INSTITUTO POLITÉCNICO NACIONAL

ESCUELA SUPERIOR DE INGENIERÍA MECÁNICA Y ELÉCTRICA

SECCIÓN DE ESTUDIOS DE POSGRADO E INVESTIGACIÓN

PROTOCOLOS DE ESTABLECIMIENTO Y ADMINISTRACIÓN DE LLAVE

Tesina que para obtener el grado de
Especialidad en Seguridad Informática y
Tecnologías de la Información que

P R E S E N T A

Alfredo Anduaga Ramírez

Directores de Tesina:

M. en C. María Aurora Molina Vilchis

M. en C. Gina Gallegos García

Ciudad de México, Noviembre 2009

SIP-14

INSTITUTO POLITÉCNICO NACIONAL

SECRETARÍA DE INVESTIGACIÓN Y POSGRADO

ACTA DE REVISIÓN DE TESINA

En la Ciudad de México, D. F. siendo las 18:00 horas del día 18 del mes de noviembre del 2009 se reunieron los miembros de la Comisión Revisora de Tesina designada por el Colegio de Profesores de Estudios de Posgrado e Investigación de SEPI-ESIME-CULH. para examinar la tesina titulada:

"Protocolos de Establecimiento y Administración de la Llave"

Presentada por el alumno:

Anduaga	**Ramírez**	**Alfredo**
Apellido paterno	Apellido materno	Nombre(s)

Con registro:

B	0	8	1	6	6	9

aspirante de:

ESPECIALIDAD EN SEGURIDAD INFORMÁTICA Y TECNOLOGÍAS DE LA INFORMACIÓN

Después de intercambiar opiniones los miembros de la Comisión manifestaron ***SU APROBACIÓN DE LA TESINA***, en virtud de que satisface los requisitos señalados por las disposiciones reglamentarias vigentes.

LA COMISIÓN REVISORA

Director de tesina

M. en C. María Aurora Molina Vilchis

Co-Director de tesina

Dr. Enrique Escamilla Hernández

M. en C. Gina Gallegos García

INSTITUTO POLITÉCNICO NACIONAL
ESTADOS UNIDOS MEXICANOS
S. E. P.
SECCIÓN DE ESTUDIOS DE
ESIME CULHUACÁN

EL PRESIDENTE DEL COLEGIO

Dr. Héctor Manuel Pérez Meana

INSTITUTO POLITÉCNICO NACIONAL

SECRETARÍA DE INVESTIGACIÓN Y POSGRADO

CARTA CESIÓN DE DERECHOS

En la Ciudad de México, D.F. el día 17 del mes noviembre del año 2009, el que suscribe Alfredo Anduaga Ramírez alumno del Programa de Especialidad en Seguridad Informática y Tecnologías de la Información con número de registro B081669, adscrito a SEPI ESIME Culhuacán, manifiesta que es autor intelectual del presente trabajo de Tesis bajo la dirección de los M. en C. Gina Gallegos García y M. en C. María Aurora Molina Vilchis y cede los derechos del trabajo intitulado "PROTOCOLOS DE ESTABLECIMIENTO Y ADMINISTRACIÓN DE LLAVE", al Instituto Politécnico Nacional para su difusión, con fines académicos y de investigación.

Los usuarios de la información no deben reproducir el contenido textual, gráficas o datos del trabajo sin el permiso expreso del autor y/o director del trabajo. Este puede ser obtenido escribiendo a la siguiente dirección aanduagar@gmail.com. Si el permiso se otorga, el usuario deberá dar el agradecimiento correspondiente y citar la fuente del mismo.

Alfredo Anduaga Ramírez.

DEDICATORIA

A mis padres:

Porque con sus palabras me apoyan en todos sentidos
y me impulsan a seguir alcanzando mis metas. Gracias!

AGRADECIMIENTOS

A mis asesoras:

Porque en vez de darme el pescado me enseñaron a pescar. Por aprender que las raíces del triunfo son cada una de las veces que nos levantamos de los tropiezos que enfrentamos y por ende los fracasos son los tropiezos de los que uno no se levanta.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

El presente trabajo de tesis presenta la descripción de los protocolos de establecimiento y administración de llave, comenzando con el panorama general del proceso de establecimiento de llave, conceptos generales y fundamentales, clasificación de los protocolos y finalmente la descripción de los protocolos propuestos, lo cual se logro mediante la elaboración de diagramas de secuencia y la revisión del funcionamiento de dichos protocolos, haciendo uso de herramientas criptográficas desarrolladas como una aplicación de código abierto. Todo esto permitió conocer sus características y la forma en que trabajan, para subsanar el problema del intercambio seguro de llave de la siguiente forma: protocolos de acuerdo de llave para intercambiar un secreto compartido y para la administración de llave, los protocolos de distribución de la misma.

Es así que se logró conocer las características de los protocolos de establecimiento y administración de llave lo que permitirá que en los ambientes en donde destaca la necesidad de proteger la información y que por su naturaleza deben existir altos niveles de seguridad informática, se puedan tomar decisiones para la implementación de alguno(s) de estos protocolos.

ABSTRACT

This thesis presents the description of key establishment and management protocols. It begins with an overview of the key setting process, general and basic concepts. Then, we show the classification and description of proposed protocols. It was achieved through the development of sequence diagrams and by the review of the functionality of such protocols. All of this by using cryptographic tools, which are developed as an open source application.

Mentioned activities allowed us to know their characteristics and how they work, to address the problem of secure key exchange as follows: key agreement protocols to exchange a shared secret and key management, distribution protocols about it.

Consequently, it was possible to know the characteristics of the protocols for key establishment and management, which will allow make decisions in order to implement one (s) of reviewed protocols, in environments that stresses the need to protect information and that by its nature must be high levels of security.

JUSTIFICACIÓN

En la actualidad la mayoría de las empresas dependen de su información y para protegerla requieren implementar y garantizar servicios de seguridad, para lo cual deben incorporar herramientas criptográficas. Sin embargo, la mayoría de las veces no son conscientes de lo que esto implica, ya que proporcionan seguridad a la información pero comúnmente se olvidan de la importancia de la llave. Es así que una de las contribuciones de esta tesina es describir y documentar las características de los protocolos más representativos de establecimiento y administración de llave, dando a conocer los detalles criptográficos para su funcionamiento, lo que permitirá que en los ambientes en donde destaca la necesidad de proteger la información y que por su naturaleza deben existir altos niveles de seguridad informática, se puedan tomar decisiones para la implementación de alguno(s) de estos protocolos, que ofrezcan seguridad a la llave, ya que éstos están definidos para poder realizar el intercambio de llave y la distribución de la misma entre dos o más entidades.

INTRODUCCIÓN

En los ambientes informáticos nadie puede garantizar una seguridad perfecta, por lo que información sensitiva como lo son las llaves criptográficas, puede quedar en manos de algún intruso. Es así que la criptografía permite incorporar servicios de seguridad al transmitir y/o almacenar la información. Sin embargo, un criptosistema no es suficiente para garantizar la seguridad de la información, ya que ésta última depende de nuestras llaves. Por ello es que es importante contar con protocolos de establecimiento y administración de llave. No obstante existe una importante gama de éstos por lo que resulta difícil saber cuál es el protocolo adecuado para cada necesidad. Es por ello que en este trabajo se realiza la descripción de dichos protocolos.

Este trabajo consta de cuatro capítulos divididos de la siguiente forma:

En el capítulo 1 se menciona el panorama general del proceso de establecimiento de llave, mencionando los conceptos generales y la problemática actual de los protocolos. En el capítulo 2 se mencionan los conceptos fundamentales, el establecimiento y administración de llave, los tipos de protocolos, los modelos de establecimiento de llaves simples y el ciclo de vida de las llaves. En el capítulo 3 se estudia y describen tres protocolos de establecimiento de llave. En el capítulo 4 se realiza la descripción de los protocolos de administración de llave. Finalmente se presentan las conclusiones de este trabajo que ayudarán a la selección de protocolos de establecimiento de llave, para futuras implementaciones en ambientes con altas restricciones de seguridad.

OBJETIVOS

Objetivo General.

Hacer una descripción de las características de los protocolos más representativos de establecimiento y administración de llave, lo que permitirá conocer los detalles criptográficos de su funcionamiento, con la finalidad de documentar dichos protocolos para la toma de decisiones futuras en ambientes que por su naturaleza presentan altas exigencias en la seguridad.

Objetivos Particulares.

Para lograr el objetivo de este trabajo será necesario lo siguiente:

- Identificar los protocolos de establecimiento y administración de llave más representativos en la práctica.
- Estudiar los fundamentos teóricos de dichos protocolos.
- Describir el funcionamiento criptográfico de los protocolos.
- Analizar por medio de diagramas de secuencia el comportamiento de los protocolos.
- Buscar herramientas criptográficas para la ejecución de los protocolos.
- Mostrar mediante ejemplos ilustrativos obtenidos de las herramientas, el comportamiento criptográfico de los protocolos.
- Presentar en una tabla comparativa las características principales de cada uno de los protocolos.

CAPITULO 1. PANORAMA GENERAL DEL PROCESO DE ESTABLECIMIENTO DE LLAVE

1.1. CONCEPTOS GENERALES

Gracias a la evolución de las computadoras, éstas comparten la necesidad de disponer de un conjunto de servicios de seguridad, que permitan proteger a las entidades, a los datos y a los equipos implicados. Estos servicios son [1]:

a) Confidencialidad: se refiere a que la información no está disponible para entidades, procesos o individuos no autorizados.
b) Integridad: es la propiedad de que los datos no han sido cambiados, destruidos o perdidos de una manera accidental o no autorizada.
c) Autenticación: establece la garantía de que una entidad es quien dice ser.
d) No repudio: es un servicio de seguridad que provee protección en contra de una denegación en la participación de una comunicación.
e) Disponibilidad: se refiere al grado de que un sistema o componente está accesible cuando es solicitado por alguna entidad.

Lo anterior se logra con la criptografía la cual se define como: la rama inicial de las matemáticas que hace uso de métodos y técnicas, con el objeto de cifrar y/o proteger un mensaje por medio de un algoritmo usando una o más llaves [2].

La criptología, la cual con base en [3] se define como: (del griego kryptós=oculto; lógos=estudio): es la ciencia que trata los problemas relacionados con la seguridad en el intercambio de mensajes cifrados, entre un emisor y un receptor a través de un canal de comunicaciones o red de computadoras y reúne la criptografía y el criptoanálisis. Así mismo el criptoanálisis (kryptós=oculto; Analyein=descomposición), es el arte o ciencia

de determinar la llave o descifrar mensajes sin conocer la llave. Una tentativa de criptoanálisis sin autorización se llama ataque.

El cifrado [4] es el proceso por el cual la información se transforma (codifica) en información cifrada (incomprensible) a través de un algoritmo y una llave. El descifrado es el proceso por el cual se recupera la información original al aplicar un algoritmo y una llave a la información cifrada. Así los elementos básicos de la criptografía son los algoritmos de cifrado-descifrado y la llave. La llave determina el tipo de transformación que se realiza sobre los datos. En los sistemas computacionales e informáticos, la llave es una cadena de datos (almacenada electrónicamente).

Existen dos tipos de criptografía: simétrica y asimétrica. En la criptografía simétrica, también conocida como criptografía de llave secreta, se emplea la misma llave para realizar los procesos de cifrado y descifrado. En la criptografía asimétrica, también conocida como criptografía de llave pública, se emplean dos llaves criptográficas, una llave pública y una llave privada, como su nombre lo establece la primera puede ser conocida por todo el mundo y la segunda se mantiene en secreto. Se utiliza la llave pública para cifrar información y su respectiva llave privada para descifrar [4].

En base en [5] un criptosistema se define como la quíntupla: (m, c, k, E, D), donde:

- m representa el conjunto de todos los mensajes sin cifrar (texto plano) que pueden ser enviados.
- c representa el conjunto de todos los posibles mensajes cifrados, o criptogramas.
- k representa el conjunto de llaves que se pueden emplear en el criptosistema.
- E es el conjunto de transformaciones de cifrado o familia de funciones que se aplica a cada elemento de m para obtener un elemento de c.

Existe una transformación diferente E^k para cada valor posible de la llave k.

- D es el conjunto de transformaciones de descifrado, análogo a E.

La clasificación de los criptosistemas se hace en función de la disponibilidad de la llave de cifrado-descifrado. Existen por tanto, dos grandes grupos de criptosistemas que son [6]:

a) Criptosistema de llave secreta (llave privada, llave única o simétrico).
b) criptosistema de llave pública (o asimétrico).

El esquema general de un criptosistema simétrico se puede apreciar en la Fig. 1.1. En este caso, A quiere enviar un mensaje m a B. Para hacerlo, cifra el mensaje m con la llave secreta k y el algoritmo de cifrado E. Así, envía el texto cifrado c a B. B aplica a c el algoritmo de descifrado D con la misma llave k y obtiene el texto en claro m.

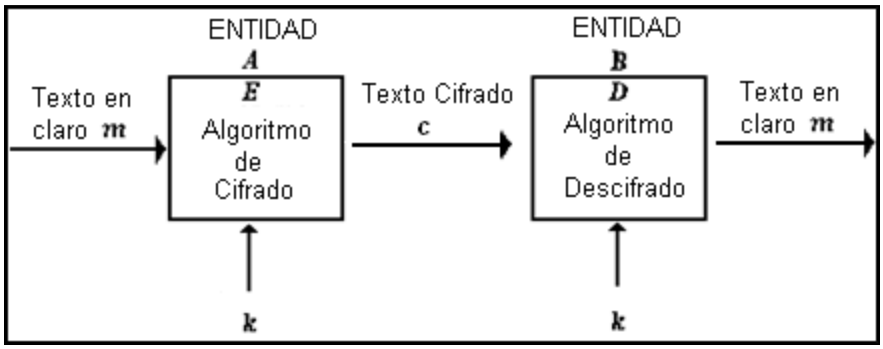

Fig. 1.1 Esquema general de un criptosistema simétrico.

El esquema general de un criptosistema asimétrico se puede apreciar en la Fig. 1.2. En este caso, A quiere enviar un mensaje m a B. Para hacerlo realiza lo siguiente $E_{e_B\,(m)=c}$ es decir, cifra el mensaje m con la llave pública de B (e_B) y el algoritmo de cifrado E, así, envía el texto cifrado c a B. B realiza lo siguiente: $D_{d_B\,(c)=m}$ es decir, aplica a c el algoritmo de descifrado D con su llave privada d_B y obtiene el texto en claro m.

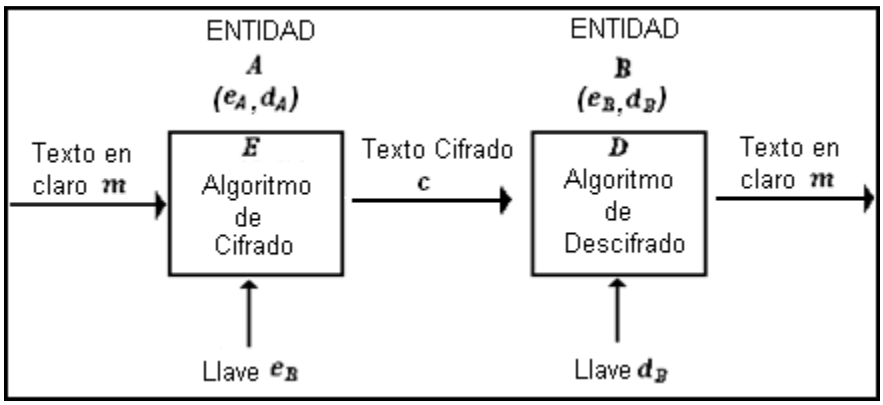

Fig. 1.2 Esquema general de un criptosistema asimétrico.

Uno de los principios básicos que rigen la criptografía es el principio de Kerckhoffs. Este principio se fundamenta en el hecho de que la seguridad de un criptosistema se basa únicamente en su llave secreta. Es decir, un criptosistema es bueno cuando se puede describir todo su funcionamiento y a pesar de ello un adversario no puede descifrar el texto cifrado del criptosistema sin conocer la llave. Dado que uno de los posibles ataques que pueden darse en un criptosistema es el de intentar probar todas las llaves (ataque por fuerza bruta), el número de llaves posibles es un factor importante cuando se trabaja con criptosistemas. Teniendo en cuenta que se acostumbra que la llave sea un número, el número de llaves posibles se encuentra estrechamente vinculado a la longitud de la llave, así en una longitud de la llave de cuatro dígitos, tomando en cuenta el alfabeto: {0 al 9}, tenemos que con 10^4 = 10,000 pruebas ya se habrían probado todas las llaves, mientras que si se toman llaves de ocho dígitos en el mismo alfabeto, se precisan 10^8 = 100,000,000 pruebas para verificar todas las llaves.

Normalmente se hace referencia a la longitud de la llave en bits, así una llave de 40 bits de longitud indica que son necesarias 2^{40} = 1,099,511,627,776 pruebas para encontrarla por fuerza bruta. Esto hace que se hable de criptografía fuerte o de criptografía débil según la longitud de la llave que se utiliza.

1.1.1. Vulnerabilidades, ataques y amenazas

A continuación se explicarán algunos conceptos con base en [7].

Un compromiso de seguridad es cualquier forma de pérdida o daño en un sistema de cómputo, por lo que comprometer la seguridad de este último equivale a provocar pérdida o daño al mismo.

Una vulnerabilidad consiste en cualquier debilidad que pueda explotarse para provocar un ataque a un sistema, por lo que el punto más débil de seguridad de este último consiste en el punto de mayor vulnerabilidad del mismo.

Una amenaza es cualquier circunstancia potencial suficiente para causar pérdida o daño al sistema. Algunos ejemplos de amenazas son los ataques humanos (quemar, golpear, romper, etc.), los desastres naturales, errores humanos inadvertidos (derramar agua, tirar al piso, etc.), fallas internas del hardware o del software, etc. Existen cuatro tipos de amenazas principales, que explotan las vulnerabilidades de un sistema. Estas amenazas son: interrupción, intercepción, modificación y fabricación.

Esquemáticamente estas amenazas se representan en la Fig. 1.3, en donde la entidad A representa al emisor, fuente u origen de los datos, B representa al receptor o destino de ellos e I representa al intruso, tanto A, B e I pueden ser entidades, procesos, dispositivos o computadoras.

En la interrupción las partes del sistema se pierden, se hacen no disponibles o no utilizables, como la destrucción maliciosa del hardware, el borrado de programas y archivos de datos.

La intercepción significa que a una parte no se le autoriza y/o no tiene permitido leer el contenido de un mensaje, entonces esta parte no autorizada puede ser una entidad, un proceso u otro sistema de cómputo. Algunos ejemplos son el copiado ilícito de programas o la intervención del canal para obtener datos sobre la red.

