Esquema de firma digital basado en el problema de reducción de Lattice SVP (Shortest vector problem) y CVP (Closest vector problem)

JUAN GABRIEL QUINTERO PEÑA

Universidad Industrial de Santander
Escuela de Ingeniería de Sistemas e Informática
Maestría en Ingeniería
Bucaramanga
2006

Esquema de firma digital basado en el problema de reducción de Lattice SVP (Shortest vector problem) y CVP (Closest vector problem)

JUAN GABRIEL QUINTERO PEÑA

Informe final del Trabajo de Investigación presentado como requisito para obtener el título Magíster en Ingeniería: **Área Informática Y Ciencias de la Computación**.

Director: Edilberto José Reyes González, M.Sc
Codirector: Luis Ignacio González Ramírez, M.Sc

Universidad Industrial de Santander
Escuela de Ingeniería de Sistemas e Informática
Maestría en Ingeniería
Bucaramanga
2006

RESUMEN

TITULO: ESQUEMA DE FIRMA DIGITAL BASADO EN EL PROBLEMA DE REDUCCIÓN DE LATTICE SVP (SHORTEST VECTOR PROBLEM) Y CVP (CLOSEST VECTOR PROBLEM).[*]

AUTOR: Quintero Peña Juan Gabriel.[**]

PALABRAS CLAVES: criptografía de clave pública, firma digital, funciones Hash, redes (lattices), archivos binarios.

DESCRIPCIÓN

Desde que el hombre comenzó a comunicarse con sus semejantes ha experimentado la necesidad de proteger la información confidencial de otras personas. A lo largo de la historia se han utilizado diferentes técnicas de protección, desde la esteganografía para ocultar la existencia de los mensajes secretos en imágenes hasta la criptografía de clave secreta y pública, para cifrar el contenido de los mensajes de forma que sean inteligibles para cualquiera que no posea la clave de descifrado.

Esta tesis presenta las nociones de firma digital y redes (Lattice). Se describe la secuencia de pasos necesaria para firmar un mensaje digitalmente mediante redes. La seguridad de esta técnica descansa en la complejidad computacional para resolver los problemas del vector más corto (SVP Shortest Vector Problem) y el vector más cercano de una red a un vector dado (CVP Closest Vector Problem). El objetivo es brindar una alternativa criptográfica de clave pública para la protección de la información.

Con el desarrollo del esquema se pretende comprender la aplicación del problema de reducción de Lattice a la firma digital de mensajes. Por medio de los resultados del presente trabajo se pueden estudiar alternativas para combinar los algoritmos de firma digital existentes con los basados en Lattice. Este libro comienza con un bosquejo del trabajo realizado, partiendo de la descripción del plan de proyecto, los objetivos, la justificación, las etapas de desarrollo y los logros obtenidos. Al final se presentan conclusiones y recomendaciones para futuros trabajos.

---

[*] Tesis de Maestría.

[**] Facultad de Fisicomecánicas, Maestría en Ingeniería Área informática y ciencias de la computación, Director de Proyecto: Prof. Edilberto J. Reyes González M.Sc, Codirector de Proyecto: Luis I. González Ramírez M.Sc.

ABSTRACT

TITLE: Scheme of digital signature from Lattice reduction problems SVP (Shortest vector problem) y CVP (Closest vector problem).[*]

AUTHOR: Quintero Peña Juan Gabriel.[**]

Keywords: cryptography of public key ital signature, Hash functions, Lattices, binary files.

DESCRIPTION

Ever since the man began to communicate with his resemblances has experienced the necessity to protect the confidential information of other people. Throughout history different techniques of protection have been used, from the esteganografía to hide the existence of the secret messages in images to the cryptography of secret and public key, to cipher the content of the messages so that they are intelligible.

This thesis show the knowledge of digital signature and Lattice. The sequence of steps necessary to sign a message is described by means of Latticed. The security of this technique rests in the computacional complexity to solve the problems of the Shortest Problem Vector and the Closest Problem Vector. The objective is to offer a cryptographic alternative of public key for the protection of the information.

The scheme is tried to understand the application of the problem of reduction Lattice to the digital signature of messages. By means of the results of present work alternatives can be studied to combine the existing algorithms of digital signature with the Lattice. This book begins with the made work, starting off of the description of the plan of project, the objectives and the justification. In the end conclusions and recommendations for future works appear**.**

---

[*] Tesis de Maestría.

[**] Faculty of physicomechanics, Masters in Engineering, Area informatic and computer science, Director de Proyecto: Prof. Edilberto J. Reyes González M.Sc, Codirector de Proyecto: Luis I. González Ramírez M.Sc.

