo se pudo obtener un procedimiento práctico para la obtención de los polinomios de retroalimentación de los registros de desplazamiento lineales a partir del conocimiento de $2L$ elementos consecutivos de una sucesión de salida, siendo L la longitud del registro.
- Además, se expusieron métodos teóricos para la recuperación del estado inicial de los registros de desplazamiento, los cuales pueden constituir amenazas reales bajos entornos que soporten las suposiciones planteadas.
- A partir de estos resultados se puede llegar a la conclusión de que los LSFR no se pueden utilizar por si solos, hay que introducirles otros mecanismos para aumentar su fortaleza.

Recomendaciones

Recomendaciones

Para mejorar las técnicas expuestas para el análisis de los registros de desplazamiento con retroalimentación lineal, de manera que se incremente la rigurosidad de la teoría planteada se recomienda:

- Modificar el procedimiento para la recuperación del estado inicial, de manera que se prescindiera del instante de tiempo en que se obtuvo la salida.
- Extender el procedimiento para obtener el polinomio de retroalimentación de los LFSRs a partir del conocimiento de salidas no sucesivas.

Bibliografía

1. Arachchige, C. K. (1991). A Fast Algorithm for Gaussian Elimination over GF (2) and Its Implementation on the GAPP.
2. Biham, E., & Dunkelman, O. (2000). Cryptanalysis of the A5/1 GSM Stream Cipher. 43–51.
3. Bruen, A., & Mollin, R. (2009). Cryptography and Shift Registers.
4. E.R., B. (1968). Algebraic Coding Theory.
5. Glen, A. (2002). *On the Period Length of Pseudorandom Number Sequences*.
6. Golomb, S. (1982). *Shift register sequences*.
7. Goresky M., K. A. (2012). *Algebraic Shift Register Sequences*.
8. Guarino, S. (2010). *Ciphertext-only reconstruction of LFSR-based stream ciphers*.
9. Herlestam, T. (1986). On functions of linear shift register sequences. 119–129.
10. Jansen, C. J., & Boeke, D. E. (1998). The Shortest Feedback Shift Register That Can Generate A Given Sequence.
11. Kholosha, A. (2003). Investigations in the Design and Analysis of Key-Stream Generators.
12. López, M. J. (2009). *CRIPTOGRAFÍA Y SEGURIDAD EN COMPUTADORES*.
13. Massey, J. (1969). Shift-register synthesis and BCH decoding. 122–127.
14. Mendoza, J. (2009). *ÁLGEBRA CLÁSICA*.
15. Menezes, A., VanOorschot, P., & Vanstone, S. (1996). *Handbook of Applied Cryptography*.
16. Niederreiter, R. L. (1986). *Introduction to Finite fields*.
17. Panario, G. L. (2013). Handbook of finite fields.
18. Reed, J. A., & Sloane, N. J. (1985). SHIFF-REGISTER SYNTHESIS (MODULO m).
19. Rueppel, R. (1986). Analysis and design of stream ciphers.
20. Schneier, B. (1996 de 1 de 1). *Applied Cryptography*. Recuperado el 25 de mayo de 2014

Bibliografía

21. Siegmund M. Redl, M. K. (1995). An Introduction to GSM.
22. Tilborg, H. C. (2005). *ENCYCLOPEDIA OF CRYPTOGRAPHY AND SECURITY*.
Henk C. A. van Tilborg.
23. Vernam, G. (1926). Cipher printing telegraph systems for secret wire and radio telegraphic communications. 109–115.
24. Yoshiyasu Takefusi, T. K. (1983). *Fast Matrix Solver in GF(2)*. Recuperado el 15 de 5 de 2014
25. Zenner, E. (2004). *On Cryptographic Properties of LFSR-based Pseudorandom Generators*.