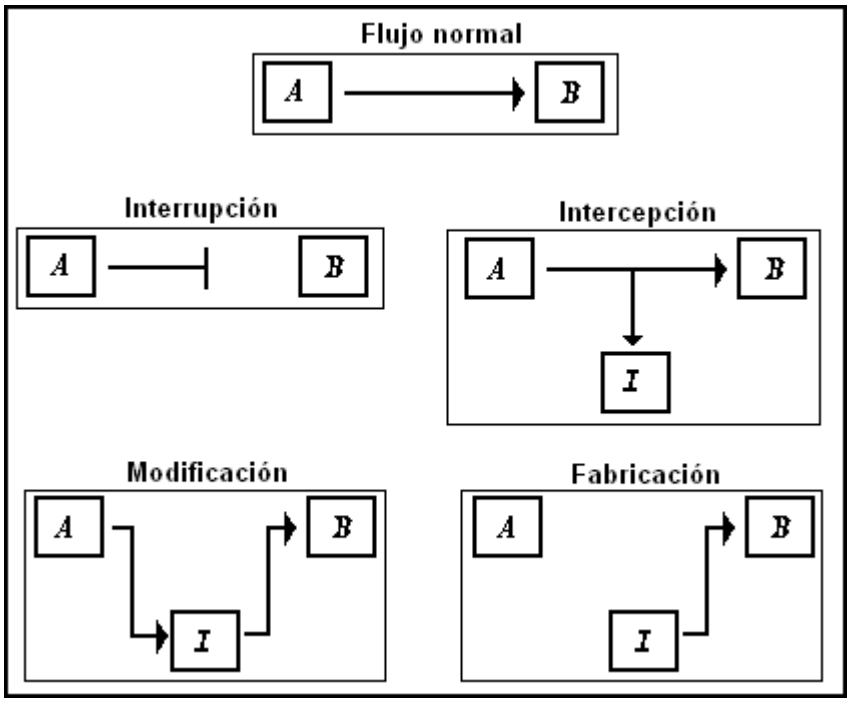

Fig. 1.3 Tipos de Amenazas

La modificación es cuando una parte no autorizada logra acceso al activo del sistema y puede manipularlo. Por ejemplo el intruso puede cambiar el contenido en una base de datos, alterar un programa para realizar un cálculo distinto para el que fue diseñado, modificar datos en una comunicación, etc.

La fabricación consiste en que una parte no autorizada puede fabricar objetos falsos en un sistema. Por ejemplo la inserción de transacciones en un sistema de comunicación en red o agregar registros en una base de datos ya existente.

Un ataque se define como cualquier acción que explota una vulnerabilidad. Existen diversos tipos de ataques los cuales se dividen en ataques pasivos y activos.

Un ataque pasivo consiste en solo observar comportamientos o leer información, sin alterar el estado del sistema ni la información. En este sentido este tipo de ataque atenta contra la confidencialidad.

Un ataque activo tiene la capacidad de modificar o afectar la información o el estado del sistema o a ambos, por lo que este tipo de ataques no solo afecta la confidencialidad o la privacidad sino también la integridad y la autenticidad.

1.2. CARACTERÍSTICAS DE LOS CRIPTOSISTEMAS

El elemento más importante de todo criptosistema es el cifrador, que ha de utilizar el algoritmo de cifrado para convertir el texto claro en un criptograma, pero para poder hacer esto, el cifrador depende de un parámetro exterior llamado llave de cifrado y para el descifrador se le llama llave de descifrado, que es aplicado a una función matemática irreversible (al menos computacionalmente): no es posible invertir la función a no ser que se disponga de la llave de descifrado. De esta forma, cualquier conocedor de la llave y de la función matemática, será capaz de descifrar el criptograma y nadie que no conozca dicha llave será capaz de descifrarlo, aún en el caso de que se conozca la función utilizada.

Cuando dos entidades quieren comunicarse seguramente, lo hacen a través de criptosistemas, esto les permite obtener confidencialidad de su información.

Un criptosistema presenta la estructura que se muestra en la Fig. 1.4. [6].

El emisor (entidad A) envía un texto en claro, que es transformado por el cifrador a través de un algoritmo de cifrado y con la ayuda de una cierta llave k, creando un texto cifrado (criptograma). Este criptograma llega al descifrador a través de un canal de comunicación (comúnmente algún tipo de red) y así convierte el criptograma de nuevo en texto claro, apoyándose ahora en otra llave (dependiendo del tipo de criptosistema, la llave puede ser o no la misma para cifrar y descifrar). El texto claro ha de coincidir con el emitido inicialmente para que se cumplan los principios básicos de la criptografía: en este hecho radica toda la importancia de los criptosistemas.

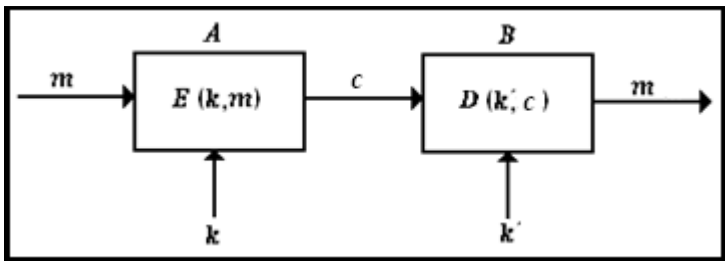

Fig. 1.4 Estructura de un criptosistema.

1.2.1. Criptosistema de llave secreta

La llave de cifrado k puede ser calculada a partir de la descifrado $k´$ y viceversa. En la mayoría de estos sistemas, ambas llaves coinciden y han de mantenerse como un secreto entre emisor y receptor, si un atacante descubre la llave utilizada en la comunicación, podrá romper el criptosistema.

El hecho de que exista al menos una llave de cifrado y descifrado entre cada dos entidades de un sistema hace impráctico la existencia de criptosistemas simétricos en las grandes redes de computadoras de hoy en día, ya que para N entidades se precisan: $N(N-1)/2$ llaves diferentes, lo cual es muy difícil en grandes sistemas.

Estos sistemas a su vez se dividen en dos grandes grupos que son: los cifradores de flujo que cifran bit por bit el texto claro y por otro

lado se tienen los cifradores de bloque que cifran bloques de bits (comúnmente cada bloque es de 64 bits) como una única unidad.

1.2.2. Criptosistema de llave pública

En este tipo de criptosistemas la llave de cifrado se hace de conocimiento general (se le llama llave pública). Sin embargo, no ocurre lo mismo con la llave de descifrado (llave privada), que se ha de mantener en secreto, ambas llaves no son independientes, pero a partir de la llave pública no es posible deducir la privada. Por lo tanto para cada entidad se tiene un par de llaves, pública ($e_{ENTIDAD}$) y privada ($d_{ENTIDAD}$). La existencia de ambas llaves diferentes, para cifrar o descifrar hace que también se conozcan a estos criptosistemas como asimétricos.

Cuando un receptor desea recibir información cifrada, ha de hacer llegar a todos las entidades, su llave pública, para que éstos cifren los mensajes con dicha llave. De este modo, el único que podrá descifrar el mensaje será el legítimo receptor mediante su llave privada.

1.3. PROTOCOLOS

Un protocolo es un acuerdo entre dos o más partes para realizar algo específico, utiliza una o más técnicas criptográficas, para obtener uno o varios servicios de seguridad.

Un protocolo tiene las siguientes características:

a) Resuelve un cierto problema o produce cierto resultado.
b) El protocolo consiste en una serie de pasos bien definidos, es decir que el protocolo cubre todas las posibles situaciones que pueden surgir durante su ejecución, así cuando todos los pasos se hayan seguido exactamente, el problema dado tiene que haber sido resuelto.

c) El protocolo involucra a dos o más partes.
d) Todas las partes involucradas conocen el protocolo y están de acuerdo en seguirlo.
e) El protocolo define claramente lo que cada parte gana o expone con su ejecución.

Existen tres tipos de protocolos: arbitrados, adjudicados y autoimplementados.

Un protocolo arbitrado se basa en una tercera parte confiable para realizarse. El árbitro no tiene ningún tipo y forma de preferencia por ninguna de las partes involucradas. En la vida real es el papel que debe jugar un juez.

Un protocolo adjudicado es una variante de los arbitrados, también se basan en una tercera parte confiable, pero esta parte, sin embargo, no siempre es requerida. Las partes involucradas ejecutan el protocolo tal como está especificado, si todas las partes respetan el protocolo, el resultado se logra sin ayuda de una tercera parte, llamada adjudicador, pero solo en el caso de que una de las partes involucradas piense que las otras partes no respetan el protocolo, entonces se invoca al adjudicador el cual analiza el problema y las reglas y dice quién está actuando bien y que es lo que se debe hacer.

Los protocolos autoimplementados son los mejores protocolos ya que se diseñan de tal manera que hacen virtualmente imposible el engaño, no requieren arbitro ni juez, garantizan que si cualquier participante en el protocolo engaña, el engaño es descubierto inmediatamente por el otro u otros participantes [7].

Existe una amplia variedad de protocolos criptográficos que dan respuesta a diferentes objetivos, además de ser un tema muy amplio también

es de rápido crecimiento. A continuación se mencionaran algunos protocolos, de acuerdo a [8]:

a) *Protocolos de Autenticación de Entidades:* Permiten garantizar que el remitente de un mensaje o la entidad con la que se establece comunicación, es realmente quien pretende ser.
b) *Protocolos de Autenticación del Mensaje:* Garantizan que el mensaje enviado no ha sido substituido por otro ni alterado (integridad del mensaje).
c) *Distribución de llaves:* Un problema importante en el sistema simétrico es la creación y transporte de las llaves a utilizar por cada par de entidades. En cuanto a las llaves de un sistema asimétrico, la problemática de su distribución es distinta (no es necesario el secreto), demandando protocolos específicos.
d) *Protocolos para Compartir Secretos:* Su objetivo es distribuir un secreto (por ejemplo la llave para abrir una caja fuerte), entre un conjunto P de participantes, de forma que ciertos subconjuntos prefijados de P puedan, uniendo sus participaciones, recuperar dicho secreto.
e) *Pruebas de Conocimiento Nulo:* Permiten a un individuo convencer a otro de que posee cierta información, sin revelarle nada sobre el contenido de la misma.
f) *Transacciones Electrónicas Seguras:* Permiten realizar de manera electrónica segura las operaciones bancarias habituales, firma electrónica de contratos, etc.
g) *Compromiso de bit:* Permiten a una entidad A comprometerse con una elección (un bit o más generalmente una serie de bits) sin revelarla hasta un momento posterior. El protocolo garantiza a otra entidad B que A no cambia su elección.
h) *Transferencias Trascordadas***:** Permiten a una entidad A enviar a otra B un mensaje o secreto entre dos posibles. A no conoce cuál de los dos ha recibido realmente B.

i) *Elecciones Electrónicas:* Permiten realizar un proceso electoral electrónicamente, garantizando la deseable privacidad de cada votante y la imposibilidad de fraude.

j) *Jugar al Póker por Internet:* Posibilita a dos entidades, físicamente separadas, mantener una partida de póker (o similar: cara o cruz, chinos, etc.), comunicándose por correo electrónico, teléfono, etc., garantizando la imposibilidad de hacer trampa.

1.4. ESTADO ACTUAL

La criptografía cubre hoy en día diferentes objetivos, a veces alejados del tradicional y más conocido que es la transmisión secreta de información. Este tipo de aplicaciones se engloba dentro de lo que se denomina Protocolos Criptográficos.

Como se mencionó anteriormente un protocolo criptográfico es un conjunto bien definido de etapas que implican a dos o más entidades y es designado para realizar una tarea específica que utiliza como herramienta algún algoritmo criptográfico.

En este trabajo se tratarán los protocolos de establecimiento de llaves, los cuales, en base en [3], se dividen de la siguiente forma:

a) Transporte de llave basado en cifrado simétrico.
b) Acuerdo de llave basado en técnicas simétricas.
c) Transporte de llave basado en cifrado de llave pública.
d) Acuerdo de llaves basado en técnicas asimétricas.

Se debe tomar en cuenta que algunos protocolos de establecimiento de llave pueden o no incluir una entidad centralizada o de confianza (servidor).

1.5. PROBLEMÁTICA

La identificación es muy importante en el intercambio de información electrónica que involucra a dos o más entidades, es así que el objetivo de los protocolos de acuerdo de llave es que un secreto compartido llegue a estar disponible para dos o más entidades, este secreto puede ser utilizado para la identificación de las entidades y/o para llaves criptográficas, sobre todo si están conectados en red.

Los problemas más comunes que se encuentran en una red son:

a) No se cuenta con un mecanismo que permita conocer la identidad de las entidades que se comunican.
b) No se cuenta con un sistema de seguridad basado en la criptografía.
c) No existen registros sobre el control de acceso a la información y/o recursos.
d) En el intercambio de información, la información puede ser alterada.
e) La información transmitida no puede ser confirmada, ni en su envío ni en su recepción.
f) De igual forma no se puede confirmar quien envió la información y quien la recibió.

Estos problemas pueden resolverse usando protocolos de establecimiento de llave, que garanticen el intercambio seguro de secreto(s) compartido(s), lo que puede utilizarse como llave(s) secreta(s). No obstante existe una gran variedad de ellos y resulta difícil saber cuál es el protocolo apropiado para cada necesidad, por lo que es necesario conocer sus características y funcionamiento, para su selección, en base a la descripción de los mismos.

Describir los protocolos de establecimiento y administración de llave permitirá conocer las características de éstos para examinar su funcionamiento con énfasis en sus ventajas y desventajas, para

posteriormente en base a los conocimientos obtenidos sobre estos, poder seleccionar un protocolo conveniente para ambientes informáticos con altas restricciones de seguridad.

Adicionalmente los protocolos de establecimiento de llave implican la necesidad de la administración de las llaves, siendo sus beneficios:

a) Evitar la intervención de terceras entidades distintas de alguna Institución propia en el manejo de sus propias llaves.
b) Evaluar y controlar la creación de las llaves para las diferentes entidades que la requieran.
c) Evaluar y controlar la revocación de las llaves, ya sea porque caduca la misma, porque alguna entidad causó baja o ya no la requiere.
d) Evaluar y controlar la actualización de las llaves si es que se requiere después de la revocación y/o eliminación.
e) Evaluar y controlar la y eliminación de las llaves después de ser evaluadas de la revocación.
f) Evaluar y controlar el almacenamiento histórico de las llaves después de ser revocadas.

Para que un protocolo de intercambio de llaves tenga éxito es necesario asegurar la identificación de las entidades, ya que de otra forma el protocolo puede ser víctima de alguna entidad maliciosa mediante ataques como “el hombre en medio”, “usurpación de identidad” entre otros. También se debe tomar en cuenta que aunque se haya realizado el intercambio de llaves de forma satisfactoria, existe la necesidad y la problemática de administrar las llaves públicas de las entidades. Esto se enlista en los siguientes puntos:

a) Autenticidad de llave. Como se mencionó anteriormente el objetivo primario de la autenticación de la llave pública de una entidad es evitar ataques como hombre en medio y usurpación de identidad.

b) Actualización de llaves. Cada par de llaves debe ser cambiado después de un determinado periodo de validez.
c) Revocación de llaves. Cuando alguna entidad comprometa (pierda, olvide, borre, etc.) su llave privada, ésta debe ser eliminada para posteriormente generar una nueva.
d) Eliminación de llaves. Se refiere al hecho de que si un empleado deja de laborar en la organización, su respectiva llave pública debe ser eliminada automáticamente.

1.5.1. Problemas con las llaves

Existe el problema que se deriva de tener que administrar y proteger numerosas llaves, necesarias para acceder a los diferentes servicios que el trabajo en red nos ofrece.

Usar una misma llave para muchas operaciones es peligroso, ya que conforme pasa el tiempo es cada vez más probable que alguien acceda a la llave, con el consiguiente peligro que esto conlleva. Tanto es así que, por ejemplo, muchos administradores de una red o sistema obligan a las entidades de la misma a cambiar forzosamente sus llaves de acceso, estableciendo fechas de caducidad. Los sistemas asimétricos no representan ningún problema a la hora de cambiar las llaves, ya que la distribución de las llaves públicas es abierta, con lo que en seguida podrán acceder a las nuevas llaves las entidades interesadas. Pero en los sistemas simétricos el cambio de la llave origina un trastorno considerable, ya que se debe distribuir esa nueva llave a todas las entidades con las que se requiere comunicarse con seguridad.

CAPITULO 2. ACUERDO, ESTABLECIMIENTO Y ADMINISTRACIÓN DE LLAVE

2.1. CONCEPTOS FUNDAMENTALES

2.1.1. Tipos de llave

Una llave criptográfica es un parámetro de entrada que varía la transformación realizada por un algoritmo criptográfico, es decir es una secuencia de símbolos que controlan las operaciones de cifrado y descifrado [1].

Con base en [9] se definen tres tipos de llaves:

- Llaves de sesión
- Llaves de sistema
- Llaves maestras

a) Llaves de sesión

Son utilizadas en una sesión únicamente y permiten cifrar y descifrar los mensajes que envían las entidades.

La llave de sesión es: un tipo de llave que se deriva de secreto(s) compartidos por la(s) entidad(es). Esta llave es intercambiada frecuentemente [10]. Este tipo de llave se ilustra en la Fig. 2.1.

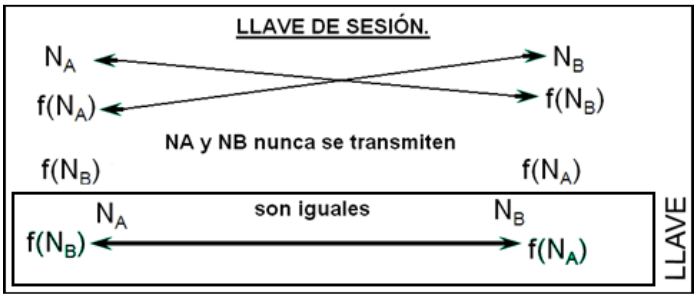

Fig. 2.1 Acuerdo de llave de sesión.

b) Llaves de sistema:

Son utilizadas entre los servidores o entre un servidor y un cliente para definir un canal seguro, cifrando la información. Este tipo de llave se ilustra en la Fig. 2.2.

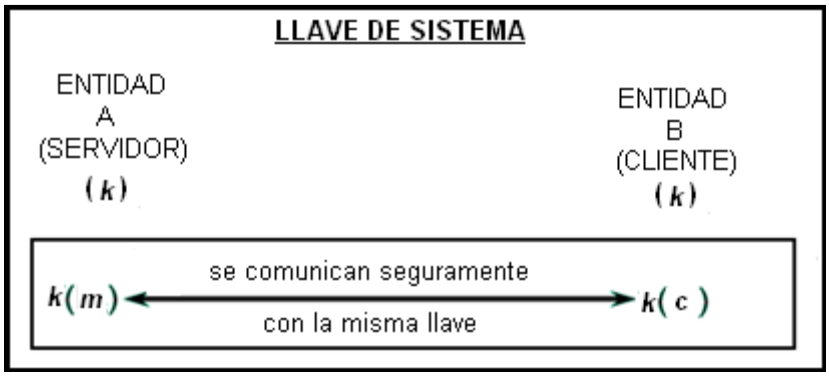

Fig. 2.2 Llave de Sistema.

c) Llaves maestras (o de servidor):

Son utilizadas para cifrar las otras llaves almacenadas dentro del servidor. Este tipo de llave se ilustra en la Fig. 2.3.

