Universidad Nacional de Loja
Carrera Computación
Facultad de Energía las Industrias y los Recursos Naturales no Renovables

ACTIVIDAD AUTÓNOMA

TÍTULO DEL ENSAYO

Estudiante	Melissa Tuza Jiménez		
Paralelo	Séptimo A		
Professor	Ing. Cristian Narváez G. Mg.Sc.		
Unidad	Criptografía computacional		
Fecha	10/01/2024	**Plagio:** Si:No	**Calificación:** .....
Observación.:			

Introducción

En el mundo actual la criptografía permite mantener la seguridad de grandes cantidades de información, entre un punto fuerte sobresale el algoritmo de Diffie-Hellman que permite desarrollar el intercambio de claves, al momento de establecer una clave que será compartida por ambas parte, previamente antes de desarrollar la comunicación. Dentro del presente ensayo, se explora conceptos básicos de cómo funciona Diffie-Hellman, explicando como se realiza el proceso de intercambio de llaves. Además, sobresalen conceptos que intervienen y se fusionan productivamente, como grupos multiplicativos y aditivo, como interfieren y permiten mejorar las posibles vulnerabilidades del algoritmo, ofreciendo mayor rendimiento para finalmente considerar y ser consientes del nivel de rendimiento que en sí ofrece Diffie-Hellman y la precaución necesaria que se puede considerar.

Desarrollo

En el mundo actual la seguridad de la información es de gran importancia, para ello el algoritmo de Diffie-Hellman proporciona un mecanismo de intercambio de claves seguras mediante el proceso de claves compartidas, a continuación se analiza la importancia y conceptos matemáticos para el desarrollo de una comunicación segura dentro de entornos virtuales.

0.1. ¿Qué es el algoritmo de Diffie-Hellman?

Se trata de un algoritmo que realiza un intercambio de claves, este algoritmo constituye el protocolo TLS. Desarrollado por Whitfield Diffie y Martin Hellman, criptógrafos que presentaron este algoritmo en el año de 1976, siendo considerado como un elemento fundamental de la clave pública. Tiene como premisa el intercambio de claves, se da entre un emisor y un remitente, en donde ambos actores son totalmente desconocidos y definen una clave para establecer y mantener la comunicación. Este algoritmo tiene como propósito evitar el cifrado de la clave privada, por ende al momento de definir una clave pública con un tamaño considerable, se convierte en un proceso totalmente intratable debido a la complejidad que resulta resolver este logaritmo. Otro punto a considerar, es que al momento de desarrollar el proceso de intercambio de claves, no se da paso a la autenticación del emisor y remitente, por ende, se plantean dos alternativas, como lo son: por un lado, aplicar protocolos adicional de autenticación o a su vez, implementar las firmas digitales. Verificar que uno de los dos actores es realmente parte de la conversación es importante, por ende se requiere de validar la identidad de los actores. Para ello, puede ser empleada la autenticación de clave pública, en donde se saca ventaja del nivel de asimetría que

existe dentro de las claves criptográficas. Corroborando la identidad sin necesidad de conocer más información innecesaria como puede ser, la exposición de la clave privada. Otra manera de validar la identidad de las partes es la aplicación de protocolos basados en firmas digitales, teniendo en cuenta que su principio es mantener las claves públicas integras para realizar la comparación de claves al momento de intercambiarlas. Al momento de agregar un mecanismo de autenticación adicional, se garantiza la autenticidad del emisor, tanto como del remitente. Por ende, es considerado un algoritmo seguro. [1] [3]

0.2. ¿En qué se basa el algoritmo de Diffie-Hellman ?