ANEXOS

Anexo 1

Implementación de un registro de desplazamiento (Schneier, 1)

```
int LFSR ()
{
    static unsigned long ShiftRegister = 1;
    /* Anything but 0. */
    ShiftRegister = (((ShiftRegister >> 31) ^ (ShiftRegister >> 6) ^ (ShiftRegister >> 4)
        ^ (ShiftRegister >> 2) ^ (ShiftRegister >> 1) ^ ShiftRegister))
        & 0x00000001) << 31) | (ShiftRegister >> 1) ;
    return ShiftRegister & 0x00000001;
}
```

Anexo 2

Algoritmo para generar polinomio primitivo sobre campos binarios (elaborado por el LCA).

```
void polinomios_primitivos(long m) {
    long long rango = pow(2.0,m)-1;
    long long pol2 = pow(2.0,(double)rango)+1;
    long long p = pow(2.0,m+1);
    for(long long i=pow(2.0,m)+1;i<pow(2.0,m+1);i+=2) {
        long long v = 2;
        for(long long j=0;j<rango-1;j++) {
            v*=2;
            if (v>=p)
                v ^= 2*i;
            if (v==2)
                break;
        }
        if (v!=2) {printf("%d\n",i); cont++;}
    }
}
```

Anexo 3

Tabla de polinomios primitivos sobre campos binarios (Schneier, 1)

Los elementos dentro del paréntesis representan, de izquierda a derecha, los exponentes de cada término del polinomio primitivo comenzando por su grado.

(1, 0)	(36, 11, 0)	(68, 9, 0)	(97, 6, 0)
(2, 1, 0)	(36, 6, 5, 4, 2, 1, 0)	(68, 7, 5, 1, 0)	(98, 11, 0)
(3, 1, 0)	(37, 6, 4, 1, 0)	(69, 6, 5, 2, 0)	(98, 7, 4, 3, 1, 0)
(4, 1, 0)	(37, 5, 4, 3, 2, 1, 0)	(70, 5, 3, 1, 0)	(99, 7, 5, 4, 0)
(5, 2, 0)	(38, 6, 5, 1, 0)	(71, 6, 0)	(100, 37, 0)
(6, 1, 0)	(39, 4, 0)	(71, 5, 3, 1, 0)	(100, 8, 7, 2, 0)
(7, 1, 0)	(40, 5, 4, 3, 0)	(72, 10, 9, 3, 0)	(101, 7, 6, 1, 0)
(7, 3, 0)	(41, 3, 0)	(72, 6, 4, 3, 2, 1, 0)	(102, 6 5 3 0)
(8, 4, 3, 2, 0)	(42, 7, 4, 3, 0)	(73, 25, 0)	(103, 9, 9)
(9, 4, 0)	(42, 5, 4, 3, 2, 1, 0)	(73, 4, 3, 2, 0)	(104, 11, 10, 1, 0)
(10, 3, 0)	(43, 6, 4, 3, 0)	(74, 7, 4, 3, 0)	(105, 16, 0)
(11, 2, 0)	(44, 6, 5, 2, 0)	(75, 6, 3, 1, 0)	(106, 15, 0)
(12, 6, 4, 1, 0)	(45, 4, 3, 1, 0)	(76, 5, 4, 2, 0)	(107, 9, 7, 4, 0)
(13, 4, 3, 1, 0)	(46, 8, 7, 6, 0)	(77, 6, 5, 2, 0)	(108, 31, 0)
(14, 5, 3, 1, 0)	(46, 8, 5, 3, 2, 1, 0)	(78, 7, 2, 1, 0)	(109, 5, 4, 2, 0)
(15, 1, 0)	(47, 5, 0)	(79, 9, 0)	(110, 6, 4, 1, 0)
(16, 5, 3, 2, 0)	(48, 9, 7, 4, 0)	(79, 4, 3, 2, 0)	(111, 10, 0)
(17, 3, 0)	(48, 7, 5, 4, 2, 1, 0)	(80, 9, 4, 2, 0)	(111, 49, 0)
(17, 5, 0)	(49, 9, 0)	(80, 7, 5, 3, 2, 1, 0)	(113, 9, 0)
(17, 6, 0)	(49, 6, 5, 4, 0)	(81, 4, 0)	(113, 15, 0)
(18, 7, 0)	(50, 4, 3, 2, 0)	(82, 9, 6, 4, 0)	(113, 30, 0)
(18, 5, 2, 1, 0)	(51, 6, 3, 1, 0)	(82, 8, 7, 6, 1, 0)	(114, 11, 2, 1, 0)
(19, 5, 2, 1, 0)	(52, 3, 0)	(83, 7, 4, 2, 0)	(115, 8, 7, 5, 0)
(20, 3, 0)	(53, 6, 2, 1, 0)	(84, 13, 0)	(116, 6, 5, 2, 0)
(21, 2, 0)	(54, 8, 6, 3, 0)	(84, 8, 7, 5, 3, 1, 0)	(117, 5, 2, 1, 0)
(22, 1, 0)	(54, 6, 5, 4, 3, 2, 0)	(85, 8, 2, 1, 0)	(118, 33, 0)
(23, 5, 0)	(55, 24, 0)	(86, 6, 5, 2, 0)	(119, 8, 0)
(24, 4, 3, 1, 0)	(55, 6, 2, 1, 0)	(87, 13, 0)	(119, 45, 0)
(25, 3, 0)	(56, 7, 4, 2, 0)	(87, 7, 5, 1, 0)	(120, 9, 6, 2, 0)
(26, 6, 2, 1, 0)	(57, 7, 0)	(88, 11, 9, 8, 0)	(121, 18, 0)
(27, 5, 2, 1, 0)	(57, 5, 3, 2, 0)	(88, 8, 5, 4, 3, 1, 0)	(122, 6, 2, 1, 0)