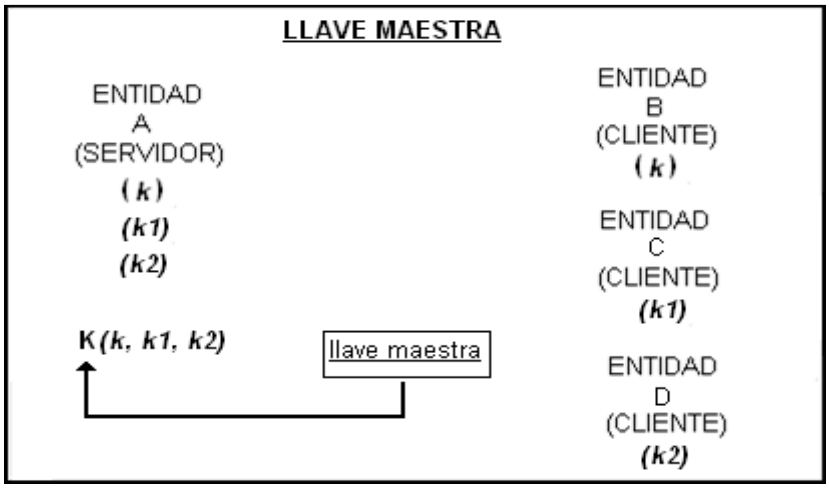

Fig. 2.3 Llave Maestra.

A continuación se mencionan algunos conceptos fundamentales tratados en [3].

2.1.2. Jerarquía de llave

La confidencialidad puede ser subclasificada de la naturaleza de la información que está siendo protegida: datos de entidades vs llave.

Esto sugiere una jerarquía de varios niveles de llave como sigue:

a) Llaves maestras: llaves en el más alto nivel de la jerarquía, en donde ellas mismas no son criptográficamente protegidas. Estas son distribuidas manualmente o instaladas inicialmente y se protegen por procedimientos de control y procedimientos físicos o aislamiento electrónico.
b) Llaves que cifran llaves: las llaves de cifrado simétrico o llaves públicas utilizadas para transportar o almacenar llave de otras llaves ejemplo: en los protocolos de transporte de llave. Estos pueden ser llamados: llaves de transporte de llave y pueden ellas mismas ser aseguradas bajo otras llaves.
c) Llaves de datos: usadas para proveer operaciones criptográficas a los datos de la entidad (cifrado y autenticación). Estos son generalmente llaves simétricas de corto plazo; sin embargo las llaves privadas para firmas digitales en criptografía asimétrica, son usualmente llaves de largo plazo.

Las llaves de una capa son usadas para proteger información de alguna capa inferior. Esta limitación está destinada para hacer que los ataques sean más difíciles y limitar la exposición de comprometer una llave específica.

2.1.3. Criptoperiodos, llaves de largo plazo y llaves de corto plazo

El criptoperiodo de una llave es el tiempo sobre el cual ésta es válida para usar por partes legítimas.

Los criptoperiodos pueden servir para:

a) Limitar la información (relacionada a una llave específica) disponible para criptoanálisis.
b) Limitar la exposición en el caso de comprometer una llave simple.
c) Limitar el uso de una tecnología particular para su tiempo efectivo de vida estimado.
d) Limitar el tiempo disponible para ataques de criptoanálisis intensivos computacionalmente (en aplicaciones donde la protección de la llave de largo plazo no se requiere).

Además de la jerarquía de llave, éstas pueden ser clasificadas basadas en consideraciones temporales como sigue:

a) Llaves de largo plazo: estas incluyen llaves maestras, a menudo las llaves que cifran llaves y las llaves usadas para facilitar acuerdo de llave.
b) Llaves de corto plazo: éstas incluyen llaves establecidas para transportar llaves o para acordar llaves y a menudo son usadas como llaves de datos o llaves de sesión para una sesión de comunicación simple.

En general las aplicaciones de comunicaciones incluyen llaves de corto plazo, mientras las aplicaciones para almacenar datos requieren llaves de largo plazo. Las llaves de largo plazo típicamente protegen llaves de corto plazo. Las llaves Diffie-Hellman son una excepción en algunos casos, ya que para obtener éstas, se establecen secretos compartidos con datos que pueden viajar en claro por la red y por tanto no necesitan ser protegidos por ninguna llave. Los criptoperiodos limitan el uso de llaves de periodos fijos, tras lo cual deben ser remplazados.

2.2. CLASIFICACIÓN DE LOS PROTOCOLOS

El ámbito de los protocolos criptográficos es lo suficientemente amplio como para hacer necesario el establecimiento de criterios de clasificación de los mismos. Así, si se atiende al número de entidades que intervienen, se puede distinguir entre protocolos *bipartitos* y *multipartitos*. En los primeros, el número de entidades directamente implicadas se limita a dos, mientras que en los otros sólo existe la restricción sobre la finitud de dicho número.

Otra clasificación se puede realizar en función de si existe un intercambio recíproco de información entre las entidades, es decir si están establecidas las figuras de emisor y receptor. Siguiendo este razonamiento, se realiza la siguiente diferenciación:

a) Si durante el desarrollo del algoritmo una entidad tiene el papel de emisor y su contrario intenta obtener la entrada del primero o una transformación de ésta, se trata de un *protocolo unilateral* o *unidireccional*. Esto es lo que sucede en protocolos tales como la transferencia inconsciente, las demostraciones de conocimiento nulo, etc.
b) Si por el contrario, todos los participantes juegan idénticos papeles siendo emisor y receptor a la vez se habla de *protocolo multilateral*, *multidireccional* o *de intercambio mutuo* (bilateral o bidireccional en el caso de los bipartitos). Esta situación se produce en protocolos tales como la firma de contratos, el lanzamiento de monedas, etc. [11].

2.3. ESTABLECIMIENTO DE LLAVE

Establecimiento de llave es un proceso o protocolo por el cual un secreto compartido llega a estar disponible para dos o más entidades, estos secretos pueden ser: llaves simétricas que pueden tener propósitos criptográficos incluyendo el cifrado, entre otros. También incluyen aspectos

más amplios de gestión de llave incluyendo: distribución de llaves públicas, certificados y ciclo de vida de las llaves.

Los protocolos de establecimiento de llave se clasifican en dos tipos: a) distribución de llave y b) acuerdo de llave, ver Fig. 2.4. El primero es una técnica en donde una entidad crea u obtiene un valor secreto y lo transfiere de forma segura a otro(s). El segundo es una técnica en la cual un secreto compartido es derivado por dos o más entidades como una función de información asociada por cada uno de éstos (idealmente) tal que ninguna entidad puede predeterminar el valor del resultado.

Fig. 2.4 Distribución de llave VS Acuerdo de llave.

Los esquemas de establecimiento de llave dinámica son aquellos en los que la llave que se crea por un par o grupo de entidades varía en ejecuciones posteriores. También es conocido como: establecimiento de llave de sesión, estas llaves son dinámicas, lo que permite a los protocolos ser inmunes a los ataques de llave que se verán en el punto 2.2.2.

También existen los protocolos basados en identidad. Se dice que los protocolos de establecimiento de llave son basados en la identidad, si la información de identidad (ejemplo: nombre y dirección o un índice de identificación) de la entidad implicada, es usada como la llave pública de la entidad (dependencias, instituciones, entidades, procesos, etc.).

Con base en [12] el establecimiento de llaves secretas es uno de los mayores problemas de la criptografía simétrica. Es así que solamente existen 2 formas de direccionar el problema del establecimiento de llave: la primera es el uso de una KDC, tal como Kerberos y la segunda es el uso de un protocolo de establecimiento de llave.

2.3.1. Adversarios en protocolos de establecimiento de llave

La comunicación entre las entidades en los protocolos de establecimiento de llave son llamados: “principales”, y se asume que tienen nombres únicos. Además de las entidades legítimas se puede tener la presencia de terceras entidades no autorizadas, las cuales tienen los siguientes nombres: oponente, intruso, atacante, adversario, etc.

Cuando se habla de la seguridad de los protocolos, se asume que los mecanismos criptográficos son usados como algoritmos de cifrado y esquemas de firma digital. Un adversario no hace ataques de criptoanálisis directamente a los mecanismos que integran un protocolo sino que analiza la manera en la cual éstos son combinados, por lo que ataca el protocolo mismo. Es decir, aprovecha las debilidades que tiene el uso y combinación de los mecanismos y no los ataca directamente.

Cuando dos o más entidades se comunican mediante un protocolo, los mensajes son transmitidos sobre redes inseguras, en donde un adversario puede tener control de los datos y con la habilidad de grabar, alterar, insertar, redireccionar, reordenar, e inyectar nuevos mensajes. Así mismo un adversario puede también ser capaz de comunicarse con entidades autorizadas inexpertas para iniciar un nuevo protocolo.

Un adversario en un protocolo de establecimiento de llave puede establecer muchas estrategias lo que incluye intentar:

a) Deducir una llave de sesión usando información ganada por escuchas.
b) Participación encubierta en un protocolo iniciado por una entidad con otro, para alterar mensajes así como estar disponible para deducir la llave.
c) Iniciar uno o más protocolos (posiblemente simultáneamente) y combinar mensajes de uno con otros, así como enmascarar algunas entidades o llevar a cabo ataques (activos y/o pasivos).

2.3.2. Secrecía perfecta y ataques de llave conocidos

En el análisis de protocolos de establecimiento de llave, se debe considerar el impacto de compromiso de varios tipos de llave, incluso si tal compromiso no es normalmente esperado. Comúnmente se considera el efecto siguiente:

a) Compromiso de llaves secretas a largo plazo (simétrico o asimétrico).
b) Compromiso de llaves de sesión pasadas.

Un protocolo tiene perfección del secreto avanzado si el compromiso de llaves de largo plazo no compromete llaves de sesión pasadas.

Un protocolo es vulnerable a un ataque de llave conocida si el compromiso de las llaves de sesión pasadas, permite incluso a un adversario pasivo comprometer llaves de sesión futuras o suplantación por un adversario activo en el futuro.

Ataques de llaves conocidos sobre protocolos de establecimiento de llave son ataques análogos para texto conocido sobre algoritmos de

cifrado. Un motivo para su consideración es que en algunos ambientes (debido a la implementación y decisiones de ingeniería), la probabilidad del compromiso de llaves de sesión puede ser mayor que el de llaves de largo plazo.

En algunos sistemas las llaves de sesión pasadas pueden ser descubiertas por varias razones (después de la autenticación, para posiblemente detectar el uso del canal de autenticación como un canal cubierto o escondido).

2.3.3. Uso de servidores de confianza

Muchos protocolos de establecimiento de llave incluyen una entidad centralizada o de confianza. Esta entidad es conocida por una gran variedad de nombres dependiendo del rol que juegue, estos nombres son: TTP (Trusted Third Party – Tercera parte de confianza), Servidor de confianza, Servidor de autenticación, KDC (Key Distribution Center – Centro de Distribución de Llave), KTC (Key Translation Center – Centro de Traslación de Llave) y CA (Certification Authority – Autoridad Certificadora) [2].

2.4. ADMINISTRACIÓN DE LLAVE

Schneider en [8] establece que una de las partes más difíciles de la criptografía es la administración de llaves, de igual forma Kaeo en [13] reconoce que el manejo de las llaves es un problema crítico dentro de la seguridad de los sistemas de comunicación ya que depende de factores sociales más que técnicos. El Instituto Nacional de Estándares y Tecnología (NIST) del Gobierno de los Estados Unidos desarrolló en el FIPS-171, con base en el estándar X9.17 de generación de llaves, un manual de procedimiento para la administración de llaves simétricas.

2.4.1. Políticas

La propia administración de llaves criptográficas es esencial para el uso efectivo de la seguridad criptográfica. Las llaves son análogas a la combinación de la seguridad. Si una combinación segura llega a ser conocida a un adversario, la seguridad más fuerte no provee seguridad contra los ataques. Similarmente una pobre administración de llave puede fácilmente comprometer algoritmos fuertes. La seguridad de la información protegida con criptografía depende directamente de la fortaleza de las llaves. Todas las llaves necesitan ser protegidas contra modificaciones y las llaves privadas necesitan ser protegidas contra la divulgación no autorizada. La administración de llaves provee la base para la generación, almacenamiento, distribución y destrucción de llaves de forma segura [14].

El problema que se plantea en una red de computadoras es asegurar las comunicaciones entre las entidades que la conforman y que se quieren comunicar. Las soluciones que se han visto para esto utilizan llaves de cifrado.

En el caso de los algoritmos simétricos alguien tiene que distribuir las llaves secretas que se van a utilizar. En el caso de algoritmos asimétricos es necesario que alguien certifique la validez de las llaves públicas.

Una de las soluciones para resolver este problema es la administración de llaves.

2.4.2. Proceso de Administración de llave

La administración de llaves involucra su: generación, autenticación, almacenamiento y distribución [15].

El proceso de administración de llave se ilustra en la Fig. 2.5.

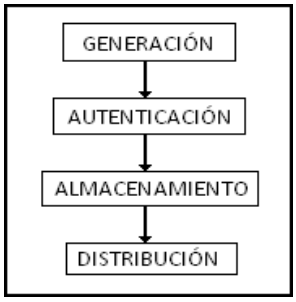

Fig. 2.5 Procesos de administración de llave.

a) Generación

Se refiere a la creación de las llaves de acuerdo con ciertos requerimientos; la autenticación al proceso de validar el origen que hace la petición del servicio de las llaves; el almacenamiento involucra salvaguardar la integridad, disponibilidad y confidencialidad de las llaves durante su tiempo de vida y la distribución es el proceso de transferir las llaves de manera segura a las entidades participantes.

La generación de llaves es un proceso crítico ya que de nada sirve tener un algoritmo robusto si se tiene una llave débil. Es importante señalar que toda información cifrada es sujeta a un ataque de fuerza bruta, es decir, probar todo el espacio de llaves. Un ataque más adecuado es el de diccionario en el que solo se prueba el espacio más común. Por ejemplo, DES utiliza una llave de 56 bits, lo cual da un espacio de llaves de 2^{56}. Sin embargo, un método pobre para la generación de llaves puede reducir el espacio por ejemplo hasta 2^{40} lo cual implica hacer un ataque de fuerza bruta 10 mil veces más sencillo. Esto es debido a que la generación de llaves se delega a las entidades, estos por lo general escogen llaves débiles lo cual hace más fácil el comprometer la seguridad de

la información. Es importante señalar que el algoritmo sigue siendo el mismo y la fortaleza del sistema depende directamente de la llave. Se puede tener un algoritmo muy robusto pero si elegimos una llave débil todo el sistema será débil. Se debe recordar que la seguridad es tan fuerte como el más débil de los eslabones, y definitivamente en la generación de las llaves se tiene un eslabón bastante débil. Sin embargo, se debe decir que la solución es sencilla, es más ni siquiera se necesita un sofisticado método para la elección de la llave, sólo se requiere que ésta tenga dimensión y entropía acorde a la sensibilidad de la información.

Una solución más compleja al problema de la generación de llaves es utilizar un generador de números pseudo-aleatorios. Como comentaba Kaeo en [13], efectivamente se involucra el factor humano dentro de la elección de las llaves, por lo que se tiene que ser severo en la política para asegurar que éste no será el eslabón más débil.

La generación de llaves es un factor que puede comprometer la seguridad del esquema, ya que puede ser que la información cifrada resida en el sistema conectado al ambiente hostil, entonces podría ser robada, ya que se parte del hecho que los sistemas pueden ser penetrados, y aplicársele un ataque de fuerza bruta o de diccionario. La solución a este problema es que la información cifrada también puede ser distribuida a través de secretos compartidos por lo que ya no reside físicamente en el sistema.

b) La distribución y autenticación

El problema de la distribución y autenticación de las llaves ha sido solucionado por la criptografía asimétrica, toda llave pública (utilizada para el cifrado) tiene una y solo una pareja llamada llave

privada (utilizada para el descifrado). Esta última a su vez es protegida por una llave simétrica.

c) El almacenamiento:

En el caso del almacenamiento de las llaves privadas, éstas por lo general residen en el servidor conectado al ambiente hostil y solo están protegidas con otra llave que es simétrica. Debido a que gran cantidad de información se está cifrando con una sola llave pública y por lo tanto solo puede ser descifrada con su respectiva llave privada, es necesario establecer un esquema de almacenamiento seguro de dicha llave ya que si ésta se compromete, implica que una gran cantidad de información también se comprometa.

Por lo anterior; la administración de llaves criptográficas, es esencial para el uso eficaz de las técnicas criptográficas, ya que cualquier pérdida de llaves puede comprometer la confidencialidad, autenticidad y/o integridad de la información.

El objetivo de la administración de la llave es mantener la relación de la llave y la llave, de manera tal que contrarreste las amenazas tales como [2]:

a) Compromiso de confidencialidad de llaves secretas.
b) Compromiso de autenticidad de llave secreta o llave pública. Los requerimientos de autenticidad incluyen conocimiento o verificabilidad de la identidad verdadera de la parte con la que una llave es compartida o asociada.
c) Uso no autorizado de llave secreta o llave pública. Ejemplos incluyen el uso de una llave la cual no tiene una longitud válida.

2.4.3. Técnicas para distribuir llaves públicas

Los protocolos que incluyen criptografía de llave pública son típicamente descritos asumiendo a priori la posesión de llaves públicas (autenticación) de partes apropiadas. Esto permite generalizar entre varias opciones para adquirir dichas llaves. Las alternativas para distribuir llaves públicas explícitas con garantía o autenticidad verificable, incluye exponenciales públicos como en el acuerdo de llave de Diffie-Hellman, lo cual contiene lo siguiente:

a) Entrega punto a punto sobre un canal de confianza. Las llaves públicas autenticadas de otras entidades son obtenidas directamente de la entidad asociada por intercambio personal, o sobre un canal directo, el cual garantiza la integridad y la autenticidad (ejemplo: mensajería de confianza o mail registrado).
b) Acceso directo a un archivo público de confianza (registro de llave pública). Una base de datos pública, la integridad de esta es de confianza, puede ser configurada para contener el nombre y la llave pública autenticada de cada entidad del sistema. Esto puede ser implementado como un registro de llave pública operado por una parte de confianza. Las entidades adquieren llaves directamente de este registro. Mientras el acceso remoto al registro sobre canales no seguros es aceptable en contra de adversarios pasivos, un canal seguro es requerido para accesos remotos en la presencia de adversarios activos. Un método que autentique un archivo público es la autenticación de árboles de llaves públicas.
c) Uso de un servidor de confianza en línea: Estos proveen acceso al equivalente de un archivo público almacenando llaves públicas autenticadas, regresando una petición de llaves públicas en transmisiones firmadas, la confidencialidad no es requerida. La parte solicitante posee una copia de la firma del servidor verifica la

llave pública, permitiendo verificación de la autenticidad de dichas transmisiones. Algunas desventajas: el servidor de confianza debe estar en línea, puede llegar a tener cuellos de botella y los enlaces de comunicación deben de estar establecidos con la entidad receptora y el servidor de confianza.

d) Uso de un servidor fuera de línea y certificados. En un proceso de un tiempo, cada parte A contacta una parte de confianza fuera de línea conocida como Autoridad Certificadora (AC), para registrar su llave pública y obtener la firma de la AC verificando la llave pública (permitiendo la verificación de otros certificados de entidades). La AC certifica la llave pública de A vinculándola a una cadena que identifica a A, así crea un certificado.

e) Uso de sistemas que garantizan la autenticidad de parámetros públicos implícitamente. En este sistema se incluyen los sistemas basados en identidad y aquellos que usan llaves certificadas implícitamente.

2.5. PROTOCOLOS DE ESTABLECIMIENTO Y ADMINISTRACIÓN DE LLAVE

Con base en [2], los protocolos se dividen en sistemas simétricos y asimétricos, los cuales se mencionan a continuación.

