Autómatas Celulares Para la Conversión Criptográfica

Grupo AuCel José Oscar Mugetti Mare - director
Universidad Tecnológica Nacional – Facultad Regional San Francisco
Av. De la Universidad 501 – San Francisco (Córdoba)
aucel@sanfrancisco.utn.edu.ar

La aplicación desarrollada se realiza en el campo de las ciencias computacionales, específicamente en la criptología donde definiendo especificaciones formales y características del autómata en sí, se puede utilizar esta herramienta para obtener resultados algorítmicos eficientes y tratamiento adecuando de las claves generadas por funciones criptográficas.

Un Autómata Celular es una herramienta computacional que es parte de la Inteligencia Artificial basada en modelos biológicos, el cual está básicamente compuesto por una estructura estática de datos y un conjunto finito de reglas que son aplicadas a cada nodo o elemento de la estructura.[1]

Los objetivos propuestos en el grupo es llegar a comprender el comportamiento predictivo de los autómatas celulares y descubrir cómo puede este comportamiento representar los estados binarios de una palabra clave para que a partir de determinadas reglas que a través de iteraciones en tiempo formal resulte una nueva clave, denominada función clave hash, que tenga tales características que no permita a partir de ella obtener la palabra clave original. Una vez realizado esto, nos proponemos a realizar análisis sobre las funciones claves hash obtenidas, para lograr una reducción de colisiones, tal que nos permita utilizar todo este proceso en un algoritmo de cifrado criptográfico.

Los autómatas celulares son una colección finita o infinita de células idénticas dispuestas uniformemente según un espacio dimensional y que poseen un estado determinado, que va cambiando con el paso discreto del tiempo según una determinada regla de transición de estados. Esta regla está definida por el estado de sus células vecinas. [2]

Elementos de un autómata celular:

- Dimensión
- Estados posibles
- Vecindad
- Regla de transición

La evolución de un AC a lo largo del tiempo se representa de forma sencilla sin más que escribir las sucesivas configuraciones de sus células, una debajo de otra.

Criptología

La Criptología es, tradicionalmente, la disciplina científica que se dedica al estudio de la escritura secreta, es decir, estudia los mensajes que, procesados de cierta manera, se convierten en difíciles o imposibles de leer por entidades no autorizadas. Criptografía se ocupa de las técnicas de cifrado o codificado destinadas a alterar las representaciones lingüísticas de ciertos mensajes con el fin de hacerlos ininteligibles a receptores no autorizados.

Proceso de cifrado

El proceso para cifrar un mensaje consiste en transformarlo mediante un algoritmo de modo que sólo quien esté autorizado podría invertir el proceso de cifrado (descifrado) para recuperar el texto original.

Funciones hash

Una función hash H es una función computable mediante un algoritmo, que tiene como entrada un conjunto de elementos, que suelen ser cadenas, y los convierte (mapea) en un rango de salida finito, normalmente cadenas de longitud fija. Es decir, la función actúa como una proyección del conjunto U sobre el conjunto M. [3]

La idea básica de un valor hash es que sirva como una representación compacta de la cadena de entrada.

Aleatoriedad y Pseudoaleatoriedad

Consideraremos que algo es aleatorio, cuando no se puede volver a reproducir con los medios actuales, en un tiempo más o menos corto, en exactamente las mismas condiciones que se hizo anteriormente

Las pruebas de aleatoriedad (o test de aleatoriedad), son pruebas estadísticas usadas para decidir si una determinada muestra o conjuntos de datos responde a un patrón o puede considerarse aleatoria. La aleatoriedad es un campo de definición que, en matemáticas, se asocia a todo proceso cuyo resultado no es previsible más que en razón de la intervención del azar. [4]

Desarrollo

El propósito de la investigación es crear una función hash que permita determinar una imagen con un alto

grado de seguridad para evitar que una determinada información confidencial sea decodificada fácilmente.

La idea de utilizar las reglas de transición de Wolfram es lograr un generador de bits *pseudoaleatorios*, es decir, que el algoritmo determinista logre el mayor grado de aleatoriedad posible, para que a partir de la conformación binaria de la clave o mensaje se pueda obtener a iterativamente una clave hash asociada que tenga la característica de que no pueda ser invertible su proceso.