TABLA DE CONTENIDO

INTRODUCCIÓN 1

1. PANORAMA GENERAL DEL PROYECTO 2

1.1. DESCRIPCIÓN DEL PROBLEMA DE INVESTIGACIÓN 2
1.1.1. PLANTEAMIENTO DEL PROBLEMA 3
1.2. JUSTIFICACIÓN 4
1.3. OBJETIVOS 5
1.3.1. OBJETIVO GENERAL 5
1.3.2. OBJETIVOS ESPECÍFICOS 5
1.4. METODOLOGÍA DE DESARROLLO 6
1.5. LOGROS 7
1.6. BOSQUEJO DEL PRESENTE TEXTO 8

2. FUNDAMENTOS TEÓRICOS 10

2.1. DEFINICIONES BÁSICAS 10
2.1.1. CRIPTOGRAFÍA 10
2.1.2. CRIPTOSISTEMA 11
2.1.2.1. Clasificación 12
2.2. FUNCIÓN RESUMEN (HASH) 14
2.3. FIRMA DIGITAL 16
2.3.1. MÉTODOS DE FIRMA DIGITAL 17
2.3.2. ESQUEMAS DE FIRMA DIGITAL 18
2.3.2.1. Esquema De Firma Con Apéndice 19
2.3.2.2 Esquema De Firma Con Mensaje Recuperable 20

3. PROBLEMAS DE SEGURIDAD EN LA WEB 21

3.1. MARCO LEGAL 21
3.1.1. REGULACIÓN EN COLOMBIA [15] 25
3.1.2. ENTIDADES DE CERTIFICACIÓN 26
3.2. DESCRIPCIÓN DE LOS PROBLEMAS DE SEGURIDAD 27
3.2.1. CORREO ELECTRÓNICO 28
3.2.2. PRODUCTOS SOFTWARE 29

3.2.3. PROBLEMAS FUNDAMENTALES 30
3.2.3.1. Confidencialidad 30
3.2.3.2. Integridad de Datos 31
3.2.3.3. Autenticación 31
3.2.3.4. No Repudio 31
3.2.4. POSIBLES SOLUCIONES 32

4. MODELO FIRMA DIGITAL CON LATTICE 33

4.1. LATTICES (REDES) 33
4.1.1. LATTICE DUAL 35
4.1.2. BASE ORTOGONAL 35
4.1.3. DEFECTO DE ORTOGONALIDAD 36
4.1.4. DEFECTO DE ORTOGONALIDAD DUAL 37
4.1.5. BASE REDUCIDA 37
4.1.6. ALGORITMO LLL 38
4.2. PROBLEMAS RELACIONADOS 39
4.2.1. SBP. PROBLEMA DE LA BASE MÁS PEQUEÑA 39
4.2.2. CVP. PROBLEMA DEL VECTOR MÁS CERCANO 40
4.2.2.1. Encontrando el punto Lattice más cercano 41
4.2.3. SVP. PROBLEMA DEL VECTOR MÁS CORTO 42
4.3. FIRMA DIGITAL CON LATTICE 42
4.3.1. GENERACIÓN DE CLAVES 44
4.3.1.1. Base Privada 44
4.3.1.2. Base Pública 44
4.3.2. ESQUEMA DE FIRMA DIGITAL CON LATTICE 45
4.3.2.1. Proceso de Firma 45
4.3.2.2. Proceso de Verificación 47

5. RESULTADOS 49

5.1. VALIDACIÓN SOFTWARE PGP Vs FIRMA DIGITAL CON LATTICE 49
5.1.1. RESEÑA DEL PGP (PRETTY GOOD PRIVACY) 49
5.1.1.1. Funcionamiento 50
5.1.1.2. Firma Digital 52
5.1.1.3. Gestión de Claves 53
5.1.2. GENERACIÓN DE CLAVES 54
5.1.2.1. PGP 54
5.1.2.2. Lattice 61
5.1.3. FIRMA DIGITAL 63
5.1.3.1. Lattice 66