2.5.1. Protocolos basados en sistemas simétricos

a) Transporte

Como se mencionó anteriormente los protocolos de transporte o de distribución de llave, permiten transmitir seguramente una llave secreta, con base en [2], la clasificación de estos protocolos basados en sistemas simétricos son:

i. Transporte y derivación de llave simétrica sin un servidor.
ii. Protocolo de intercambio de autenticación de llave 2 (AKEP2).
iii. Transporte de llave sin un acuerdo de llaves a priori.
iv. Kerberos y protocolos basados en servidores.
    A. Protocolo de autenticación Kerberos.
    B. Protocolo de compartimiento de llave de Needham-Schroeder.
v. Protocolo de llave compartida de Needham-Schroeder.

b) Acuerdo

Los protocolos de acuerdo de llave, permiten pactar seguramente una llave, con base en [2], uno de estos protocolos basados en sistemas simétricos es:

i. Sistema de predistribución de llave simétrica de Bloom.

2.5.2. Protocolos basados en sistemas asimétricos

a) Transporte

Con base en [2], la clasificación de los protocolos de transporte o de distribución de llave, que permiten transmitir seguramente una llave, basados en sistemas asimétricos son:

i. Transporte de llave usando cifrado de Llave Pública (PK) sin firma.
    A. Transporte de llave One-pass por cifrado de llave pública.
ii. Protocolo de llave pública de Needham-Schroeder.
iii. Protocolos combinando cifrado PK y firmas.
    A. Cifrando llaves Firmadas.
    B. Cifrado y Firma separadamente.
    C. Firmando Llaves cifradas.
    D. X.509 protocolos de autenticación fuerte.

E. Protocolo X.509 autenticación fuerte 2 caminos (two-pass).
F. Protocolo X.509 autenticación fuerte 3caminos (three pass).

iv. Protocolos híbridos de transporte de llave usando cifrado PK.
A. Protocolo Beller-Yacobi (4-pass).
B. Protocolo Beller-Yacobi (2-pass)

b) Acuerdo

Con base en [2], los protocolos de acuerdo de llave, que permiten establecer un secreto compartido entre dos o más entidades, basados en sistemas asimétricos son:

i. Diffie-hellman y su relación con protocolos de acuerdo de llave.
A. Acuerdo de llave de Diffie-Hellman.
B. ElGamal acuerdo de llave en un paso.
C. MTI Protocolos de acuerdo de llave en dos pasos.
D. Protocolo MTI/A0 acuerdo de llave.

2.6. MODELOS DE ESTABLECIMIENTO DE LLAVES SIMPLES

Una de las cuestiones a tener en cuenta en el diseño de los protocolos es el modelo formal que subyace, entendiendo por modelo formal las condiciones teóricas en las que el protocolo en cuestión es seguro. De tal manera, se distinguen los protocolos seguros ante participantes semi-honestos y los protocolos seguros ante participantes maliciosos [11].

a) Modelo semi-honesto

Se dice que un participante es *semi-honesto* si sigue las reglas del juego pero intenta obtener toda la información que le sea posible a partir de los datos de entrada que reciba del resto de participantes.

b) Modelo malicioso

Se dice que un participante es malicioso si se desvía de manera arbitraria del desarrollo del protocolo en cuestión.

2.6.1. El problema de distribución de llave n^2

En un sistema con n entidades que incluyan técnicas de llave simétrica, si cada par de entidades puede necesitar comunicarse seguramente, cada par debe compartir una llave secreta distinta. En este caso cada parte debe tener n-1 llaves secretas, el número total de llaves en el sistema el cual puede necesitar ser centralmente respaldado, es entonces $n(n-1)/2$, o aproximadamente $n^{2\cdot}$ Como el tamaño de un sistema incrementa, este número llega a ser inaceptablemente grande.

En sistemas basados en técnicas de llave simétrica, la solución es usar servidores de llave centralizados: como en una red con topología de estrella, con una tercera parte de confianza en el centro o un hub de comunicaciones. Para el problema de distribución de llave n^2, las técnicas de llave pública ofrecen una solución alternativa.

2.6.2. Administración de llave punto a punto y centralizada

Las comunicaciones punto a punto y administración de llave centralizada, usan centros de distribución de llave o centros de traslación de llave, son ejemplos de una distribución de llave simple. Aquí “simple” implica incluir al menos una tercera parte. Esto es ilustrado en la Fig. 2.6. en donde k_{XY} denota una llave simétrica compartida por X e Y.

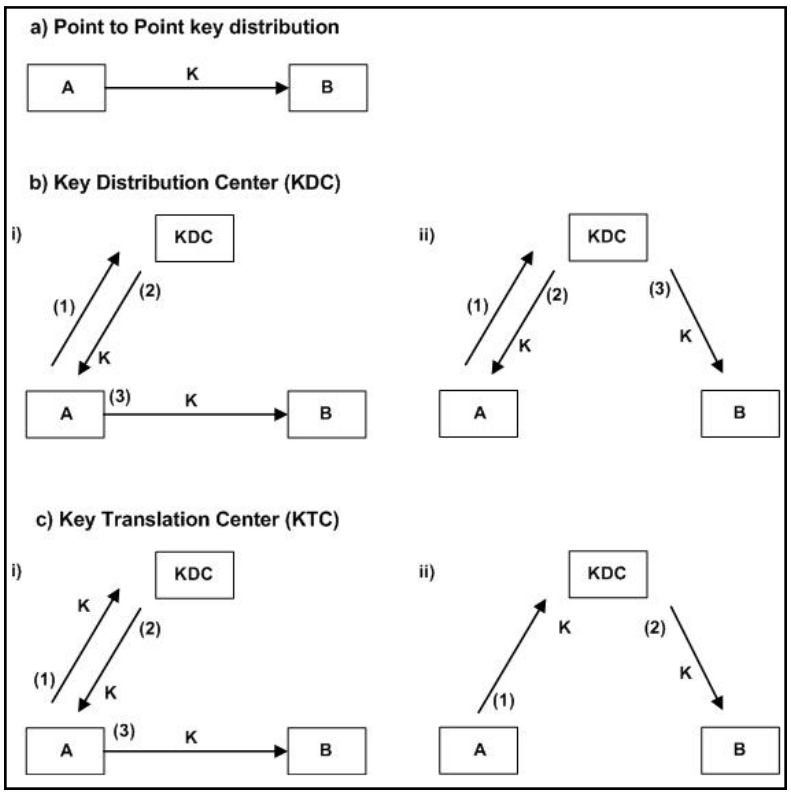

Fig. 2.6 Modelos de distribución de llave simple (llave simétrica)

a) Mecanismos punto a punto. Esto incluye la comunicación de dos partes directamente.

b) Centros de distribución de llaves ($KDCs$). Los $KDCs$ son utilizados para distribuir llaves entre las entidades, las cuales comparten distintas llaves con el KDC pero no con otro.

   Un protocolo básico KDC consiste en: una petición de A para compartir una llave con B, la KDC genera o adquiere una llave k, la envía cifrada con k_{AT} (llave con la que se comunica la entidad A y el KDC) a A, con copia de k (para B) cifrada con k_{BT} (llave con la que se comunica la entidad B y el $KDC\ T$). Alternativamente T puede comunicar k (seguramente con k_{BT}) a B directamente.

   Centros de Traslación de llave ($KTCs$). Los objetivos de las $KTCs$ son parecidas a las $KDCs$, pero aquí una de las partes (por

ejemplo A), suministra la llave de sesión en lugar del centro de confianza.

Un protocolo básico KTC consiste en: A envía una llave k a la KTC cifrado con k_{AT} (llave con la que se comunica la entidad A y el KTC). La KTC descifra y vuelve a cifrar k con k_{BT} (llave con la que se comunica la entidad B y el KTC), luego regresa esta a A (y retransmite a B) o la envía a B directamente.

Las $KDCs$ proveen generación de llave centralizada, mientras que las $KTCs$ distribuyen la generación de llaves. Ambas son técnicas centralizadas e incluyen un servidor de confianza en línea.

2.7 CICLO DE VIDA DE LAS LLAVES

La administración de la llave es más simple cuando todas las llaves criptográficas son fijas en todo el tiempo. Los criptoperiodos necesitan la actualización de llaves. Esto impone requerimientos adicionales, como autoridades certificadoras, las cuales mantienen y actualizan las llaves de las entidades.

2.7.1. Protección del tiempo de vida

Con respecto al almacenamiento a largo plazo de las llaves, la duración de la protección requerida depende de la función criptográfica (ejemplo: cifrado, firma, autenticación de origen de datos/integridad) y el tiempo de la sensibilidad de los datos en cuestión.

2.7.2. Seguridad en la actualización de llaves

Las llaves deben ser actualizadas antes de que expire el criptoperiodo. La actualización incluye el uso de las llaves existentes

para establecer una nueva llave, a través de un protocolo de establecimiento de llave.

Para limitar la exposición en caso de compromiso de una de las llaves secretas a largo plazo o llaves de sesión pasadas, las dependencias entre llaves deben ser evitadas. Por ejemplo asegurar una nueva llave de sesión cifrándola con una llave de sesión pasada no es recomendable.

2.7.3. Almacenamiento de tiempo de vida para varios tipos de llave

El almacenamiento de llaves secretas debe ser asegurado para proveer confidencialidad y autenticidad. Las llaves públicas almacenadas deben ser aseguradas de tal forma que su autenticidad se pueda verificar. La garantía de confidencialidad y autenticidad, contrarrestan las amenazas de divulgación y modificación respectivamente, así como pueden ser provistas por técnicas criptográficas, técnicas de procedimiento (basadas en confianza), o protección física (resistente a manipulaciones de hardware).

La verificación de las firmas de llave pública, puede requerir archivar las llaves para permitir la verificación de la firma en puntos futuros de tiempo, incluyendo posiblemente, que posteriormente la llave privada deje de ser usada. Algunas aplicaciones pueden requerir que las firmas de llaves privadas no sean respaldadas ni archivadas: tales llaves revelaron para cualquier otra parte que el dueño potencialmente invalida la propiedad de no repudiación.

Las llaves usadas para la autenticación de la entidad no necesitan ser respaldadas o archivadas. Todas las llaves secretas usadas para el cifrado o autenticación de origen de datos debería permanecer en secreto tanto tiempo como la seguridad que requieren los datos mismos

(tiempo de vida de la protección) y es necesario respaldar o archivar para prevenir pérdidas de este dato.

2.7.4. Ciclo de vida de la administración de llave

Con excepción de sistemas simples donde las llaves secretas permanecen fijas todo el tiempo, los criptoperiodos asociados con las llaves requieren que las llaves sean actualizadas periódicamente. La actualización de la llave necesita procedimientos y protocolos adicionales, a menudo incluyen comunicaciones con terceras partes en sistemas de llave pública. La secuencia de estados de la llave, la cual progresa a lo largo de su tiempo de vida, es llamada: el ciclo de vida de la administración de la llave. Las etapas del ciclo de vida, pueden incluir:

a) Registro de entidades: una entidad llega a ser un miembro autorizado de un dominio de seguridad. Este incluye adquisiciones, o creación e intercambio, de llave inicial tal que se comparte password o PINs por seguridad, técnica de un tiempo (ejemplo: intercambio de personal, mail registrado, mensajería de confianza).
b) Inicialización de entidades: una entidad inicializa su aplicación criptográfica (ejemplo: instala e inicializa software o hardware), incluyendo uso o instalación de llave inicial obtenida durante su registro.
c) Generación de llave: deben incluir medidas para asegurar características apropiadas para la aplicación o algoritmos y aleatoriedad en el sentido de ser predecible (para adversarios) con insignificante probabilidad. Una entidad puede generar sus propias llaves o adquirir llaves desde un sistema de componentes de confianza.

d) Instalación de la llave: La llave es instalada para uso operacional dentro de un software o hardware de la entidad, a través de una variedad de técnicas, incluyendo una o más de las siguientes: manual de entrada de un password o PIN, transferencia de un disco, dispositivo de memoria de solo lectura. La llave inicial puede servir para establecer o asegurar una sesión en línea a través de la cual trabajan llaves ya establecidas. Durante actualizaciones subsecuentes, la nueva llave es instalada para reemplazar la que está en uso, idealmente a través de una técnica de actualización segura.

e) Registro de llaves: En asociación con la llave de instalación, la llave puede ser oficialmente registrada (por una autoridad registradora) y asociada con un nombre único el cual distingue a las entidades. Para las llaves públicas, los certificados de llave pública pueden ser creados por una Autoridad Certificadora y permite la disponibilidad a otros a través de un directorio público u otros medios.

f) Uso normal: El objetivo del ciclo de vida de las llaves es facilitar la disponibilidad operacional de la llave para estándares de propósito criptográfico. Bajo circunstancias normales, este estado continúa hasta la expiración del criptoperiodo, este puede ser también subdividido, por ejemplo: para cifrado de llaves públicas, un punto puede existir en el cual la llave pública no se considera válida para el cifrado, pero la llave privada permanece en uso para el descifrado.

g) Respaldo de la llave: asegura el medio de almacenamiento para proporcionar una fuente de datos para la recuperación de la llave.

h) Actualización de llave: antes de la expiración del criptoperiodo, la llave operacional es remplazada por una nueva. Esta actualización puede incluir alguna combinación de generación de llaves,

derivación de llaves, ejecución del protocolo de establecimiento de llave de dos partes, o comunicaciones con una tercera parte de confianza. Para llaves públicas la actualización y registro de nuevas llaves incluye protocolos de comunicaciones seguras con Autoridades Certificadoras.

i) Archivo: una llave en uso normal puede ser archivada para proveer una fuente para llaves de recuperación bajo circunstancias especiales (ejemplo: la solución de disputas que incluyen repudiación).

j) Sin registro y destrucción de llave: una vez que no hay más requerimientos para el valor de una llave o para mantener su asociación con una entidad, la llave se da de baja (removida de todos los registros oficiales de llaves existentes) y todas las copias de las llaves son destruidas. En el caso de llaves secretas, todas las huellas (existencia, creación, características, etc.) son seguramente borradas.

k) Recuperación de llave: si la llave es perdida o comprometida (ejemplo: debido a la falla del equipo o al password olvidado), puede ser posible restablecer la llave de una copia de seguridad.

l) Revocación de llave: Puede ser necesario remover las llaves desde un uso operacional a priori a su horario de expiración original, por razones que incluyen compromiso de llave. Para llaves públicas distribuidas por autoridades certificadas, esto incluye certificados revocados.

2.7.5. Estado de las llaves dentro del ciclo de vida

Los eventos típicos incluyen la llave, el tiempo de vida de la llave define etapas del ciclo de vida. Estas pueden ser agrupadas para definir un grupo más pequeño de estados para llaves criptográficas,

relacionadas a su disponibilidad de uso. Una clasificación del estado de las llaves es el siguiente:

a) Pre-operacional: La llave aún no está disponible para operaciones criptográficas normales.
b) Operacional: La llave está disponible y en uso normal.
c) Post-operacional: La llave no es tan grande en uso normal, pero el acceso fuera de línea a esta, es posible para propósitos especiales.
d) Obsoleto: La llave no está disponible. Todos los registros del valor de la llave son borrados.

CAPITULO 3. PROTOCOLOS DE ESTABLECIMIENTO DE LLAVE

3.1. PROTOCOLOS DE ESTABLECIMIENTO DE LLAVE PROPUESTOS PARA SU DESCRIPCIÓN

La selección adecuada de los protocolos de establecimiento y administración de llave es un proceso que incluye conocer las características y el funcionamiento de éstos. Sin embargo existe una gama importante de estos protocolos, por lo que para su selección se deben seguir ciertos criterios, los cuales se mencionan a continuación.

Los requisitos solicitados más interesantes para un protocolo son que éste sea público y disponible para todo el mundo, que se pueda desarrollar en un amplio rango de soluciones hardware y software.

La elección depende en mucho de qué necesidades de seguridad se desean satisfacer, de la aplicación para la que se implementen así como su adecuación para ser implementados en hardware y software, de los recursos de cómputo que se tengan disponibles, de su simplicidad y a sus condiciones de uso (licencia).

Así mismo se puede pensar en dos aspectos al seleccionar los protocolos criptográficos [16]:

El primero es la complejidad computacional, que mide el esfuerzo de cálculo que es necesario realizar para romper un determinado algoritmo o protocolo criptográfico. Aunque hay definiciones teóricas precisas, un algoritmo o protocolo se considera en la práctica computacionalmente seguro si el mejor método conocido para romperlo necesita unos recursos computacionales (tiempo de CPU o memoria) exageradamente elevados. Otro enfoque se basa en reducir el algoritmo o protocolo a un problema equivalente

que se tiene cierta confianza en que es muy difícil de resolver. Por ejemplo, si un algoritmo se basa en la factorización de números muy grandes se puede considerar seguro computacionalmente.

El segundo aspecto es la seguridad incondicional, que mide la seguridad de un protocolo o algoritmo cuando no ponemos límites en los recursos computacionales que puede utilizar un adversario para romperlo. Se dice que un algoritmo o protocolo es incondicionalmente seguro cuando no se puede romper ni siquiera con recursos infinitos.

Los algoritmos y protocolos de seguridad se estudian generalmente desde el punto de vista de su complejidad computacional. Obviamente, sería preferible disponer de algoritmos incondicionalmente seguros, pero esto es muy costoso en algunos casos, e imposible en otros. Por ejemplo, la teoría nos dice que los sistemas de cifrado incondicionalmente seguros utilizan claves extremadamente largas, lo cual no es práctico. De manera similar, la teoría nos dice que no existen sistemas de clave pública incondicionalmente seguros.

En los capítulos 3 y 4 se hablará de la descripción y del análisis de los protocolos de establecimiento y administración de llave respectivamente.

3.1.1. Acuerdo de llave de Diffie-Hellman

Junto con el problema de la autenticación, la motivación de Diffie-Hellman para la introducción de la criptografía de llave pública fue el problema de la distribución de llaves (de llave secreta) en una red de comunicaciones.

En una red, cada par de entidades A y B necesitan eventualmente una llave k_{AB} para crear un canal privado virtual entre ambos. Uno de los problemas de esto es que una llave no puede ser

enviada por la propia red de comunicaciones (por hipótesis insegura). Si el número de entidades es elevado entonces dicho problema crece exponencialmente, además que por motivos de seguridad, una llave k_{AB} debe ser cambiada periódicamente (de hecho suele ser una llave de sesión utilizada solo para una comunicación).

El problema mencionado es solo una parte del problema, más general, denominado gestión y distribución de llaves que involucra cuestiones como el de quien asume la responsabilidad de la creación de tales llaves (con diferentes alternativas: autoridad central, diferentes niveles jerárquicos, sistema totalmente descentralizado), diferentes tipos de llaves (de comunicaciones, maestras, de transacción), los requisitos de seguridad en el almacenamiento y empleo de las mismas, etc. [2].

a) El Problema de los logaritmos discretos.

El problema inverso de la exponenciación es el cálculo de logaritmos discretos. Dados dos números a, b y el módulo n, se define el logaritmo discreto de a en base b módulo n como:

$$c = log_b(a)\ (mod\ n) \leftrightarrow\ a =\ b^c\ (mod\ n) \qquad \textbf{(1)}$$

En la actualidad no existen algoritmos eficientes que sean capaces de calcular en tiempo razonable logaritmos de esta naturaleza y muchos esquemas criptográficos basan su resistencia en esta circunstancia. El problema de los logaritmos discretos está íntimamente relacionado con el de la factorización, de hecho está demostrado que si se puede calcular un logaritmo, entonces se puede factorizar fácilmente (el recíproco no se ha podido demostrar) [17].

b) Características Generales

El secreto compartido puede utilizarse como llave simétrica o de sesión, por lo que el cifrado con llaves simétricas es mucho menos costoso, en términos computacionales.