Las bases de Diffie-Hellman se establecen con conceptos matemáticos como la aritmética modular, es decir, los módulos son divididos por números aritméticos. Además, manejan funciones Hash, con el fin de realizar la conversión de una variable de tamaño irregular para convertirlo y obtener en una variable de tamaño fijo. Por otro lado, maneja números primos, el proceso que conlleva para resolverlos, de acuerdo al tamaño del número primo, se atribuye que es el nivel de seguridad del algoritmo. Debido a que se trabaja con un logaritmo discreto de números primos para desarrollar un proceso cíclico finito agrupado dado por el elemento de g. De esta forma, al momento de utilizar la clave pública para obtener la clave privada al omento de derivar la clave, resultará sumamente complicado, por tal motivo, este algoritmo se enfoca en mantener una clave compartida para establecer la comunicación dentro de un medio seguro establecido previamente. Todos los conceptos antes mencionados al combinarse aportan dentro del contexto criptográfico, en la clave pública, para finalmente obtener una herramienta que permite establecer, garantizar y mantener una comunicación segura. [5]

0.3. ¿Cómo funciona el intercambio de claves de Diffie-Hellman?

Es necesario comprender que este algoritmo se enfoca en la complejidad computacional al momento de resolver el logaritmo discreto, por ende, es de gran utilidad, por ende, se lo emplea en protocolos como TLS y SSL. El emisor y receptor del mensaje aplican los principios de Diffie-Hellman para plantear una vía de comunicación segura mediante una clave compartida por ambos. Por un lado, el emisor cifra el mensaje mediante el algoritmo de AES poniendo en uso la clave compartida creada al inicio. y el vector de inicialización. Por otro lado, el receptor descifra el mensaje mediante tres elementos, la clave compartida, el vector de inicialización, que básicamente corresponde a un valor que se obtiene de forma aleatoria para aportar mayor dificultad al momento de intentar descifrar el texto. Una vez definido los valores correspondientes al número primo grande y a la base que se deseen otorgar. Tanto el emisor como el receptor calculan de forma independiente su clave privada para luego intercambiar las claves generadas con el fin de recalcular una clave compartida, partiendo de sus claves públicas y privadas. Posteriormente, el emisor cifra el mensaje aplicando el algoritmo de AES mediante el modo de CBC, se trata de un modo de operación que dentro de cada bloque de datos, depende del bloque anterior para ser cifrado, además interviene el inicializador de vector para trabajar con el cifrado del primer bloque. Una vez demostrado que el algoritmo, por sí solo, no ofrece un nivel de verificación al momento de autenticar a uno de los dos actores, un claro ejemplo es el algoritmo de Man in the middle, este algoritmo permite evaluar el nivel de rendimiento al momento de realizar ataques, en donde el atacante trata de intervenir en la comunicación con el fin de alterar los mensajes, puede ser que suplante la identidad de del emisor mientras que el receptor revela la clave secreta sin percatarse, entonces el atacante ha tenido paso para acceder a mensajes no autorizados. Para ello, el atacante aplica los puntos de inyección, básicamente corresponde a un protocolo que está

encaminado a inducir uno de los parámetros adicionales que interfieran con el fin de identificar los parámetros establecidos para desarrollar la comunicación. [4]

0.4. ¿Cómo intervienen grupos multiplicativos en comparación de grupos aditivos en la seguridad y vulnerabilidad dentro de Diffie-Hellman?