5.1.4. VERIFICACIÓN DE LA FIRMA DIGITAL 67
5.1.4.1. PGP 67
5.1.4.2. Lattice 69
5.2. ANÁLISIS DE RESULTADOS 71

6. CONCLUSIONES Y RECOMENDACIONES 74

6.1. CONCLUSIONES 74
6.2. RECOMENDACIONES 75

BIBLIOGRAFÍA 77

ANEXOS 80

LISTA DE TABLAS

Tabla 1. Comparación de PGP frente a Firma con Lattice 73

LISTA DE FIGURAS

Fig 1. Criptosistema con clave secreta (simétrico).....12
Fig 2. Criptosistema con clave pública (asimétrico).....13
Fig 3. Ejemplo de aplicación de una función Hash 14
Fig 5. Proceso de Firma digital 19
Fig 7. Ejemplo de un Lattice en dos dimensiones.....33
Fig 8. Ejemplo de una Base para un Lattice en seis dimensiones.....34
Fig 9. Algoritmo LLL.....38
Fig 10. Ejemplo del CVP en dos dimensiones 40
Fig 11. Algoritmo CVP 41
Fig 12. Ejemplo SVP en dos dimensiones.....42
Fig 13. Esquema general de firmado con Lattice.....43
Fig 14. Creación del vector de información.....46
Fig 15. Estructura del mensaje Firmado S.....47
Fig 16. Recuperación del Resumen $h'(M)$ 48
Fig 17. Verificación de un archivo firmado.....48
Fig 18. Software PGP 49
Fig 19. Codificación de un mensaje PGP 52
Fig 20. Ejemplo de clave pública con PGP.....55
Fig 21. Generación de claves con PGP. Paso 1 55
Fig 22. Generación de claves con PGP. Paso 2.....56
Fig 23. Generación de claves con PGP. Paso 3.....57
Fig 24. Generación de claves con PGP. Paso 4.....57
Fig 25. Generación de claves con PGP. Paso 5.....58
Fig 26. Generación de claves con PGP. Paso 6.....59
Fig 27. Generación de claves con PGP. Paso 7.....59
Fig 28. Generación de claves con PGP. Paso 8.....60
Fig 29. Visor de Claves PGP 60
Fig 30. Firma digital con Lattice. Opción generar Claves.....61
Fig 31. Generación de Claves.....62
Fig 32. Resultado de la generación de Claves 62
Fig 33. Resultado de la generación de Claves 63
Fig 34. Barra de herramientas de PGP.....64
Fig 35.Selección de archivo a cifrar y firmas 64
Fig 36.Selección de los destinatarios del mensaje a firmar 65
Fig 37.Confirmación de la identidad del usuario firmante 65
Fig 38.Proceso de cifrado del archivo con PGP.....66
Fig 39. Selección de la opción Firmar (Firma Digital con Lattice) 66
Fig 40. Elección del tipo opciones de Firma Digital con Lattice 67
Fig 41. Mensaje de finalización Firma con Lattice exitosa.....67

Fig 42.Selección del proceso Decrypt/Verify 68
Fig 43.Selección del archivo firmado 68
Fig 44. Selección del usuario receptor del mensaje.....69
Fig 45. Selección de la ruta y nombre del archivo obtenido con PGP 69
Fig 46. Selección de la opción Verificar (Firma Digital con Lattice) 70
Fig 47. Opciones de Verificar Firma Digital mediante Lattice 71
Fig 48. Resultado de firma digital mediante Lattice válida 71

LISTA DE ANEXOS

ANEXO 1. EQUIPO REQUERIDO.....81

INTRODUCCIÓN

Se invita a revisar este aporte a quienes estén explorando alternativas de protección de mensajes utilizando mecanismos de firma digital.

El grupo de investigación LINCE[1] de la Escuela de Ingeniería de Sistemas e Informática de la Universidad Industrial de Santander en su línea de investigación Trionix, Seguridad Informática y Protección de Aplicaciones Software, ha venido desarrollando trabajos de investigación y construyendo el conocimiento necesario para impulsar a la EISI-UIS[2] como pionera en esta área en el departamento de Santander, Colombia.

Entre los proyectos desarrollados al interior del grupo se encuentra el presente trabajo, el cual apunta hacia el desarrollo de un esquema de firma digital basado en los problemas de reducción de Lattice SVP[3] y CVP[4]. Los resultados obtenidos se comparan con datos provenientes de un software comercial que desempeña funciones similares de firma digital de mensajes.

Con el desarrollo del esquema se pretende comprender la aplicación del problema de reducción de Lattice a la firma digital de mensajes. Por medio de los resultados del presente trabajo se pueden estudiar alternativas para combinar los algoritmos de firma digital existentes con los basados en Lattice.

---

[1] Grupo de Investigación en Inteligencia Artificial y Sistemas de Conocimiento Experto
[2] Escuela de Ingeniería de Sistemas e Informática de la Universidad Industrial de Santander
[3] Shortest Vector Problem. Problema del vector más corto.

1. PANORAMA GENERAL DEL PROYECTO

Este libro resume el trabajo realizado en el proyecto de maestría titulado "*Esquema de firma digital basado en el problema de reducción de Lattice SVP (Shortest vector problem) y CVP (Closest vector problem)"*, desarrollado dentro del marco investigativo del grupo LINCE[1], en el área de Seguridad Informática y Protección de Aplicaciones Software.

En este capítulo se hace un bosquejo del trabajo realizado, partiendo de la descripción del plan de proyecto, los objetivos, la justificación, las etapas de desarrollo y los logros obtenidos. Al final se presenta una descripción general de la organización y temática de los demás capítulos del texto.

1.1. DESCRIPCIÓN DEL PROBLEMA DE INVESTIGACIÓN

La facilidad que brinda la Web entorno a la comunicación entre personas permite disminuir el consumo del papel y la tradicional mensajería con la ventaja del aumento en la velocidad de entrega, aunque presenta una dificultad al asociar al mensaje la identidad del usuario. Ésto ocasiona que el intercambio de información a través de la Web se convierta en una actividad insegura debido a que no se tiene certeza de quien remite ni la integridad de los datos. Puede darse el caso que un tercero suplante al emisor o altere el envío sin que exista alguna forma de validar la integridad de la información, lo cual facilita el fraude por parte de cualquiera que posea conocimientos medios en informática.

---

[4] Closest Vector Problem. Problema del vector más cercano.

Una posible solución a esta situación la brinda la criptografía de clave pública, en particular las firmas digitales. Por medio de una firma digital se puede garantizar la autenticidad, integridad, confiabilidad y el no repudio de los mensajes enviados a través de cualquier medio que soporte estas técnicas de protección de información.