Anexos

(28, 3, 0)	(58, 19, 0)	(89, 38, 0)	(123, 2, 0)
(29, 2, 0)	(58, 6, 5, 1, 0)	(89, 51, 0)	(124, 37, 0)
(30, 6, 4, 1, 0)	(59, 7, 4, 2, 0)	(89, 6, 5, 3, 0)	(125, 7, 6, 5, 0)
(31, 3, 0)	(59, 6, 5, 4, 3, 1, 0)	(90, 5, 3, 2, 0)	(126, 7, 4, 2, 0)
(31, 6, 0)	(60, 1, 0)	(91, 8, 5, 1, 0)	(127, 1, 0)
(31, 7, 0)	(61, 5, 2, 1, 0)	(91, 7, 6, 5, 3, 2, 0)	(127, 7, 0)
(31, 13, 0)	(62, 6, 5, 3, 0)	(92, 6, 5, 2, 0)	(127, 63, 0)
(32, 7, 6, 2, 0)	(63, 1, 0)	(93, 2, 0)	(128, 7, 2, 1, 0)
(32, 7, 5, 3, 2, 1, 0)	(64, 4, 3, 1, 0)	(94, 21, 0)	(129, 5, 0)
(33, 13, 0)	(65, 18, 0)	(94, 6, 5, 1, 0)	(130, 3, 0)
(33, 16, 4, 1, 0)	(65, 4, 3, 1, 0)	(95, 11, 0)	(131, 8, 3, 2, 0)
(34, 8, 4, 3, 0)	(66, 9, 8, 6, 0)	(95, 6, 5, 4, 2, 1, 0)	(132, 29, 0)
(34, 7, 6, 5, 2, 1, 0)	(66, 8, 6, 5, 3, 2, 0)	(96, 10, 9, 6, 0)	(133, 9, 8, 2, 0)
(35, 2, 0)	(67, 5, 2, 1, 0)	(96, 7, 6, 4, 3, 2, 0)	(134, 57, 0)
(135, 11, 0)	(152, 6, 3, 2, 0)	(178, 87, 0)	(270, 133, 0)
(135, 16, 0)	(153, 1, 0)	(183, 56, 0)	(282, 35, 0)
(135, 22, 0)	(153, 8, 0)	(194, 87, 0)	(282, 43, 0)
(136, 8, 3, 2, 0)	(154, 9, 5, 1, 0)	(198, 65, 0)	(286, 69, 0)
(137, 21, 0)	(155, 7, 5, 4, 0)	(201, 14, 0)	(286, 73, 0)
(138, 8, 7, 1, 0)	(156, 9, 5, 3, 0)	(201, 17, 0)	(294, 61, 0)
(139, 8, 5, 3, 0)	(157, 6, 5, 2, 0)	(201, 59, 0)	(322, 67, 0)
(140, 29, 0)	(158, 8, 6, 5, 0)	(201, 79, 0)	(333, 2, 0)
(141, 13, 6, 1, 0)	(159, 31, 0)	(202, 55, 0)	(350, 53, 0)
(142, 21, 0)	(159, 34, 0)	(207, 43, 0)	(366, 29, 0)
(143, 5, 3, 2, 0)	(159, 40, 0)	(212, 105, 0)	(378, 43, 0)
(144, 7, 4, 2, 0)	(160, 5, 3, 2, 0)	(218, 11, 0)	(378, 107, 0)
(145, 52, 0)	(161, 18, 0)	(218, 15, 0)	(390, 89, 0)
(145, 69, 0)	(161, 39, 0)	(218, 71, 0)	(462, 73, 0)
(146, 5, 3, 2, 0)	(161, 60, 0)	(218, 83, 0)	(521, 32, 0)
(147, 11, 4, 2, 0)	(162, 8, 7, 4, 0)	(225, 32, 0)	(521, 48, 0)
(148, 27, 0)	(163, 7, 6, 3, 0)	(225, 74, 0)	(521, 158, 0)
(149, 10, 9, 7, 0)	(164, 12, 6, 5, 0)	(225, 88, 0)	(521, 168, 0)
(150, 53, 0)	(165, 9, 8, 3, 0)	(225, 97, 0)	(607, 105, 0)
(151, 3, 0)	(166, 10, 3, 2, 0)	(225, 109, 0)	(607, 147, 0)
(151, 9, 0)	(167, 6, 0)	(231, 26, 0)	(607, 273, 0)
(151, 15, 0)	(170, 23, 0)	(231, 34, 0)	(1279, 216, 0)
(151, 31, 0)	(172, 2, 0)	(234, 31, 0)	(1279, 418, 0)
(151, 39, 0)	(174, 13, 0)	(234, 103, 0)	(2281, 715, 0)
(146, 5, 3, 2, 0)	(161, 60, 0)	(218, 83, 0)	(521, 32, 0)