La secuencia de bits correspondiente a una determinada palabra "clave" determina la configuración inicial de nuestro AC. Para obtener una nueva configuración del AC es necesario utilizar una regla determinada sobre la configuración actual, bit a bit, para obtener la sucesión unitaria que determina la nueva configuración, cabe mencionar que las condiciones del entorno utilizadas son las Condiciones Periódicas.

Dentro de las características procedimentales de nuestra aplicación, definimos que la configuración del autómata debe ser de hasta 128 células, es decir que la palabra que vayamos a procesar puede ser de hasta 16 caracteres (128 bits), también definimos un mínimo de 4 caracteres para la palabra clave.

Una vez ubicada esta "clave" como configuración inicial, obtuvimos a través de una cierta cantidad de iteraciones el código hash final asociado a la palabra. Luego de haber realizado un software que genere los hash, a partir de una palabra clave introducida, y estableciendo que la palabra debe contener entre 4 y 16 letras, que pueden tener repetición y símbolos especiales, fue posible determinar que las posibles combinaciones son de más de 42 mil millones de combinaciones, que resulta imposible determinarlos por el universo, así que se toma una muestra obtenida a partir de la fórmula estadística de muestreo.[5] Con ello determinamos que la muestra teniendo un nivel de confianza del 95,5% y un error del 2% es de aproximadamente 25000 corridas. Se tomó un diccionario de palabras, al cual se les introdujeron modificaciones para alterar los símbolos y establecer mayor cantidad de palabras, con un total de 8.500.000 palabras, hecho que superó ampliamente la muestra determinada. Se generaron las claves hash a las cuales se realizaron las pruebas de aleatoriedad y pseudoaleatoriedad mediante métodos matemáticos y software diseñado a tal efecto. Es importante destacar que, los resultados de aleatoriedad fueron altamente positivos, esto es, dichas claves, superaron 13 de las 15 pruebas NIST, [7] parámetro suficiente para establecer la aleatoriedad de la clave generada, confirmando la imposibilidad de revertir el proceso; es decir a partir del hash obtener la palabra origen, o desencriptar el mismo.

La elección de la cadena de caracteres tiene un rango dentro de los 4 y 16 caracteres, y los caracteres permitidos de la tabla ASCII son los "Caracteres imprimibles". Esta cadena elegida, se coloca en el centro de la disposición de 512 celdas, previamente convertido cada carácter a su correspondiente binario. El espacio restante se rellena con ceros.

Esta disposición se corresponde a la configuración inicial del Autómata Celular, a partir de esta se irá iterando cada configuración para obtener la configuración consecuente.

Se trabajó cada clave con 300 iteraciones y la posterior obtención de la cadena de 64 caracteres que determina nuestra cadena Hash por "clave".

Este procedimiento fue aplicado sobre un diccionario de palabras validadas de 8.500.000 palabras diferentes. Los resultados obtenidos fueron analizados y utilizados para evaluar si a partir de claves diferentes fueron obtenidas cadenas Hash iguales. Nos encontramos con que este fenómeno no ocurrió (0 colisiones) pudiendo cumplir nuestro objetivo de minimizar-eliminar colisiones.[6]

En las explicaciones anteriores quedaron establecidos las diferentes operaciones de las variables y los instrumentos de medición utilizados, como así también la forma de analizar los datos obtenidos.

Referencias

[1] A New Kind of Science, por Stephen Wolfram, WolframMedia Inc., 2002.

[2] Random Sequence generation by cellular automata, Stephen Wolfram, WolframMedia Inc 2008.

[3] Probabilistic Encryption * SHAFI GOLDWASSER AND SILVIO MICALI Laboratory of Computer Science, Massachusetts Institute of Technology, Cambridge, Massachusetts 1983)

[4] A Statistical Test Suite for Random and Pseudo random Number Generators for Cryptographic Application, NIST Special Publication 800-22 (with revisions dated May 15, 2001)

[5] Applied Cryptography: Protocols, Algorithms, and Source Code in C, Bruce Schneier 2007)

[6] Collision Based Computing, Andrew Adamatzky, Ed Springer 2002)

[7] National Institute of Standards and Tecnology - Special Publicatios 800-22 Revisión 1ra. "A Statical Test Suite for Random and Pseudorandom, Number Generators for Cryptographic Applicarions).