1.1.1. Planteamiento Del Problema

Desde que el hombre comenzó a comunicarse con sus semejantes ha experimentado la necesidad de proteger la información confidencial de otras personas. A lo largo de la historia se han utilizado diferentes técnicas de protección, desde la esteganografía para ocultar la existencia de los mensajes secretos en imágenes hasta la criptografía de clave secreta y pública, para cifrar el contenido de los mensajes de forma que sean inteligibles para cualquiera que no posea la clave de descifrado.

Aplicando criptografía de clave pública una persona puede enviar un archivo cifrado a cualquier individuo que tenga una clave pública y una privada asignada. Pero se puede llegar a presentar el problema de negación de autoría del mensaje, desconfianza de la identidad del destinatario o alteración del mensaje enviado. Todo esto podría llevar al interesado en proteger su información a pensar que no existen garantías y a desconfiar de esta técnica.

Una manera de dar solución a este problema es mediante el uso de una firma digital aplicada al momento de enviar el mensaje a través de un medio digital.

Una firma digital es una cadena de datos creada a partir de un mensaje (o parte de él), de forma que sea difícil que quién lo envía reniegue la acción (repudio) y que el

individuo que recibe pueda asegurar que el emisor es realmente quien dice ser, es decir, el receptor de un mensaje digital puede asegurar cual es el origen del mismo (autenticación). Además, una firma digital garantiza la integridad de los datos (que no se hayan modificado durante la transmisión).

El mecanismo de firma digital por ser de clave pública basa su seguridad en algún problema matemático que proporciona una función de una vía (one way function), como son: factorización de números primos grandes (RSA[5]), curvas elípticas, logaritmos discretos y muchos otros, entre los cuales se encuentra el problema de reducción de Lattice. De manera que aplicando cualquiera de ellos se puede garantizar que la información almacenada no podrá ser recuperada mediante el proceso inverso a la técnica usada sin el conocimiento de la clave.

Existen estándares para la implementación de firma digital como el DSS (Digital Signatura Standard), firmas basadas en el RSA, el Gamal, entre otros. La propuesta de este trabajo de investigación es la aplicación del concepto matemático del problema de reducción de Lattice SVP[3] y CVP[4] para el diseño de un esquema criptográfico de firma digital en busca de aportar a la solución de los problemas de seguridad que se presentan en la transmisión de mensajes a través de la Web.

1.2. JUSTIFICACIÓN

La realización de este proyecto aporta los conceptos necesarios para la creación de un esquema de firma digital basado en el problema de reducción de Lattice,

[5] RSA. Algoritmo de clave pública inventado por Ron Rivest, Adi Shamir, y Leonard Adleman.

apoyando la línea de investigación en Seguridad Informática al interior de la EISI-UIS[2]. Aunque existen proyectos relacionados en este campo en el país, aun no se le brinda la importancia que ha ganado con el auge de las telecomunicaciones, razón por la cual no se ha destacado ninguna universidad o institución en la realización de alguna propuesta que garantice la seguridad de la información digital enviada a través de la Web.

Una posibilidad que ofrece esta investigación es la protección de mensajes por medio de una aplicación software que genere y verifique la firma digital aplicada.

1.3. OBJETIVOS

1.3.1. Objetivo General

Aplicar el concepto matemático del problema de reducción de Lattice SVP[3] y CVP[4] a la firma digital en busca de la solución de los problemas de seguridad que se presentan en la transmisión de mensajes a través de la Web.

1.3.2. Objetivos Específicos

- ✓ Identificar y describir los problemas de seguridad que se presentan en la transmisión de mensajes a través de la Web.

✓ Diseñar un esquema criptográfico de firma digital basado en el problema de reducción de Lattice SVP[3] y CVP[4] para la firma de mensajes.

✓ Recopilar la información referente a los conceptos básicos de Lattice requerida para la construcción del esquema criptográfico de firma digital.

✓ Implementar un prototipo de una aplicación software que permita la generación y verificación de firma digital basado en el problema de reducción de Lattice SVP[3] y CVP[4].

1.4. METODOLOGÍA DE DESARROLLO

Para el cumplimiento de los objetivos planteados en este proyecto se diseñaron las siguientes fases.

Fase 1. Estudio de la literatura

Tiene dos objetivos: el primero es recopilar la información necesaria para la comprensión de los teoremas y conceptos matemáticos que soportan la teoría de los Lattices y la firma digital; el segundo es identificar nuevas investigaciones y desarrollos que aporten conocimientos necesarios para la realización de este proyecto y proporcionen realimentación a la comunidad científica. También se busca permanecer en contacto con los avances que se llevan en este campo; para esto se consultarán las bases de datos disponibles en la UIS[6] (IEEE, Applied Science Technology, entre otras), las publicaciones de los centros de investigación y aportes que se encuentren en la Web. Adicionalmente se deben consultar los problemas de seguridad en la transmisión de mensajes a través de la Web.