Su eficacia es compleja debido a que matemáticamente se debe de cumplir con las propiedades de los valores que utilizan ambas entidades, para que al realizar éstas los cálculos necesarios, puedan obtener valores exactos y para que ambas puedan obtener finalmente un resultado idéntico y válido.

Mientras dos entidades (A y B) que se quieran comunicar, logren transmitir una a la otra el primer valor inicial que calcularon, después cada una de ellas podrá independientemente calcular el segundo valor para posteriormente utilizarlo como llave.

Este protocolo puede realizarse en ciertos ambientes, siempre y cuando se tomen las medidas de seguridad necesarias ya que mientras no exista el ataque de hombre en medio (difícilmente), cumple y sirve mayoritariamente para negociar llaves.

Aunque este protocolo crea un valor (secreto compartido), no tiene características que le permitan utilizarse directamente en algún tipo de algoritmo que utiliza llaves especificas para su uso, pero el valor compartido se puede utilizar como semilla para generar una llave específica.

La seguridad del algoritmo depende de la dificultad del cálculo de un logaritmo discreto. Esta función es la inversa de la potencia discreta, o sea, de calcular una potencia y aplicar una función mod.

- Potencia discreta: $Y = X^a \, mod \, q$
- Logaritmo discreto: $X = ln \, d_{a,q} \, (Y)$

El problema de Diffie-Hellman [17], [12] y [2] está íntimamente relacionado con el problema de los logaritmos discretos, y es la base de algunos sistemas criptográficos de llave pública, entre otros.

Antes de enunciarlo hablaremos del término *generador*. Dado el conjunto Z_P^*, con p primo, diremos que $\propto \, \epsilon \, Z_P^*$ es un generador de Z_P^*, si se cumple:

$$\forall \, b \, \epsilon \, Z_P^*, \; \exists \, i \, tal \, que \; \propto^i = b \qquad \textbf{(2)}$$

El enunciado del problema es el siguiente: dado un número primo p, un número $\propto$ que sea un generador de Z_P^* y los elementos $\propto^a, \propto^b$, encontrar $\propto^{ab} \; (mod \, p)$.

Se conoce $\propto^a$ y $\propto^b$, pero no el valor de a ni el de b. De hecho, si pudiésemos efectuar de forma eficiente logaritmos discretos, sería suficiente con calcular a y luego:

$$(\propto^b)^a = \propto^{ab} \qquad \textbf{(3)}$$

La ventaja de este sistema es que no son necesarias llaves públicas, sino una información compartida entre las dos entidades que desean comunicarse.

Sean A y B las entidades a comunicarse. En primer lugar, se calcula un número primo p y un generador $\propto$ de Z_P^*, con: $2 \leq \propto \leq p - 2$. Esta información es pública y conocida por ambos. El algoritmo queda como sigue (ver Fig. 3.1):

1. A escoge un número aleatorio x, comprendido entre 1 y $\mathrm{p}-2$ y envía a B el valor: $ya = \propto^{\mathrm{x}} (\mathrm{mod}\ \mathrm{p})$.
2. B escoge un número aleatorio y, análogamente al paso anterior, y envía a A el valor: $yb = \propto^{y} (mod\ p)$.
3. B recoge y_a y calcula: $k = (\propto^{x})^{y} (mod\ p)$.
4. A recoge y_b y calcula $k = (\propto^{y})^{x} (mod\ p)$.

En la Fig. 3.1 se muestra un diagrama de secuencia en donde se puede apreciar paso a paso el protocolo de Diffie-Hellman.

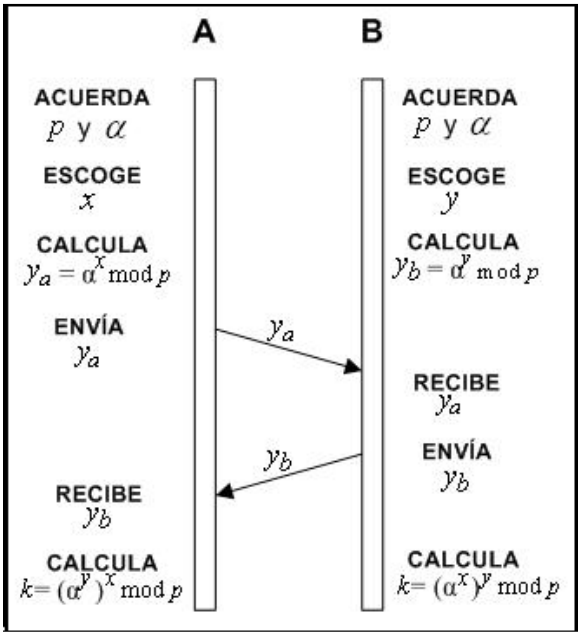

Fig. 3.1 Diagrama de secuencia del protocolo de Diffie-Hellman

3.1.2. Ataque a Diffie-Hellman

A continuación se explicará si un intruso puede atacar este protocolo en base a [16].

Un intruso que conozca las claves públicas p y $\propto$ e intercepte el valor ya que ha enviado A y el valor yb que ha enviado B, no podrá descubrir los valores x e y y mucho menos $\propto^{\mathrm{xy}} (\mathrm{mod}\ \mathrm{p})$.

Salvo que se enfrente al Problema del Logaritmo Discreto (PLD), el cual se vuelve computacionalmente intratable para valores grandes del primo p.

La seguridad del intercambio de clave de Diffie y Hellman radica en la imposibilidad computacional a la que se enfrentará el criptoanalista al tener que resolver el problema del logaritmo discreto para encontrar la clave privada que se encuentra en el exponente de la expresión: $\propto^{\mathrm{i}} \bmod \mathrm{p} = \mathrm{C}$.

El algoritmo propuesto inicialmente es vulnerable ante un ataque del tipo “man in the middle”. No obstante, esta vulnerabilidad puede evitarse con los protocolos que se verán más adelante.

A continuación se explicará el ataque a este protocolo:

1. A elige un número a con $1 < a < p - 1$, calcula $y_a = \propto^{\mathrm{a}} \bmod \mathrm{p}$ y envía a B el valor y_a.
2. C intercepta este valor $(\mathrm{y_a})$, elige un número c con $1 < c < p - 1$, calcula $\mathrm{y_c} = \propto^{\mathrm{c}} \bmod \mathrm{p}$ y envía a B el valor $\mathrm{y_c}$.
3. B elige un número b con $1 < b < p - 1$ calcula $\mathrm{y_b} = \propto^{\mathrm{b}} \bmod \mathrm{p}$ y envía a A el valor $\mathrm{y_b}$.
4. C intercepta este valor $(\mathrm{y_b})$ y envía a A el valor $\mathrm{y_c}$.
5. A y B calculan sus llaves $\mathrm{k_A} = (\propto^{\mathrm{c}})^{\mathrm{a}} \bmod \mathrm{p}$, $\mathrm{k_B} = (\propto^{\mathrm{c}})^{\mathrm{b}} \bmod \mathrm{p}$,
6. C calcula también la llaves: $\mathrm{k_{CA}} = (\propto^{\mathrm{a}})^{\mathrm{c}} \bmod \mathrm{p}$, $\mathrm{k_{CB}} = (\propto^{\mathrm{b}})^{\mathrm{c}} \bmod \mathrm{p}$.

Por lo tanto a partir de ahora C puede interceptar todos los mensajes que se intercambian A y B.

En la Fig. 3.2 se muestra un diagrama de secuencia en donde se puede apreciar paso a paso el ataque al protocolo de Diffie-Hellman.

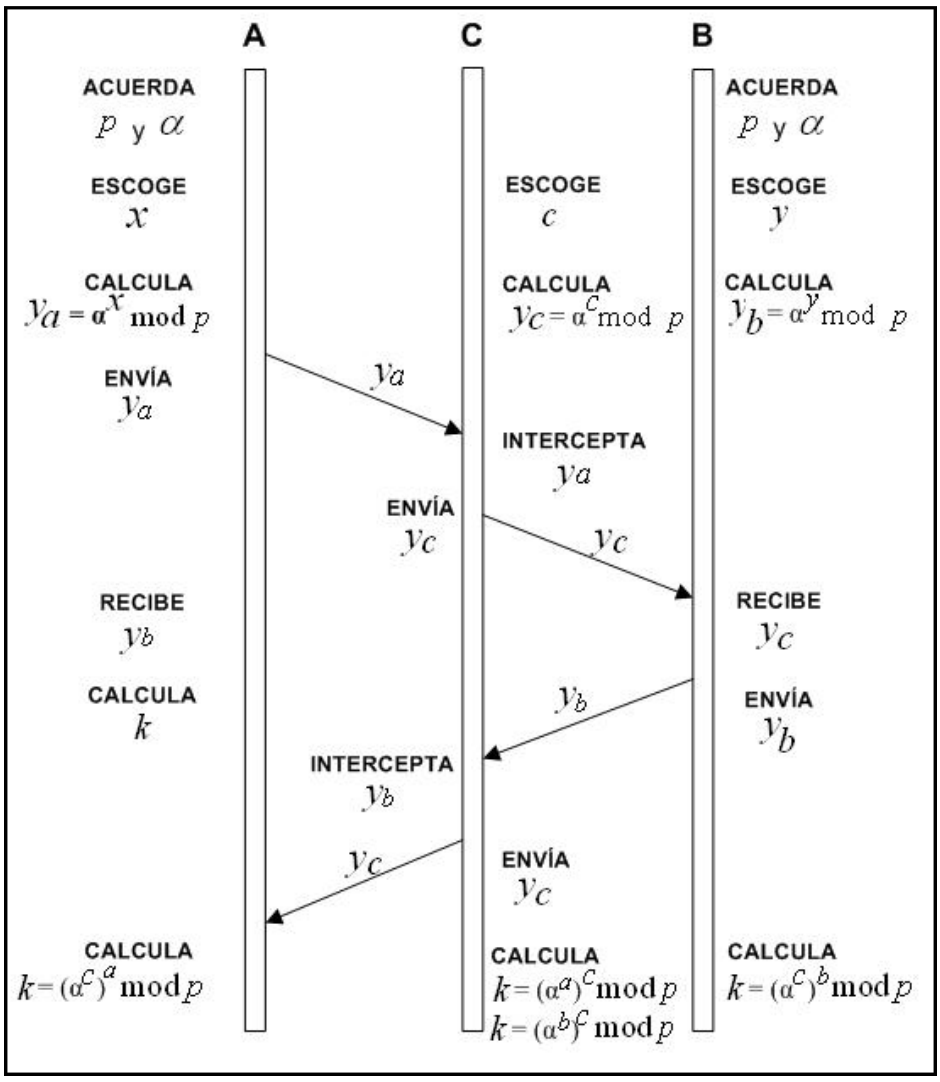

Fig. 3.2 Diagrama de secuencia del ataque al protocolo de Diffie-Hellman

3.1.3. Funcionamiento de Diffie-Hellman

A continuación se describirá el funcionamiento del protocolo de Diffie-Hellman. Para explicar el funcionamiento de este protocolo se utilizará la herramienta "CrypTool" versión 1.4.21, la cual es una herramienta educativa y gratuita orientada a la enseñanza de la criptografía y el criptoanálisis.

El escenario es entre dos entidades: A y B que desean intercambiar un secreto compartido. En este caso las entidades $A\ y\ B$ son Alice y Bob respectivamente.

Como primer paso se deben introducir los parámetros públicos que se utilizarán en este protocolo que son el módulo primo p y el generador $\propto$. Ver Fig. 3.3.

En este caso se tomo el algoritmo Test de Miller-Rabin que nos sirve para generar números primos.

El valor de p es el siguiente:

10226195899104442379158206723856694810384951165791538358292827403832714759344 7

El valor de $\propto$ es el siguiente:

8908030497528120745646807260197861428425716080724039796425987187627598718762787175560 28

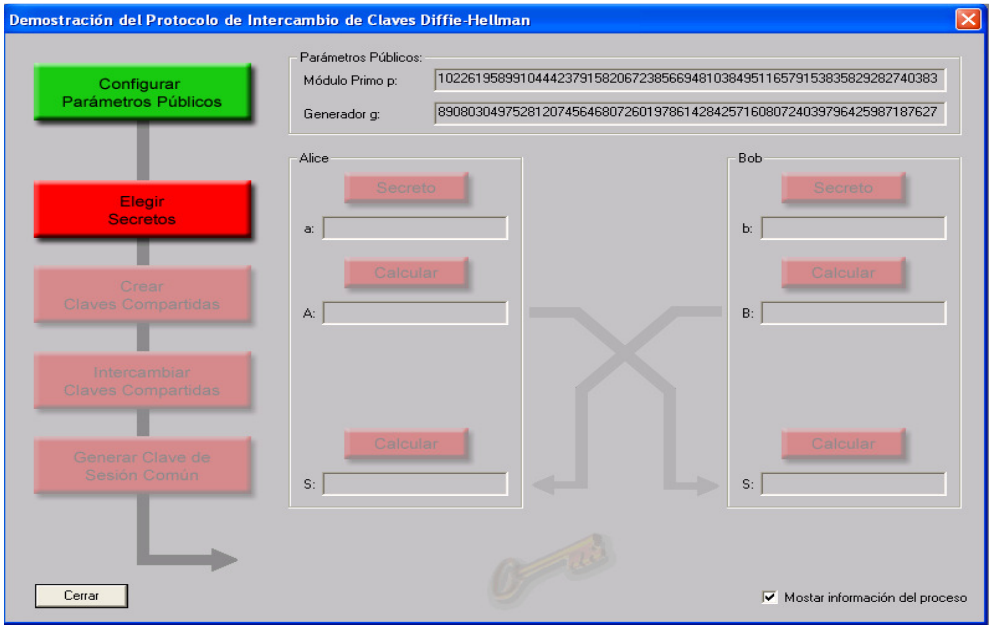

Fig. 3.3 Primer paso parámetros públicos

Como segundo paso se eligen de forma independiente los números secretos para las entidades A y B, los cuales deben ser un número natural, preferentemente mucho mayor que uno pero menor que el definido anteriormente como módulo primo p. Ver Fig. 3.4.

Para la entidad A tenemos el número $x =$

6328706711078884769030170224948596315719913363583247375242654203431975748619

Para la entidad B tenemos el número $y =$

1711966496161347772975377115523930760316516402089239494624630045288365966993

Los números secretos se muestran en asteriscos.

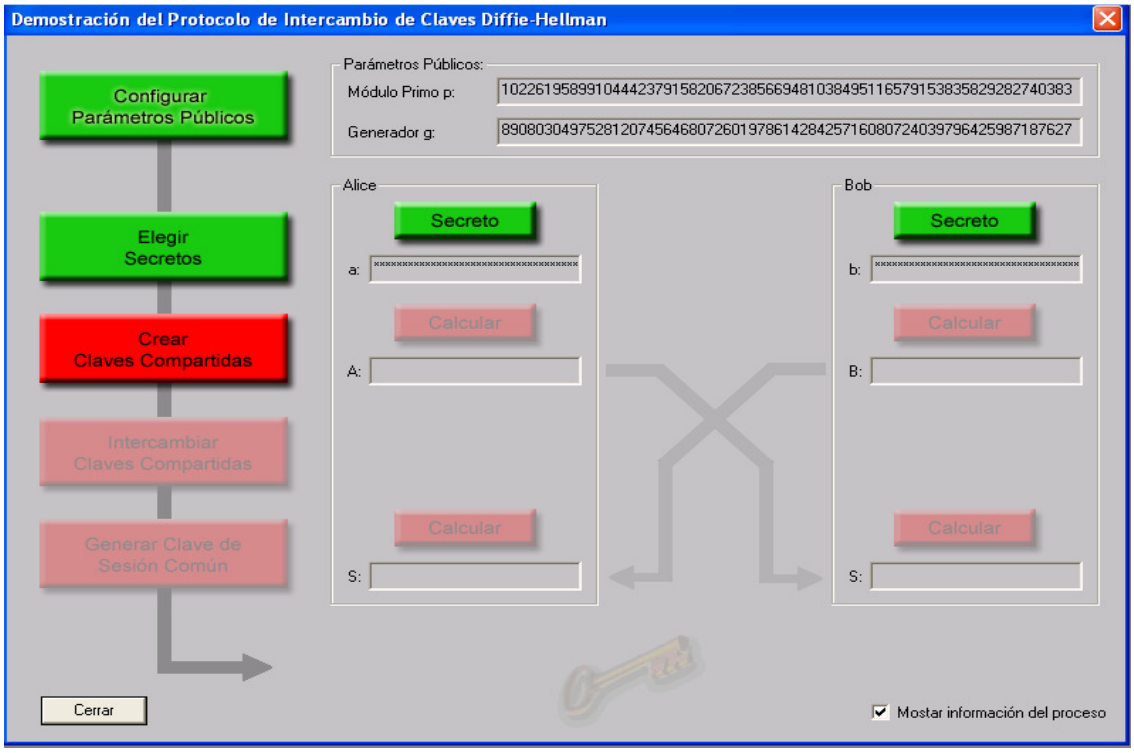

Fig. 3.4 Segundo paso parámetros secretos

Como tercer paso se crean las llaves compartidas las cuales cada entidad las calcula de la siguiente forma: Ver Fig. 3.5.

Para la entidad A tenemos: $y_a = \propto^x mod\ p =$

74118521183314683756247032420845472804992442246055400073744791085439787988683

Para la entidad B tenemos: $y_b = \propto^y mod\ p =$

90516558013079062464601828866634639422897410572733089550391462073696630977237

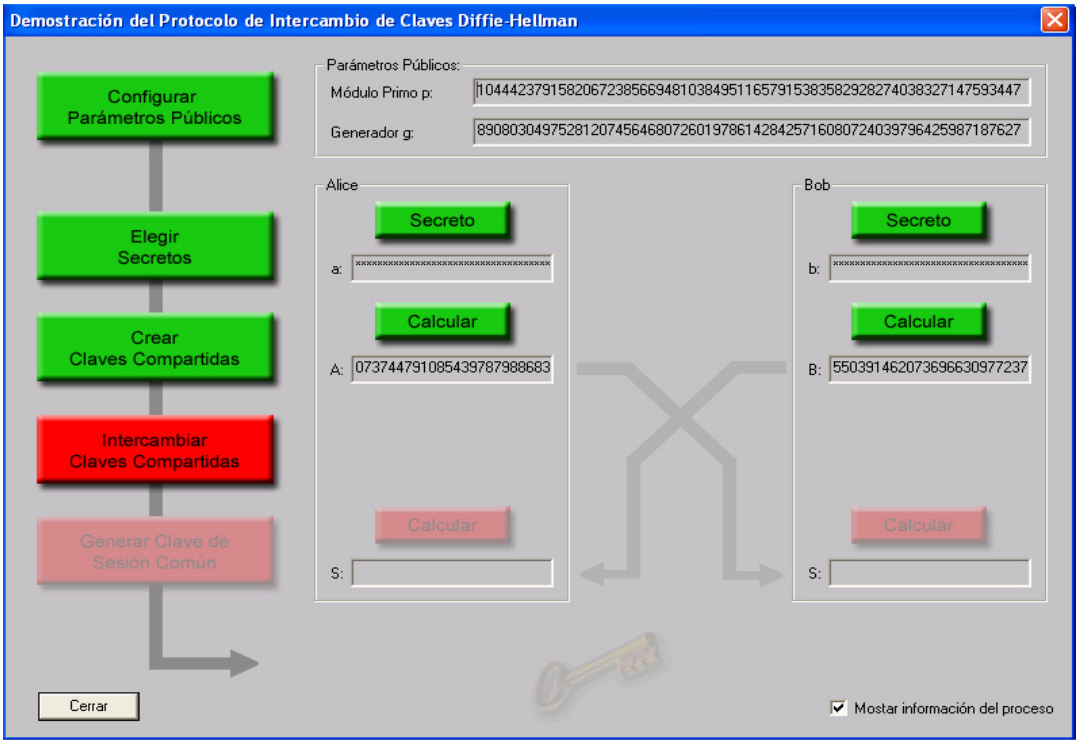

Fig. 3.5 Tercer paso calcular llaves compartidas

Como cuarto paso las entidades deben intercambiar sus llaves compartidas para que posteriormente puedan calcular su llave de sesión. Ver Fig. 3.6.