Anexos

(147, 11, 4, 2, 0)	(162, 8, 7, 4, 0)	(225, 32, 0)	(521, 48, 0)
(148, 27, 0)	(163, 7, 6, 3, 0)	(225, 74, 0)	(521, 158, 0)
(149, 10, 9, 7, 0)	(164, 12, 6, 5, 0)	(225, 88, 0)	(521, 168, 0)
(150, 53, 0)	(165, 9, 8, 3, 0)	(225, 97, 0)	(225, 97, 0)
(151, 3, 0)	(166, 10, 3, 2, 0)	(225, 109, 0)	(607, 147, 0)
(151, 9, 0)	(167, 6, 0)	(231, 26, 0)	(607, 273, 0)
(151, 15, 0)	(170, 23, 0)	(231, 34, 0)	(1279, 216, 0)
(151, 31, 0)	(172, 2, 0)	(234, 31, 0)	(1279, 418, 0)
(151, 39, 0)	(174, 13, 0)	(234, 103, 0)	(2281, 715, 0)
(151, 43, 0)	(175, 6, 0)	(236, 5, 0)	(2281, 915, 0)
(151, 46, 0)	(175, 16, 0)	(250, 103, 0)	(2281, 1029, 0)
(151, 51, 0)	(175, 18, 0)	(255, 52, 0)	(3217, 67, 0)
(151, 63, 0)	(175, 57, 0)	(255, 56, 0)	(3217, 576, 0)
(151, 66, 0)	(177, 8, 0)	(255, 82, 0)	(4423, 271, 0)
(151, 67, 0)	(177, 22, 0)	(258, 83, 0)	(9689, 84, 0)
(151, 70, 0)	(177, 88, 0)	(266, 47, 0)	