Fase 2. Diseño del esquema de firma digital

Diseño de un esquema criptográfico de firma digital basado en el problema de reducción de Lattice SVP[3] y CVP[4]. Se llevaron a cabo las siguientes actividades:

- ✓ Estudio de los conceptos matemáticos de Lattice.
- ✓ Estudio de los conceptos criptográficos de Lattice.
- ✓ Estudio de los conceptos criptográficos de firma digital.
- ✓ Estudio de esquemas de firmas digital existentes.
- ✓ Estudio de las leyes colombianas acerca de la firma digital de documentos.
- ✓ Diseño de un esquema de firma digital. Basado en el problema de reducción de Lattice SVP[3] y CVP[4].
- ✓

Fase 3. Implementación de prototipo software

Implementación de un prototipo de aplicación software que permite la generación y verificación de firma digital basado en el problema de reducción de Lattice SVP[3] y CVP[4].

Fase Documentación

Elaboración del informe final y del artículo de investigación, donde se consignan las experiencias desarrolladas, los conocimientos adquiridos y demás información obtenida a lo largo del trabajo de investigación.

1.5. LOGROS

El proyecto realizó un aporte a la academia, ya que el área de la Seguridad Informática no se trabajaba al interior de la EISI-UIS[2], y los resultados del proyecto

[6] Universidad Industrial de Santander, Bucaramanga. Colombia

ofrecen bases teóricas confiables del tema que permiten plantear trabajos posteriores que mantengan la línea de investigación activa aportando nuevos conocimientos.

A la culminación de este proyecto, se pueden destacar los siguientes aspectos:

- ✓ Se fortaleció la línea de investigación Trionix, Seguridad Informática y Protección de Aplicaciones Software, al interior de la EISI-UIS[2].

- ✓ Se diseñó un esquema de firma digital basado en el problema de reducción de Lattice.
- ✓ Se construyó un prototipo de aplicación que permite la aplicación del esquema propuesto.

- ✓ Se dejan bases para la realización de proyectos que involucren firma digital e intercambio de claves.

1.6. BOSQUEJO DEL PRESENTE TEXTO

En el capítulo 2 se exponen los fundamentos teóricos sobre el cual está soportado el proyecto. Se presentan definiciones básicas de criptografía, concepto y funcionamiento de firma digital, y funciones Hash (resumen).

El capítulo 3 describe algunos problemas de seguridad en la Web y el marco legal aplicado a la legislación colombiana que establece la reglamentación de firmas, certificados digitales y conceptos afines.

En el capítulo 4 se empieza definiendo el concepto matemático de Lattice y los problemas relacionados a éste, como son el SVP[3] y CVP[4]. Luego describe el esquema de firma digital con Lattice planteado basado en los conceptos descritos anteriormente.

El capítulo 5 describe los resultados de las pruebas realizadas que comparan el esquema diseñado con un software comercial (PGP[7]). Se finaliza con el análisis de resultados.

Finalmente se presentan las conclusiones y recomendaciones.

[7] Pretty Good Privacy

2. FUNDAMENTOS TEÓRICOS

En este capítulo se presentan los fundamentos teóricos sobre los que se apoya este trabajo. Se mencionan algunos temas propios de la criptografía como la definición de función Hash, criptosistemas, clave pública y clave secreta. Finalmente se explica el significado de "firma digital". Todos estos conceptos son esenciales si se quiere entender y justificar las características del esquema de firma digital basado en Lattice presentado en el capítulo 4.

2.1. DEFINICIONES BÁSICAS

2.1.1. Criptografía

La palabra criptografía proviene del griego *kryptos* (que significa esconder) y *gráphein* (escribir), es decir, escritura escondida. La criptografía ha sido usada a través de los años para el envío de mensajes confidenciales cuyo propósito es que sólo las personas autorizadas puedan entender su contenido.

Una definición más formal es:
"Rama inicial de las Matemáticas y en la actualidad de la Informática y la Telemática, que hace uso de métodos y técnicas con el objeto principal de cifrar y/o proteger un mensaje o archivo por medio de un algoritmo, usando una o más claves"[8].

La Criptografía sólo se refiere al uso de códigos, por lo que no engloba a las técnicas que se usan para romper dichos códigos (**Criptoanálisis**). El término

Criptología, aunque no está recogido aún en el Diccionario, se emplea para agrupar estas dos disciplinas.

2.1.2. Criptosistema

Se define como la quíntupla (M, C, K, E, D) donde:

- ✓ ***M*** es el conjunto de todos los mensajes sin cifrar (texto plano) que pueden ser enviados.

- ✓ ***C*** es el conjunto de todos los posibles mensajes cifrados (criptogramas).

- ✓ ***K*** es el conjunto de claves 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 clave ***k***.

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

Todo Criptosistema debe cumplir la condición:

$$D_{k_2}\left(E_{k_1}\left(m\right)\right) = m$$

Es decir, si se toma un mensaje *m*, se cifra empleando la clave k_1 y luego se descifra empleando la clave k_2, se obtiene de nuevo el mensaje original ***m***. En el caso de los criptosistemas con clave secreta $k_1 = k_2$ y en los de clave pública k_1 y k_2 son diferentes.

---

[8] **[RAM05].** Capitulo 2, página 36.