Así la entidad A envía a la entidad B el valor y_a y B envía a A el valor y_b. Estos valores pueden ser públicos.

En este punto del protocolo se puede tener el ataque: man-in-the-middle, mencionado en el punto 3.1.2.

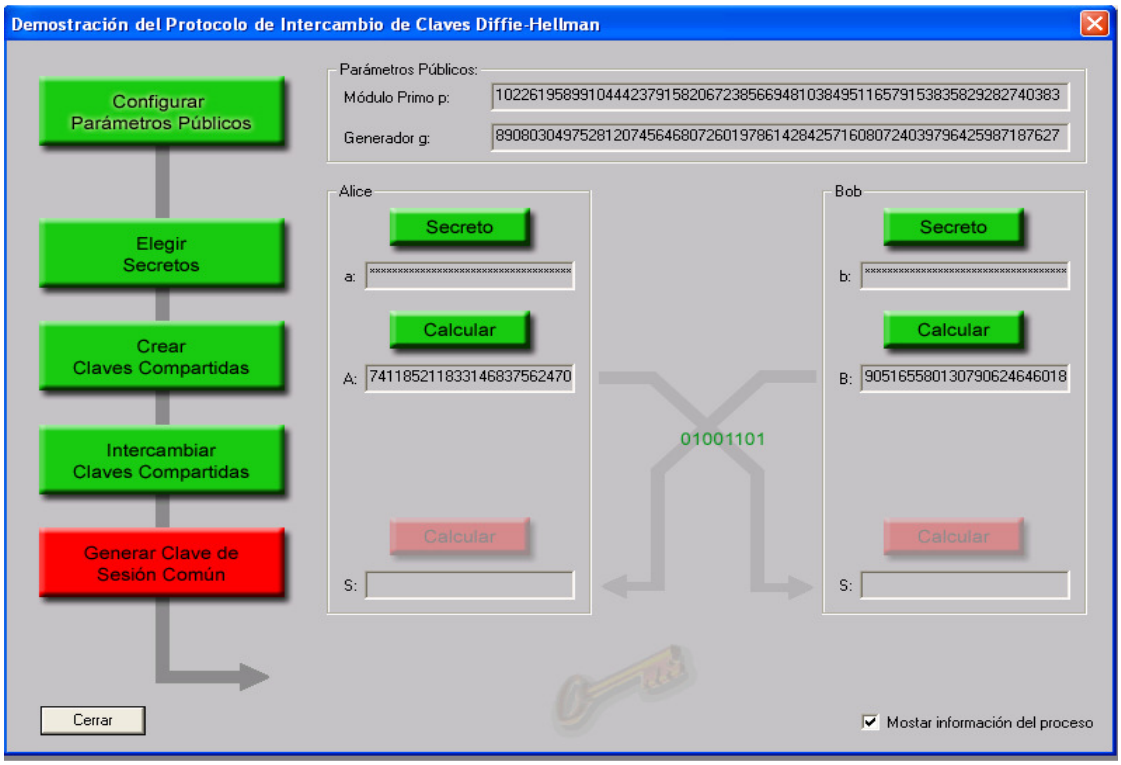

Fig. 3.6 Cuarto paso intercambiar llaves compartidas

Como quinto y último paso, cada entidad calcula la llave de sesión común entre éstas. Esta llave de sesión se calcula de la siguiente forma:

A calcula $k = {y_b}^x mod\ p$

B calcula $k = {y_a}^y mod\ p$.

Por lo que el valor de k para ambas entidades es:
1132107720998325408115750282040701355413117421560288726500548876125703750699 1

Por tanto se ha conseguido el objetivo, usando la información secreta que cada uno posee y la información pública que se intercambian, ambas entidades (A y B) logran acordar una llave secreta común con la que trabajar. Ver Fig. 3.5.

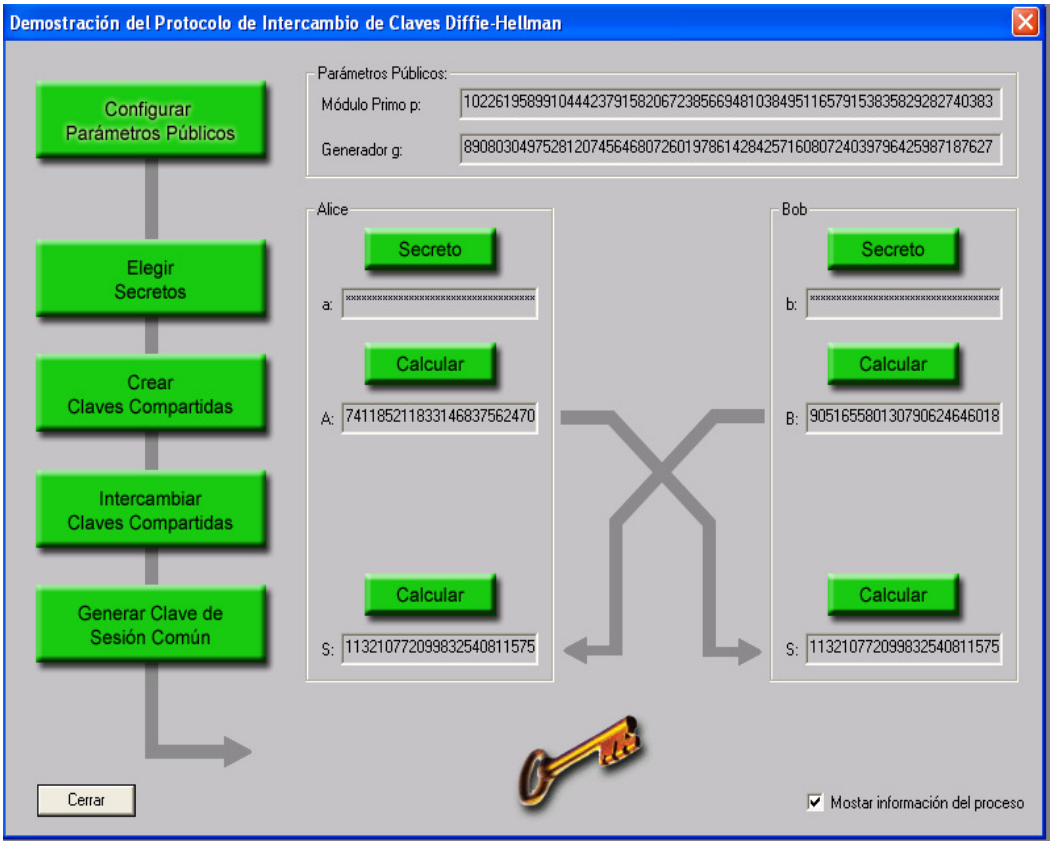

Fig. 3.7 Quinto paso generar llave de sesión

Un atacante no puede obtener la llave común generada si los valores con los que se trabajan son suficientemente grandes. Por tanto, la llave obtenida es segura y puede ser utilizada para un algoritmo de cifrado simétrico.

3.1.4. ElGamal acuerdo de llave en un paso

El acuerdo de llave ElGamal es una variante de Diffie-Hellman y provee un protocolo de un paso (intercambio de un solo mensaje) con autenticación de llave unilateral [2].

Fue diseñado en un principio para producir firmas digitales, pero posteriormente se extendió también para cifrar mensajes. Se basa en el problema de los logaritmos discretos, que está íntimamente relacionado con el de la factorización y en el de Diffie-Hellman [17].

a) Características Generales

Este protocolo es susceptible a ataques activos como el de hombre en medio.

Su eficacia es compleja debido a que matemáticamente se debe de cumplir con las propiedades de los valores que utilizan ambas entidades, para que al realizar éstas los cálculos necesarios puedan obtener valores exactos y para que ambas puedan obtener finalmente un resultado idéntico y válido.

Los pasos que se deben de seguir para poder obtener el resultado deseado son:

- Si A quiere obtener la llave de B tiene que obtenerla de un llavero de una AC (Autoridad Certificadora) en un certificado, pero si alguno de estos no está disponible no se puede completar el protocolo.

- Mientras la entidad iniciadora (A) de las dos entidades $(A\ y\ B)$ que se quieran comunicar, logre realizar el paso anterior y pueda B recibir el valor de A, posteriormente cada una de ellas

podrá independientemente calcular el segundo valor para utilizarlo como llave.

La seguridad del algoritmo al igual que Diffie-Hellman, depende de la dificultad del cálculo de un logaritmo discreto. Esta función es la inversa de la potencia discreta, o sea, de calcular una potencia y aplicar una función mod.

- Potencia discreta: $Y = X^a \, mod \, q$
- Logaritmo discreto: $X = \ln d_{a,q} \, (Y)$

El acuerdo de llave ElGamal es una variante de Diffie-Hellman, provee un protocolo de un paso (intercambio de un solo mensaje) con autenticación de llave unilateral, proporcionada a través de la llave del receptor que es conocida a priori por el iniciador, siendo ésta integrada en un certificado y por tanto se verifica su autenticidad.

3.1.5. Funcionamiento ElGamal acuerdo de llave en un paso

A continuación se explicará el funcionamiento de este protocolo.

El escenario es entre dos entidades $(A \, y \, B)$ que desean intercambiar un secreto compartido y otra entidad llamada: Tercera Entidad de Confianza o Autoridad Certificadora (AC).

1. Ambas entidades seleccionan un mismo primo p y un generador $\propto$ de Z_P^*.
2. La entidad B selecciona un número entero "y" el cual tiene las siguientes características: $1 \leq y \leq p-2$ y es su valor secreto. Posteriormente realiza el cálculo: $z_2 = \propto^y mod \, p$ y valida z_2 (valor público) a través de un certificado, el cual es emitido por una Autoridad Certificadora. Este proceso se supone seguro mediante el uso de mecanismos de seguridad como: Firma Digital entre otros.

3. La entidad A escoge un número entero "x" el cual tiene las siguientes características: $1 \leq x \leq p-2$ y es su valor secreto. Después realiza el cálculo siguiente: $z_1 = \propto^x \ mod\ p$.
4. La entidad A envía z_1 a la entidad B y para que A pueda tener el valor de B, lo obtiene certificado de la AC.
5. Cada entidad calcula su llave, siendo que la llave generada en cada entidad será la misma.

Así tenemos que el cálculo de cada entidad es el siguiente:

Para la entidad A: $\mathrm{k} = {z_2}^x \ mod\ p = \ {z_1}^y \ mod\ p$

Para la entidad B: $\mathrm{k} = {z_1}^y \ mod\ p = \ {z_2}^x \ mod\ p$

A continuación se muestra un ejemplo práctico de este protocolo, tomando como base los siguientes valores: $p = 7$, $\propto = 3$, $x = 4$, $y = 5$. Ver Fig. 3.8.

1. Las entidades A y B seleccionan $p = 7$ y $\propto = 3$.
2. La entidad B selecciona un número entero $y = 5$ y realiza el cálculo $z_2 = \propto^y \ mod\ p = \ 3^5 \ mod\ 7 = 5$. Así el valor $z_2 = 5$, se autentica con la entidad B, a través de un certificado, el cual es emitido por una Autoridad Certificadora.
3. La entidad A selecciona un número entero $x = 4$ y realiza el cálculo $z_1 = \propto^x \ mod\ p = \ 3^4 \ mod\ 7 = 4$.
4. La entidad A envía el valor $z_1 = 4$ a la entidad B y para que A pueda obtener el valor de B lo obtiene certificado de la AC
5. Cada entidad calcula su llave. Así tenemos que el cálculo para cada entidad es el siguiente:

Para la entidad A: $\mathrm{k} = {z_2}^x \ mod\ p = \ 5^4 \ mod\ 7 = 2$

Para la entidad B: $\mathrm{k} = {z_1}^y \ mod\ p = \ 4^5 \ mod\ 7 = 2$

ASÍ la llave k generada para cada entidad es la misma.

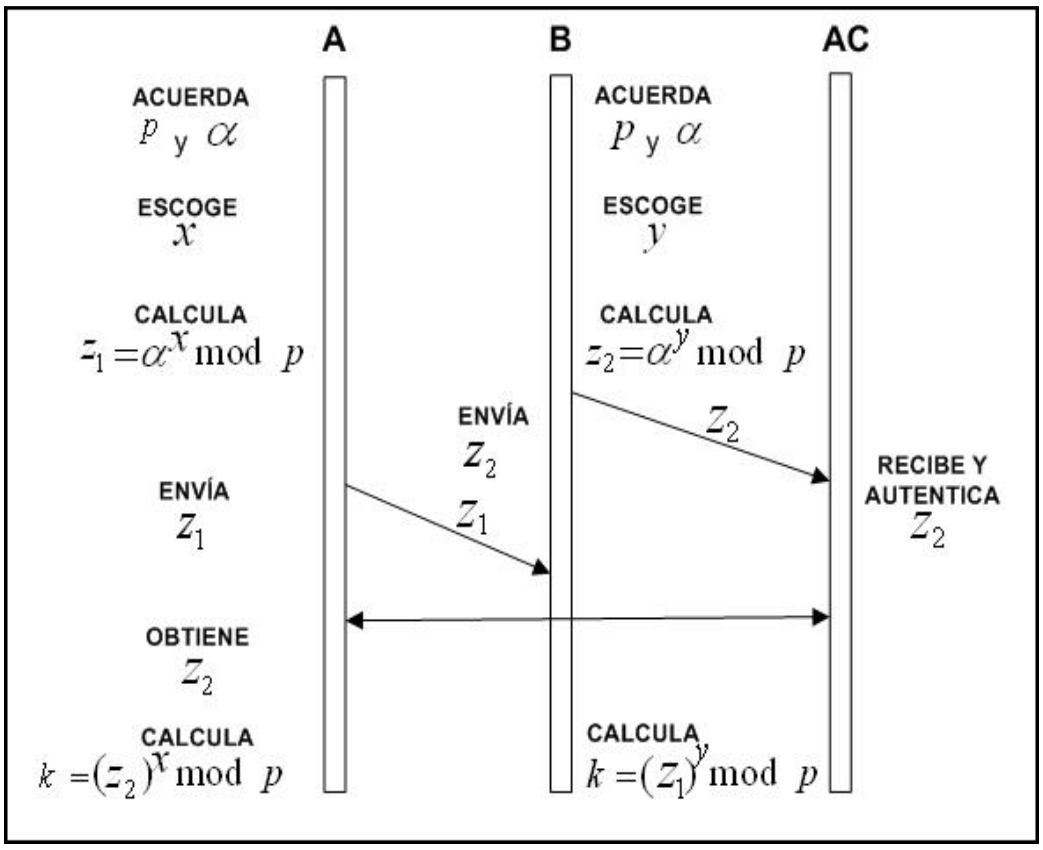

Fig. 3.8 Diagrama de secuencia del protocolo de ElGamal acuerdo de llave en un paso

El protocolo ElGamal genera un solo mensaje por el hecho de que la entidad B previamente coloca sus datos públicos en un servidor de llaves públicas (por ejemplo, en un certificado), de otra manera este protocolo sería como el de Diffie-Hellman y solo existe la autenticidad de los datos de la entidad B a la entidad A debido al hecho de que el servidor de llaves públicas se requiere en este protocolo. En términos de complejidad para resolver ElGamal, es el mismo caso de Diffie-Hellman que es resolver el problema del logaritmo discreto [2].

3.1.6. Ataque a ElGamal acuerdo de llave en un paso

A continuación se explicará como un intruso puede atacar este protocolo.

1. A elige un número x con $1 < x < p-1$, calcula $z_1 = \propto^{\mathrm{x}} \bmod \mathrm{p}$ y envía a B el valor z_1.
2. C intercepta este valor (z_1), elige un número w con $1 < w < p-1$, calcula $z_3 = \propto^{\mathrm{w}} \bmod \mathrm{p}$ y envía a B el valor z_3.
3. B elige un número y con $1 < y < p-1$ calcula $\mathrm{z}_2 = \propto^{\mathrm{y}} \bmod \mathrm{p}$ y envía a la AC el valor z_2.
4. A y B calculan sus llaves $k_A = (\propto^y)^x \, mod \, p$, $k_B = (\propto^w)^y \, mod \, p$, C calcula también la llaves: $k_C = (\propto^y)^w \, mod \, p$,

Por lo tanto a partir de ahora C puede interceptar todos los mensajes que se intercambian únicamente con la entidad B. Ver Fig. 3.9.

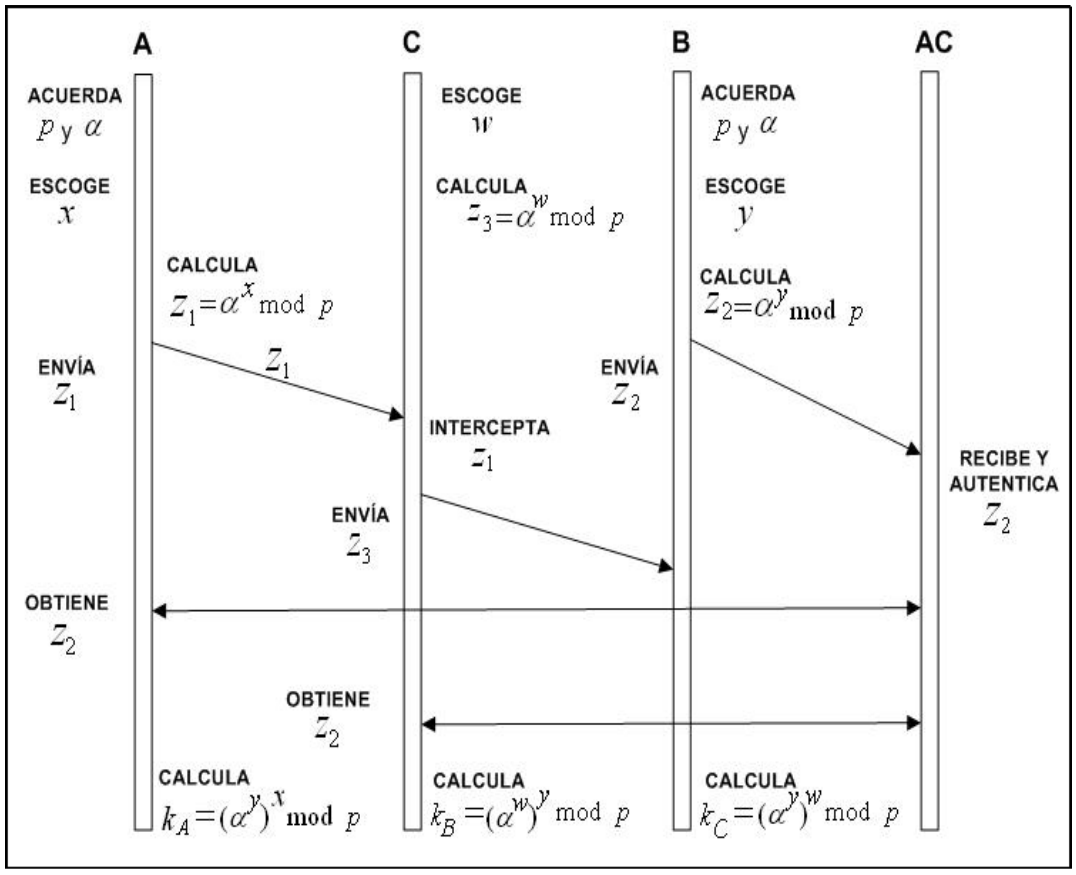

Fig. 3.9 Diagrama de secuencia del ataque al protocolo de ElGamal acuerdo de llave en un paso

3.1.7. MTI protocolo de acuerdo de llave en dos pasos

El MTI es una variante de Diffie-Hellman, también está basado en la complejidad del problema del logaritmo discreto y es un protocolo de acuerdo de llave realizando un intercambio de dos mensajes entre las entidades participantes [2].

a) Características generales.