Dentro de los grupos multiplicativos se enfoca en calcular y resolver logaritmos discretos, es decir, es un grupo de elementos que se multiplican entre quienes conforman dicho conjunto considerado dentro de un campo finito. Por ende, son considerados seguros y con una aplicación fácil al momento de implementarlos, ofrecen mayor eficiencia con respecto al rendimiento. Por ende, es necesario aplicar grupos grandes para que la seguridad sea mayor y más complejo al momento de tratar de entenderlo. De esta forma complica el proceso de descifrar una clave compartida, por otro lado, los grupos aditivos manejan tareas más simples, por ende tienden a ser menos seguros y frente a ataques pequeños tienden a ser eficientes para el atacante, debido a que operan de una forma repetitiva hasta aproximarse al siguiente elemento del mismo grupo, dejando un camino más corto a obtener la seguridad. Se deduce que si un grupo aditivo no consta de particularidades de Diffie-Hellman, al momento de intercambiar las claves no existirá seguridad y tiende a existir vulnerabilidades. Por otro lado, existe un elemento clave, como lo son los inversos triviales, teniendo en cuenta que en no todos los grupos aditivos existe este concepto, sin embargo, se hace referencia a un elemento considerado inverso debido a que es un elemento que al momento de agregarlo, anula al elemento inverso y permite con mayor facilidad a descifrar la clave compartida. Otro elemento clave que interviene en la seguridad y que saca provecho de una vulnerabilidad dentro de Diffie-Hellman es al aplicar los Script kiddies, que trabaja con un script fabricado previamente con el fin de atacar e intervenir dentro de la comunicación de Diffie-Hellman. Trabajan con una herramienta que requiere de personalización del fin que se le quiere dar a un ataque, puede cambiar la dirección IP de la máquina vulnerada, esto puede incluir, inyecciones SQL, incluso botnets que tienen como fin robar información causando daños significativos. [2]

Conclusiones

- El algoritmo de Diffie-Hellman permite resaltar cómo influye la criptografía dentro de la seguridad de la información, mediante el intercambio de claves compartidas, desarrollando la interacción entre el emisor y remitente, partiendo de vía segura, para ello sí se deduce que es necesario evaluar otro método de autenticación para las partes, es posible hacerlo mediante la difusión con conceptos como AES, entre otros, permitiendo parchar las posibles vulnerabilidades.

- Grupos multiplicativos y aditivos son conceptos que intervienen y permiten tomar medidas necesarias al momento de elegir un conjunto matemático, debido a que de eso depende del nivel de seguridad que exista al momento de realizar el proceso de intercambio de claves compartidas. Incluso si se llegará a tener un elemento reversible, se podría vulnerar y comprometer la seguridad de todo el sistema.

- El algoritmo de Diffie-Hellman tiene su nivel de seguridad, pero no deja de estar expuesto a vulnerabilidades, los grupos aditivos tienden a ser una vulnerabilidad más en comparación a los grupos multiplicativos, ya que son grupos más difíciles de factorizar debido al tamaño en sí. Al momento de comprender estos conceptos, se permite identificar las posibles amenazas

que puede sufrir, por ende aplicar los grupos multiplicativos seguros permiten protegerse contra ataques, debido a este motivo se emplea números primos grandes, complicando la probabilidad de obtener la clave compartida.

Referencias

[1] *Algoritmo Diffie-Hellman. Descripción, funcionamiento y ejemplos | Grupo Atico34*. Grupo Atico34, jun. de 2021. URL: `https://protecciondatos-lopd.com/empresas/algoritmo-diffie-hellman/` (visitado 12-01-2024).

[2] Elkin Mauricio Arboleda Zapata, Cesar Tulio Valencia Restrepo y Camilo Montoya Serna. "Comparación entre factores de ajuste multiplicativos y aditivos para producción por lactancia en un hato holstein". En: *Revista Facultad Nacional de Agronomía Medellín* (1995).

[3] ciberseg1922. *Qué es el intercambio de claves Diffie-Hellman y cómo funciona*. Ciberseguridad, jun. de 2021. URL: `https://ciberseguridad.com/guias/recursos/intercambio-claves-diffie-hellman/` (visitado 12-01-2024).

[4] Edgardo Andrés Riquelme Faúndez et al. "Algoritmos genéricos para resolver el logaritmo discreto y aplicaciones". En: (2023).

[5] Jennifer Santamaría Fernández y Daniel Renedo. *El logaritmo discreto y sus aplicaciones en Criptografía*. 2012. URL: `https://repositorio.unican.es/xmlui/bitstream/handle/10902/3101/Jennifer%20Santamaria%20Fernandez.pdf`.