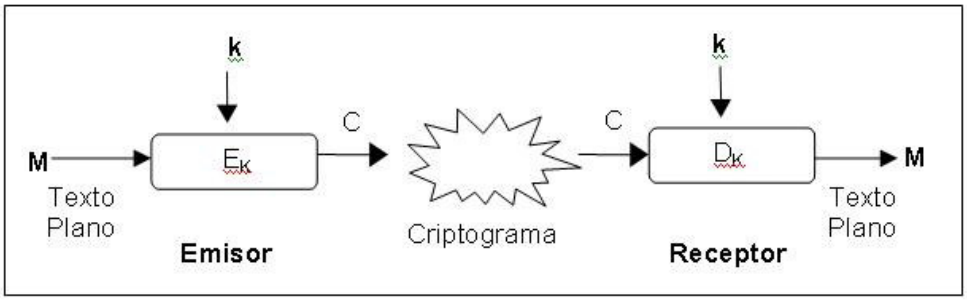
2.1.2.1. Clasificación

Es realizada según el tratamiento que se de al mensaje y el tipo de clave que se maneja.

- ✓ Según el **tratamiento del mensaje** se dividen en:
  - Cifrado en bloque (IDEA, AES, RSA* ...) 64 ó 128 bit.
  - Cifrado en flujo (A5, RC4, SEAL ...) cifrado bit a bit.

- ✓ Según el **tipo de claves** se dividen en:
  - **Cifrado con clave secreta (simétricos)**

Fig 1. Criptosistema con clave secreta (simétrico)

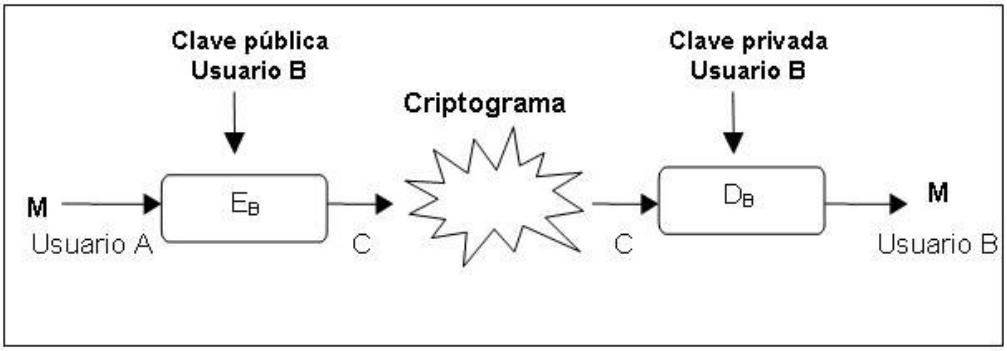


Existe una única clave (secreta) que deben compartir emisor y receptor. Con la misma clave se cifra y se descifra, por lo que la seguridad reside sólo en mantener dicha clave en secreto.

- **Cifrado con clave pública (asimétricos)**

Cada usuario crea un par de claves, una privada y otra pública, inversas dentro de un cuerpo finito. Lo que se cifra en emisión con una clave, se descifra en recepción con la clave inversa. La seguridad del sistema reside en la dificultad computacional de descubrir la clave privada a partir de la pública. Para ello se usan funciones matemáticas de un sólo sentido (one way function) o con trampa.

Fig 2. Criptosistema con clave pública (asimétrico)



En la actualidad la criptografía asimétrica o de clave pública se divide en tres familias según el problema matemático en el cual apoye su seguridad. Éstas son:

1. **F**actorización **E**ntera **PFE**

Pertenecen a esta familia el sistema **RSA** y el de **R**abin **W**illiams (**RW**)**.**

2. **P**roblema del **L**ogaritmo **D**iscreto **PLD**

Pertenecen a esta familia el sistema de **D**iffie **H**ellman (**DH**) de intercambio de claves y el sistema **DSA** de firma digital.

3. **P**roblema del **L**ogaritmo **D**iscreto **E**líptico **PLDE**

Basan su seguridad en el **P**roblema del **L**ogaritmo **D**iscreto **E**líptico (**PLDE**)**.** En esta familia se encuentran varios esquemas de intercambio de claves y de firma digital como son: el **DHE** (Diffie Hellman Elíptico), **DSAE**, (**N**yberg-**R**ueppel) **NRE**, (**M**enezes, **Q**u, **V**anstone) **MQV** [30], etcétera.

2.2. FUNCIÓN RESUMEN (HASH)

De manera matemática se puede definir una función resumen (hash functions) como proyecciones de un conjunto, generalmente con un número elevado de elementos (incluso infinitos), sobre un conjunto de tamaño fijo y mucho más pequeño que el anterior.