Aunque el MTI es una variante de Diffie-Hellman, tiene la ventaja de garantizar la autenticidad de las llaves públicas de cada entidad participante en el acuerdo de llave, debido al hecho de que estas llaves públicas están incorporadas en los certificados, siendo así posible la autenticidad de las mismas.

Este protocolo es susceptible a ataques activos.

Los pasos que se deben de seguir para poder obtener el resultado deseado son:

- Si A quiere obtener la llave pública de B tiene que obtenerla de un llavero de una AC en un certificado, igualmente si B quiere obtener la llave pública de A, pero si alguno de estos no está disponible no se puede completar el protocolo.
- Mientras las dos entidades $(A\ y\ B)$ que se quieran comunicar, logren realizar el paso anterior y ambas puedan recibirlo, posteriormente cada una de ellas podrá independientemente calcular el segundo valor para posteriormente utilizarlo como llave.

La seguridad del algoritmo al igual que Diffie-Hellman, depende de la dificultad del cálculo de un logaritmo discreto. Esta función es la inversa de la potencia discreta, o sea, de calcular una potencia y aplicar una función mod.

3.1.8. Funcionamiento del MTI protocolo de acuerdo de llave en dos pasos

A continuación se explicará el funcionamiento de este protocolo. Ver Fig. 3.10.

El escenario es entre dos entidades ($A\ y\ B$) que desean intercambiar un secreto compartido y otra entidad llamada: Tercera Entidad de Confianza o Autoridad Certificadora (AC).

1. Ambas entidades seleccionan un mismo primo p y un generador $\propto$ de Z_P^*, almacenados en un servidor de llaves.
2. Segundo paso: la entidad A selecciona una llave privada que es un entero aleatorio a, el cual tiene las siguientes características: $1 \leq a \leq p-1$ y posteriormente calcula una llave pública $z_A = \propto^a mod\ p$.
3. De forma análoga, B genera b y $z_B = \propto^b mod\ p$.
4. La entidad A escoge un secreto aleatorio x y realiza el cálculo $z_1 = \propto^x mod\ p$, tal que $1 \leq x \leq p-1$. Así mismo la entidad B escoge un secreto aleatorio y y realiza el siguiente cálculo: $z_2 = \propto^y mod\ p$.
5. Las entidades envían los resultados de las operaciones realizadas en el paso anterior.
6. Las entidades A y B calculan sus respectivas llaves de la siguiente forma:

   Para la entidad A calcula: $\mathrm{k} = {z_2}^{\mathrm{a}}\ {z_B}^{\mathrm{x}} \bmod \mathrm{p}$.

   Para la entidad B calcula: $\mathrm{k} = {z_1}^b\ {z_A}^y\ mod\ p$

   Finalmente ambas entidades generan la misma llave $\mathrm{k} = \propto^{bx+ay}$.

A continuación se muestra un ejemplo práctico de este protocolo, tomando como base los siguientes valores: $p = 19$, ∝=3, $a = 5$, $b = 6$, $x = 7$, e $y = 9$.

1. Ambas entidades seleccionan un mismo primo $p = 15$ y un generador $\propto = 3$, almacenados en un servidor.
2. La entidad A selecciona una llave privada $a = 5$ y posteriormente calcula una llave pública $z_A = \propto^a mod\ p = 3^5\ mod\ 19$ = 15.
3. De forma análoga, B genera $b = 6$ y posteriormente calcula $z_B = \propto^b mod\ p = 3^6\ mod\ 19 = 7$.
4. La entidad A escoge un secreto aleatorio $x = 7$ y realiza el cálculo $z_1 = \propto^x mod\ p = 3^7\ mod\ 19 = 2$. Así mismo la entidad B escoge un secreto aleatorio $y = 9$ y realiza el siguiente cálculo: $z_2 = \propto^y mod\ p = 3^9\ mod\ 19 = 18$.
5. La entidad A envía $z_1 = 2$ a la AC, de igual forma B envía a $z_2 = 18$. Posteriormente la entidad A toma de la AC el valor $z_2 = 18$ y la entidad B toma el valor $z_1 = 2$.
6. Las entidades A y B calculan sus respectivas llaves de la siguiente forma:

   La entidad A calcula: $\mathrm{k} = {z_2}^{\mathrm{a}}\ {z_B}^{\mathrm{x}} \bmod \mathrm{p} = 18^5\ 7^7 \bmod 19 = 12$

   La entidad B calcula: $\mathrm{k} = {z_1}^b\ {z_A}^y\ mod\ p = 2^6\ 15^9\ mod\ 19 = 12$

Finalmente ambas entidades generan la misma llave $\mathrm{k} = 12$. A pesar de la aplicación del protocolo MTI, la autenticación de las llaves públicas (z_A y z_B), estos protocolos son susceptibles a ataques activos [2].

CAPITULO 4. PROTOCOLOS DE ADMINISTRACIÓN DE LLAVE

4.1. PROTOCOLOS DE ADMINISTRACIÓN DE LLAVE PROPUESTOS PARA SU DESCRIPCIÓN

A continuación se explicarán tres protocolos de distribución de llave en base a [12].

Solo unos pocos protocolos de distribución de llave son usados hoy en día. Como son:

a) Merkles´s Puzzles.
b) Shamir three-pass protocol.
c) Cifrado asimétrico basado en protocolo de distribución de llave.
d) La extensión ElGamal de Diffie-Hellman.
e) Protocolo de distribución de llave de Needham-Schroeder.
   - Protocolo de distribución de llave de Needham-Schroeder usando llave simétrica.
   - Protocolo de distribución de llave de Needham-Schroeder usando llave pública.

4.2. FUNCIONAMIENTO DEL PROTOCOLO DE DISTRIBUCIÓN DE LLAVE BASADO EN CIFRADO-ASIMÉTRICO

Un protocolo puede ser usado por dos entidades A y B que no comparten un secreto llave inicial. B se asume que tiene una pareja de llaves de un sistema de cifrado asimétrico (E_{e_B} se refiere a la función de cifrado que es llave con e_B (llave pública de B) y D_{d_B} se refiere a la correspondiente función de descifrado que es llave con d_B (llave privada de B). A continuación se explicará el funcionamiento de este protocolo. Ver Fig. 4.1.

1. La entidad A selecciona una llave secreta k al azar de un apropiado espacio de llave k.
2. La entidad A obtiene la llave pública certificada de la entidad B, a través de una AC
3. A cifra la llave secreta k con E_{e_B} y transmite $c = E_{e_B}(k)$ a B.
4. La entidad B usa D_{d_B} para descifrar c es decir $D_{d_B}(c) = D_{d_B}(E_{e_B}(k))$.
5. Finalmente A y B comparten la llave secreta k.

Se debe tomar en cuenta si la entidad A no obtiene la llave pública certificada de la entidad con la que se quiera comunicar, a través de una $A.C.$, entonces existe el ataque de hombre en medio para este protocolo.

Muchos protocolos de seguridad criptográficos para Internet hacen uso de distribución de llave basado en cifrado asimétrico de una forma u otra, por ejemplo el protocolo SSL/TLS trabaja de esta forma, otro ejemplo es la opción de alguna llave en el intercambio de llave Internet (IKE-Internet key exchange), protocolo usado en la suite del protocolo IPsec.

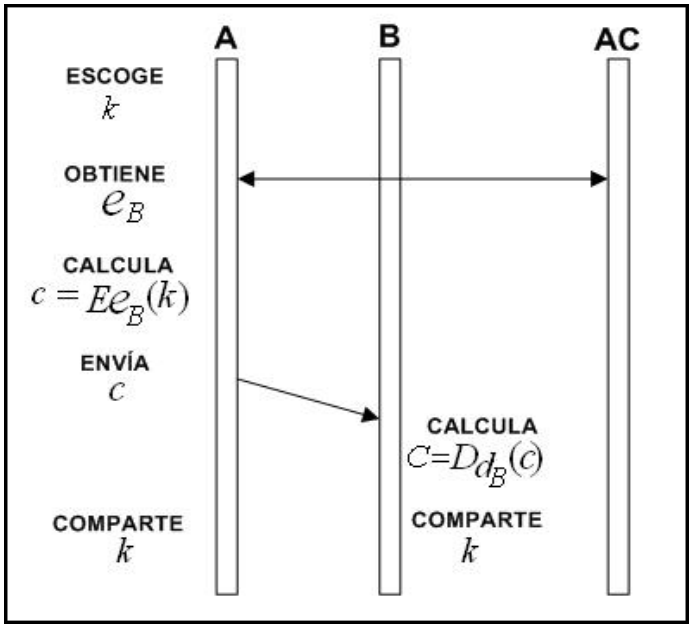

Fig. 4.1 Diagrama de secuencia del protocolo de distribución de llave basado en cifrado asimétrico

4.3. LA EXTENSIÓN ELGAMAL DE DIFFIE-HELLMAN

A continuación se explicará este protocolo en base a [18].

Aunque Diffie-Hellman se dieron cuenta de cómo las llaves podrían ser intercambiadas seguramente si el Problema del Logaritmo Discreto (DLP) es inviable de resolver, ellos no descubrieron como modificar su idea para cifrar datos.

El intercambio electrónico seguro de llaves está basado sobre una extensión del esquema Diffie-Hellman descubierto por el T. ElGamal (1985).

4.3.1. Funcionamiento de la extensión ElGamal de Diffie-Hellman

A continuación se explicará el funcionamiento de este protocolo. Ver Fig. 4.2.

Parámetros públicos: $p = 2r + 1$ y q, ambos son primos.

1. El usuario A selecciona una llave aleatoria k_A ε Z_p^* y calcula $x_A = q^{k_A}(mod\ p)$.
2. El usuario B selecciona una llave aleatoria k_B ε Z_p^* y calcula $x_B = q^{k_B}(mod\ p)$.
3. El usuario A y el usuario B intercambian x_A y x_B.
4. El usuario A calcula $x_{A,B} = (x_B)^{k_A}\ mod\ p$.
5. El usuario B calcula $x_{B,A} = (x_A)^{k_B}\ mod\ p$.
   Así, $x_{A,B} = x_{B,A}$ es usado para derivar la llave de sesión común.

$$e_{A,B} = \begin{cases} x_{A,B} & si\ \ x_{A,B}\ es\ non \\ x_{A,B} - 1 & si\ \ x_{A,B}\ es\ par \end{cases}$$

6. Cada usuario calcula el inverso multiplicativo $d_{A,B}\ mod\ p - 1$ de $e_{A,B}$.

   $d_{A,B} = e_{A,B} = 1\ (mod\ p - 1)$ para evaluar: $d_{A,B} = e_{A,B} = \ (mod\ p - 1)$.

Finalmente el cifrado y el descifrado es aplicado a un texto plano M y a un texto cifrado C en Z_p de acuerdo a las reglas:

$$E: M \to C = M^{e_{A,B}} mod p, \quad D: C \to M = C^{d_{A,B}} mod p$$

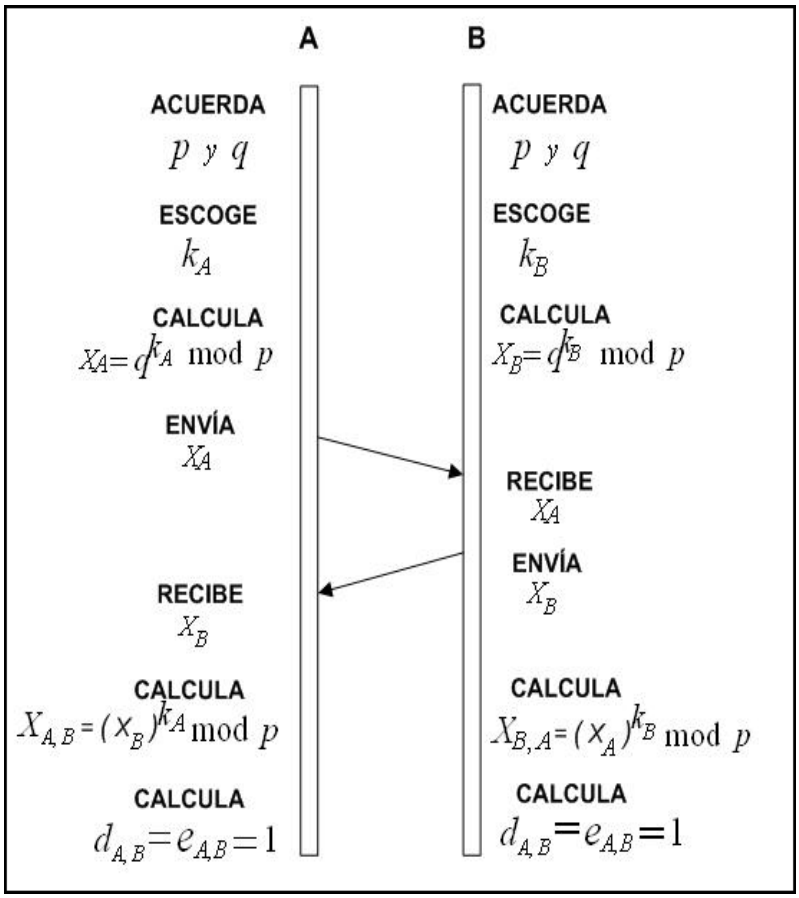

Fig. 4.2 Diagrama de secuencia del protocolo la extensión de ElGamal de Diffie-Hellman

EJEMPLO:

$p = 1283 = 2x641 + 1$ y $q = 24$

1. El usuario A selecciona $k_A = 67$ y calcula:
   $x_A = q^{K_A} mod\ p = 24^{67} mod\ 1283 = 98$.
2. El usuario B selecciona $k_B = 95$ y calcula $x_B = q^{K_B} mod\ p = 24^{95} mod\ 1283 = 933$.

3. Los usuarios A y B x_A y x_B.
4. El usuario A calcula $x_{A,B} = {x_B}^{k_A}\ mod\ p = 933^{67} mod(1283) = 135.$
5. El usuario B calcula $x_{B,A} = {x_A}^{k_B}\ mod\ p = 98^{95} mod(1283) = 135.$

   La llave en común de cifrado de los usuarios A y B es $e_{A,B} = 135.$
6. Sexto paso, cada usuario calcula el inverso multiplicativo $d_{A,B}\ mod\ p - 1$ de $e_{A,B}$.

   Finalmente la llave en común de descifrado de los usuarios A y B es $d_{A,B} = 19.$

El sistema ElGamal es un criptosistema de llave pública basado en el problema del logaritmo discreto, tal como el RSA, este permite los servicios de cifrado y de firma digital. El algoritmo de cifrado es muy similar al protocolo de acuerdo de llave de Diffie-Hellman, pero es mejor que este último porque permite realizar el cifrado de mensajes. La desventaja principal de ElGamal es la necesidad de números aleatorios y su lentitud, especialmente para firmas. ElGamal es realmente una extensión del protocolo de intercambio de llave de Diffie-Hellman, con algunas funcionalidades como el cifrado de mensajes. Sin embargo su seguridad es muy dependiente de la aleatoriedad de alguno de los parámetros utilizados dentro del algoritmo. Si estos parámetros no son muy aleatorios, ElGamal es susceptible a algunos de los problemas de Diffie-Hellman. Una desventaja de ElGamal es su velocidad. El algoritmo es muy lento, especialmente cuando es utilizado para firma.

4.3.2. Ataque a la extensión ElGamal de Diffie-Hellman

Depende de la dificultad del cálculo de un logaritmo discreto. Esta función es la inversa de la potencia discreta, o sea, de calcular una potencia y aplicar una función mod.

- Potencia discreta: $Y = X^a\ mod\ q$
- Logaritmo discreto: $X = ln\ d_{a,q}\ (Y)$

Igualmente tiene el ataque de Diffie-Hellman (hombre en medio), ya que no se cuenta con una autoridad certificadora que permita realizar la autenticación de las entidades.

4.4. PROTOCOLO DE DISTRIBUCIÓN DE LLAVE DE NEEDHAM-SCHROEDER

Con base en [18] se describe un protocolo para un servidor de llave para generar y entregar una llave de sesión para un par de usuarios usuario A y usuario B. El tema de la autenticación de dos usuarios resulta cuando una llave de sesión común es usada en una sesión usuario $A \leftrightarrow$ usuario B.

Se deben tomar en cuenta las preguntas:

¿Es el usuario A quien realmente se comunica con el usuario B?

¿Es el usuario B quien realmente se comunica con el usuario A?

En el documento mencionado se consideran dos protocolos: el primero para usuarios cifrando con un criptosistema de llave simétrica, el segundo para usuarios cifrando con un criptosistema de llave pública (PKC).

4.4.1. Needham-schroeder usando un criptosistema de llave simétrica

El servidor de llave se asume un almacenamiento seguro.

La llave secreta del usuario A con identificador $A \rightarrow k_A$ y

La llave secreta del usuario B con identificador $B \rightarrow k_B$

Se asume que:

- Solo el servidor de llave y un usuario tienen conocimiento de la llave secreta del usuario y
- No es factible descifrar mensajes sin una llave.

El proceso de intercambio de llave está compuesto de los siguientes pasos: (Ver Fig 4.3).

1. El usuario A contacta al servidor de llave y solicita que una llave de sesión k sea generada para una sesión del usuario A y del usuario B, esto se hace a través de un mensaje $REQ = (A, B, N(A))$ es transmitido en claro al servidor de llave por el usuario A y contiene los identificadores (A, B) de las dos partes y un NA (usado una sola vez), es introducido como parte de la autenticación del proceso generado por el usuario A. El servidor de llave no puede estar seguro que el mensaje REQ fue originado por el usuario A.
2. En el segundo paso el servidor de llave genera aleatoriamente una llave de sesión k, la cual es transmitida al usuario A en el mensaje $\mathrm{C_2 = E_{K_A}\{M_2\}}$ el cual contiene $\mathrm{M_2 = (N(A), ID(B), k, Auth)}$ es cifrado con la llave k del usuario A $(\mathrm{k_A})$. Incluido dentro de $\mathrm{M_2}$ está $\mathrm{Auth = E_{K_B}\{k, A\}}$, el cual será usado por A para autenticación del usuario hacia B. El usuario A no puede descifrar, modificar o construir una autenticación válida desde $\mathrm{k_B}$ (es secreta).
3. Así la posesión de k_A permite al usuario A decifrar C_2 y recuperar M_2, en particular para obtener la llave de sesión y la autenticación cifrada $Auth = E_{K_B}\{k, A\}$ el cual no puede ser descifrado, así el usuario A envía la llave de sesión k al usuario B en el mensaje $Auth = E_{k_B}\{k, A\}$=C_3.
4. De igual forma la posesión de $k(B)$ permite al usuario B descifrar $Auth = E_{K_B}\{k, A\}$, en particular para obtener la llave de sesión y el identificador A del supuesto C_3 enviado.