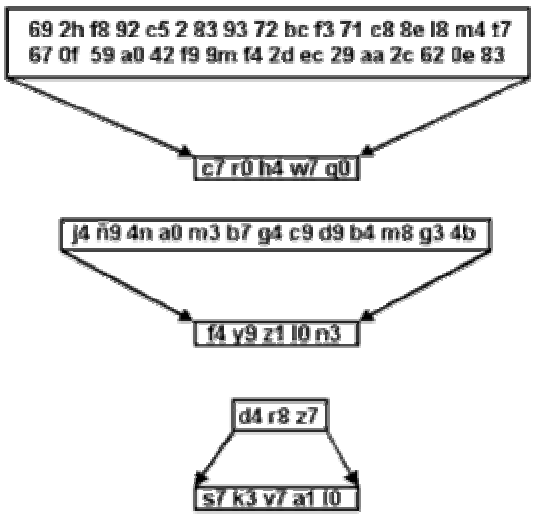
Al aplicar una función hash a un archivo se obtiene un número llamado ***número resumen***, el cual tiene las siguientes características:

✓ Todos los números resumen generados con un mismo método tienen el mismo tamaño independiente de el texto utilizado como base.

✓ Dado un texto base, es fácil y rápido (para un computador) calcular su resumen.

✓ Es imposible reconstruir el texto base a partir del número resumen.

Fig 3. Ejemplo de aplicación de una función Hash



Los algoritmos hash más conocidos son el MD5[9] y el SHA-1[10] utilizados para firmas digitales.

El uso común criptográfico de las funciones hash son la firma digital y la integridad de datos. Con firma digital, un mensaje largo es resumido (usando una función Hash) y sólo el valor Hash (número resumen) es firmado. El receptor del mensaje recibe y verifica que la firma es correcta para este valor Hash. Ésto ahorra tiempo y espacio comparado con firmar el mensaje completo, lo cual podría involucrar división del contenido en bloques de tamaño apropiado y el firmado de cada uno. La dificultad de encontrar dos mensajes con el mismo número resumen es un requerimiento de seguridad; el valor hash de un mensaje podría ser el mismo de otro, permitiendo a un individuo firmar un mensaje y después decir que él había firmado otro.

Las funciones hash pueden ser usadas para integridad de datos de la siguiente manera: el número resumen correspondiente a una entrada en particular es calculado en un momento. La integridad de este valor es protegida de alguna manera. Luego, para verificar la no alteración, el número resumen es calculado nuevamente y comparado con el valor original; si son iguales se puede afirmar que el archivo no ha sido alterado. La aplicación específica incluye la protección de virus y la distribución de software.

Funcionamiento

La forma como las funciones hash procesan un mensaje es la siguiente:

✓ La función hash toma como entrada una cadena de longitud arbitraria, supóngase de **n** bits. Luego divide este mensaje en bloques iguales, de 160 bits

[9] Función Hash que genera una cadena de 128 bit. Ver **[MEN97]**

en el caso de SHA-1[10] o 128 bits para la MD5[9]; debido a que el mensaje original por lo general no es un múltiplo del tamaño de los bloques utilizados para completar un número entero de pedazos, al último se le agrega un relleno de ceros.

En síntesis, lo que se hace es tomar el mensaje, partirlo en pedazos de longitud constante y combinar de alguna forma pedazo por pedazo hasta obtener un único mensaje.

2.3. FIRMA DIGITAL

El propósito de una firma es asociar la identidad del firmante con la información registrada en el documento (autenticidad). Las firmas manuscritas permiten realizar esta función pero si el documento es alterado el firmante seguirá avalando la información registrada en él. Las firmas digitales por el contrario permiten asociar la identidad del firmante con el documento firmado y detectar modificaciones del mismo (Integridad).

Una firma digital de un documento es un segmento de información (un grupo de bits) basado en: el documento a firmar, la clave del usuario que firma y en una función o esquema de firma.

Las firmas digitales se construyen utilizando criptografía de clave pública, la cual utiliza dos claves, una privada y otra pública. La primera se mantiene en secreto y la segunda se divulga libremente. Para firmar es necesario utilizar la clave privada

[10] Función Hash que genera una cadena de 160 bit. Ver **[MEN97]**

y para verificar la firma se utiliza la clave pública. Las firmas digitales permiten garantizar los servicios de Integridad y Autenticidad al tiempo.

Para que una firma digital producida sea válida debe cumplir:

- ✓ **Vigencia.** Haber sido creada durante el período de vigencia del certificado digital válido del firmante.
- ✓ **Verificación.** Ser debidamente verificada por la referencia a los datos de verificación de firma digital indicados en dicho certificado según el procedimiento de verificación correspondiente.
- ✓ **Emisión.** Que dicho certificado haya sido emitido o reconocido por un certificador licenciado.

2.3.1. Métodos De Firma Digital

- ✓ **Método RSA**

Es el método más usado para firmar digitalmente. Para que sea seguro la longitud de sus claves (una pública y otra privada) debe ser de 1024 bits, es decir un número de un poco más de 300 dígitos.

Conviene usar este método por razones de compatibilidad debido a su gran uso y popularidad.

- ✓ **Método DSA**

Es oficialmente aceptado para las transacciones oficiales en el gobierno de USA. Usa claves del mismo tamaño que **RSA**, pero esta basado en otra técnica. Aún así, sea podido mostrar que es casi equivalente en seguridad a **RSA**.

- ✓ **Método Curvas Elípticas**

Tiene como ventaja, comparado con los dos anteriores, la reducción hasta en 164 bits, es decir casi 45 dígitos, de las claves manteniendo la misma seguridad. Por lo cual se recomienda su uso donde existen recursos reducidos, como en Smart Cards, PDAs, etc.