   Aunque la integridad de la autenticación es asegurada, la identidad del emisor no lo es, por ejemplo, la autenticación pudo

haber sido transmitida previamente en claro por el usuario A, registrado por el usuario C y ahora repetido al usuario B. Este se queda al usuario B para autenticar que el usuario A fue la fuente del mensaje C_3 que contiene la autenticación.

5. El usuario B genera un segundo "nonce" $N(B)$ y transmite el mensaje $C_4 = E_k(N(B))$ al usuario A.

   La posesión de la llave de sesión k permite al usuario A decifrar el mensaje C_4 y recuperar el "nonce" $N(B)$ generado por el usuario B.
6. El usuario A modifica el "nonce" $N(B)$ de alguna manera estándar; por ejemplo $N(B) \rightarrow N*(B) = N(B) + 1$.
7. El usuario A transmite el mensaje $C_5 = E_k\{N*(B)\}$ al usuario B.
8. El usuario B completa la autenticación del establecimiento de la sesión y el intercambio de llave: la posesión de la llave de sesión k permite al usuario B descifrar el mensaje C_5 y verificar que el "nonce" $N(B)$ ha sido modificado apropiadamente.

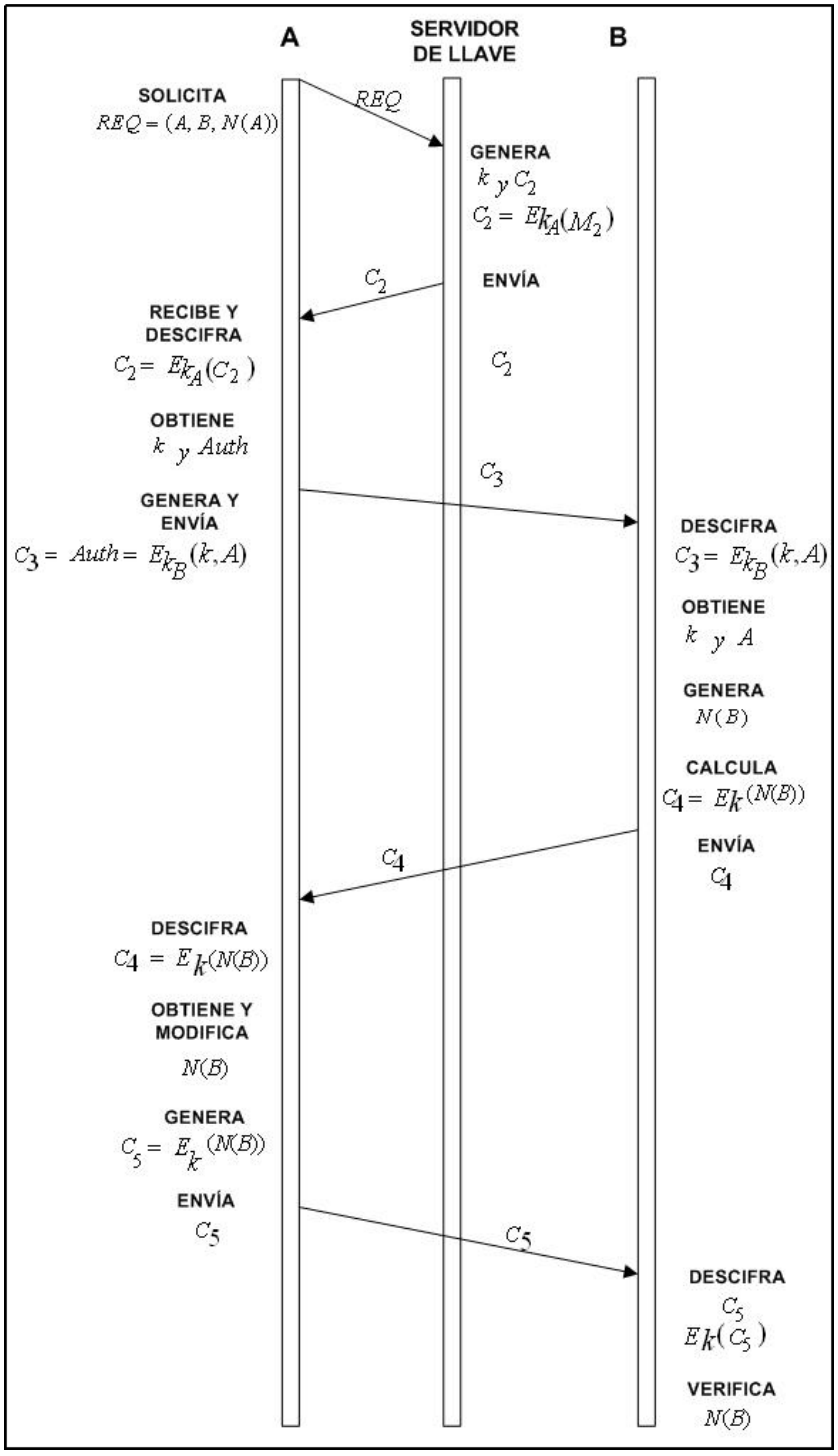

Fig. 4.3 Diagrama de secuencia del protocolo Need-Schroeder en criptosistema de llave simétrica

4.4.2. Needham-schroeder usando un criptosistema de llave pública

d_A y e_A denota las llaves privada y pública de la entidad A.

d_B y e_B denota las llaves privada y pública de la entidad B y

d_S y e_S denota las llaves privada y pública del servidor de llaves.

Esto asume que:

- Las llaves públicas del servidor de llaves son conocidas y
- El conocimiento de la llave pública del servidor (e_S) no permite la determinación de la llave privada o el descifrado de mensajes cifrados.

El proceso de intercambio de llave está compuesto de los siguientes pasos. Ver Fig. 4.4.

1. El usuario A contacta al servidor de llave y en el mensaje $REQ1$ solicita una llave de sesión k que sea generada para una sesión usuario A ↔ Usuario B. $REQ1$ contiene los identificadores (A, B) de las dos partes y es transmitida en claro al servidor de llave por el usuario A.
2. El servidor de llave responde transmitiendo el mensaje $C_2 = E_{d_S}\{M_2\}$ cifrado para el usuario A, usando la llave privada d_S del servidor de llave. Los datos de M_2 consiste del identificador B y la llave pública e_B del usuario B.
3. El usuario A genera un nonce $N(A)$, el cual junto con el identificador A es transmitido al usuario B en el mensaje $C_3 = E_{e_B}\{M_3 = N(A), A\}$, cifrado usando la llave pública e_B del usuario B. La identidad del emisor de C_3 debe ser autenticado, un proceso de dos pasos.

4. El usuario B confirma al servidor de llave transmitiendo el mensaje en claro $REQ2 = (B, A)$ al servidor de llave.
5. El servidor de llave responde transmitiendo el mensaje $C_4 = E_{d_S}\{M_5\}$. Los datos de M_5 consisten del identificador A y la llave pública (e_A) del usuario A.

   ¿Quién podría haber construido el mensaje $C_4 = E_{d_S}\{M_5\}$? Solo una parte con la llave secreta d_S del servidor de llave.

   En este punto las llaves públicas de los usuarios han sido autenticadas por mensajes del servidor de llaves. La identidad de alguna comunicación entre el usuario A y el usuario B deben ser autenticadas, un proceso compuesto de dos pasos.
6. El usuario B transmite el mensaje $C_5 = E_{e_A}\{M_5\}$ al usuario A cifrado con la llave pública e_A del usuario A. Los datos de M_5 consisten de un usuario B que genera un segundo nonce $N(B)$ con el nonce $N(A)$ recibido del usuario A en el mensaje M_3.
7. La posesión de la llave privada d_A permite al usuario A descifrar el mensaje C_5 y recuperar el segundo nonce $N(B)$, generado por el usuario B con el nonce $N(A)$ recibido del usuario A en el mensaje M_3. El usuario A puede verificar que el nonce $N(A)$ recibido es el transmitido en el mensaje M_3.
8. El usuario A responde transmitiendo el mensaje $C_6 = E_{e_B}\{M_6\}$ al usuario B cifrado con la llave pública e_B del usuario B. Los datos de M_6 consisten del nonce $N(B)$ generado por el usuario B.
9. La posesión de la llave privada d_B permite al usuario B descifrar el mensaje C_6 y checar si el nonce $N(B)$ ha sido regresado.

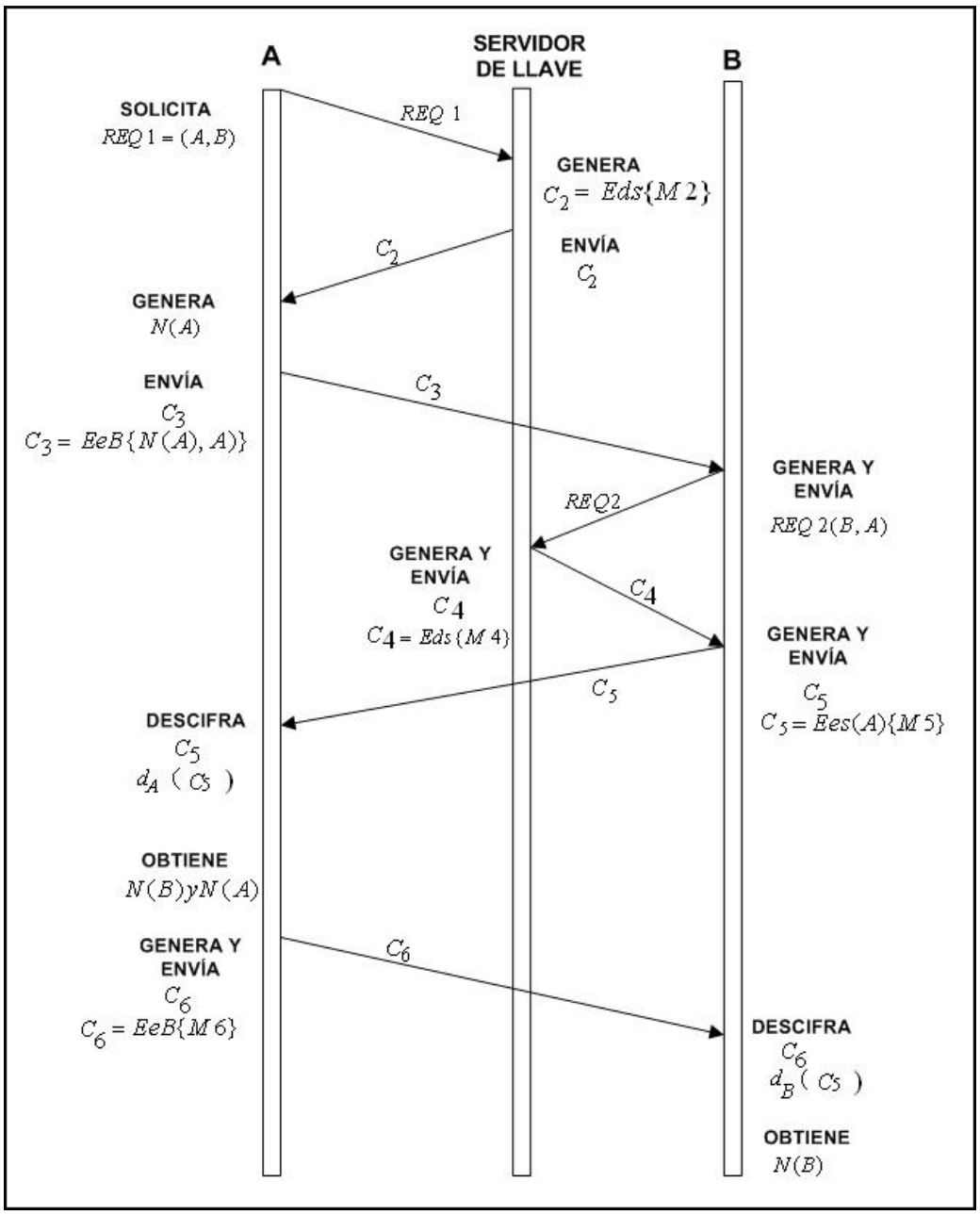

Fig. 4.4 Diagrama de secuencia del protocolo Need-Schroeder en criptosistema de llave pública

A continuación se resumen los protocolos anteriormente descritos, en las Tablas 1 y 2, en donde C. A denota Autoridad Certificadora.

NOMBRE	ATAQUES	PUBLICO	CODIGO ABIERTO	SERVICIOS QUE OFRECE	COMPLEJIDAD COMPUTACIONAL
DIFFIE-HELLMAN	**X**	**X**	**X**	Secreto compartido, identificación e intercambio de llave.	**X**
ELGAMAL EN 1 PASO	**X**	**X**		Identificación, autenticación, intercambio de llave y secreto compartido.	**X**
MTI EN DOS PASOS	**X**	**X**			**X**
CIFRADO ASIMÉTRICO	**X**	**X**			**X**
EXTENSIÓN ELGAMAL DE DIFFIE-HELLMAN	**X**	**X**			**X**
NEEDHAM-SCHROEDER EN CRIPTOSISTEMA DE LLAVE SIMÉTRICA	**X**	**X**			**X**
NEEDHAM-SCHROEDER EN CRIPTOSISTEMA DE LLAVE PÚBLICA	**X**	**X**			**X**

Tabla 1. Resumen 1 de los protocolos descritos

NOMBRE	SEGURIDAD INCONDICIONAL	ACUERDO	DISTRIBUCIÓN	UTILIZA A. C.
DIFFIE-HELLMAN	X	X		
ELGAMAL EN 1 PASO	X	X		
MTI EN DOS PASOS	X	X		X
CIFRADO ASIMÉTRICO	X		X	X
EXTENSIÓN ELGAMAL DE DIFFIE-HELLMAN	X		X	X
NEEDHAM-SCHROEDER EN CRIPTOSISTEMA DE LLAVE SIMÉTRICA	X		X	X
NEEDHAM-SCHROEDER EN CRIPTOSISTEMA DE LLAVE PÚBLICA	X		X	X

Tabla 2. Resumen 2 de los protocolos descritos

CONCLUSIONES

Es importante conocer el funcionamiento de los protocolos de establecimiento y administración de llave, ya que aunque la criptografía proporciona herramientas para establecer una comunicación segura, con base en el principio de Kerckhoffs, uno de los aspectos más importantes que se debe de considerar en dicha comunicación es la seguridad de las llaves.

Se hace mención que algunos de los protocolos descritos en esta tesina necesitan la intervención de una tercera entidad o entidad de confianza para lo cual se requiere la implementación de una infraestructura más compleja ya que entre otras cosas se necesita de la administración, registros y control de datos para que funcione de forma correcta.

Finalmente en la práctica cuando se requiera seleccionar un protocolo para su implementación, se debe tomar en cuenta al menos los siguientes tres criterios: de fácil implementación, que sea un protocolo estándar (de jure) y que no tenga licenciamiento (que sea código libre).

El trabajo futuro que se desprende de esta investigación es el análisis desde el punto de vista de las características cuantitativas de los protocolos de establecimiento y administración de llave previamente descritos, para lo cual se hará necesarios la simulación y puesta en marcha de éstos.

REFERENCIAS BIBLIOGRÁFICAS

[1] RFC 2828 Internet Security Glossary. Technologies May 2000. Disponible en: http://www.faqs.org/ftp/rfc/pdf/rfc2828.txt.pdf

[2] Alfred Menezes, Paul Oorscht, and Scott Vanstone. “Handbook of Applied Cryptography”. CRC Press, Inc., Boca Raton FL USA 1997.

[3] Instituto Nacional de Estadística e Informática. República de Perú. Disponible en: http://www.inei.gob.pe/biblioineipub/bancopub/Inf/Lib5010/cap0501.htm

[4] S. Garfinkel, G. Spafford. “Practical Unix and Internet Security”. O’Reilly & Associates Inc., 3ª Edición Beijing, E.U. Febrero 2003.

[5] Seguridad de la Información. Disponible en: Argentina.http://www.segu-info.com.ar/criptologia/criptologia.htm

[6] Francisco Javier Moliner López “Informáticos de la Generalitat VALENCIANA GRUPO A Y B, Volumen II”, 1ª Edición, MAD-Eduforma. DOGV, 2005

[7] Daltabuit, Hernández, Mallén, Vázquez. “La Seguridad de la Información”. Limusa. 1a Edición. México, 2007.

[8] B. Schneider, “Applied Criptography”. J. Wiley. Reino Unido (Inglaterra), 1994.

[9] Thierry de Saint Pierre, Director North Supply Chile, “Administración de llaves criptográficas”. Disponible en: http://www.dcc.uchile.cl/~cc51d/docs2001/c5-Kdc.pdf

[10] RFC 2522 - Session-Key Management Protocol. Disponible en: http://www.faqs.org/rfcs/rfc2522.html

[11] Hernández Goya Calendaria, “Diseño de protocolos criptográficos: Nuevas propuestas basadas en grafos”, Universidad de la laguna, Departamento de Estadística, Investigación Operativa y Computación. Disponible en: ftp://tesis.bbtk.ull.es/ccppytec/cp166.pdf

[12] Rolf Oppliger. “Contemporary Cryptography. Artech House”. Boston-Lomdon, 2005.

[13] M. Kaeo. “Designing Network Security”. Cisco Press, 2a Edición. 1999.

[14] Elaine B Barker, William C. Barker, Annabelle Lee. “Guideline for implementing cryptography in the federal government”, NIST Special Publication 800-21 Second Edition. 2005. Disponible en: http://csrc.nist.gov/publications/nistpubs/800-21-1/sp800-21-1Dec2005.pdf.

[15] Roberto Gómez Cárdenas, Ricardo C. Lira Plaza, Adolfo Grego, “Esquema de almacenamiento seguro de llaves criptográficas”, Departamento de Ciencias computacionales, Instituto Tecnológico y de Estudios Superiores de Monterrey-Campus Edo. de México. Disponible en: http://homepage.cem.itesm.mx/rogomez/Publicaciones/CIC2001.pdf

[16] Ramió Aguirre, Jorge Libro Electrónico de Seguridad Informática y Criptografía. (Curso en Diapositivas - Texto guía de clases) Versión 4.1 publicada en Internet y de libre distribución. Edición en papel; Dpto. de Publicaciones de la EUI, 2006.

[17] Manuel José Lucena López “Criptografía y Seguridad en Computadores”. Libro electrónico publicado bajo licencia Creative Commons. 4ª edición. Mayo de 2003. Disponible en el vínculo: “enlace principal” de la URL: http://wwwdi.ujaen.es/~mlucena/wiki/pmwiki.php?n=Main.LCripto

[18] Alan G. Konheim “Computer Security and Cryptography”, Wiley-Interscience, 2a edición, USA, 2007.