Este método se ha integrado como el reemplazo oficial de DSA para el gobierno de USA.

2.3.2. Esquemas De Firma Digital

Un esquema de firma cuenta con dos partes, la primera se denomina proceso de firma (similar al cifrado) y la segunda parte proceso de verificación (similar al descifrado). Existen dos tipos de esquemas de firma digital, uno denominado *esquema de firma digital con apéndice*[11] y otro *esquema de firma digital con mensaje recuperable*.

2.3.2.1. Esquema De Firma Con Apéndice

✓ **Proceso de Firma**

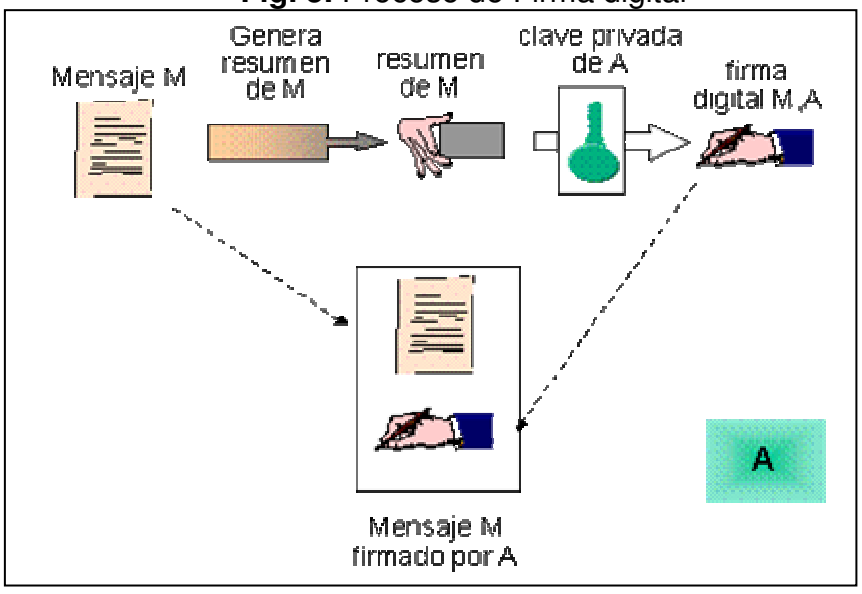
1. Se aplica al mensaje M (mensaje a firmar) una función hash que reduce su magnitud a un número resumen H(M) de longitud 128 o 160 bits, dependiendo el tipo de función que aplique, lo cual permite trabajar cualquier archivo como una cadena de tamaño constante.

2. El número resumen H(M) se somete a un proceso de cifrado según el algoritmo aplicado (RSA, DSS) con lo cual se obtiene un número h(M).

$$s = h(M)^d \bmod n$$

3. Se envía el mensaje firmado s

Fig. 5. Proceso de Firma digital



[11] Ver **[HCW80].**

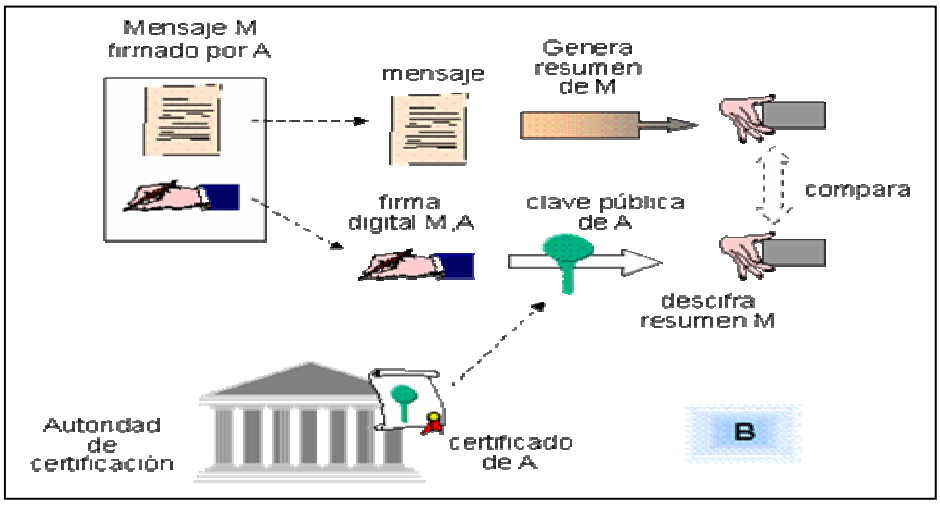
✓ **Proceso de Verificación**

1. Quien recibe *s*, se supone conoce el mensaje M, aplica la función de verificación que depende de la clave pública de quien se dice propietario del mensaje.

$$h' = s^e \bmod n$$

2. Se aplica la función hash al mensaje M y si $h(M) = h'$ entonces acepta la firma.

Fig 6. **Verificación de una Firma digital**



2.3.2.2 Esquema De Firma Con Mensaje Recuperable

En este esquema no es necesario saber el mensaje, luego que la firma es aceptada el mensaje puede recuperarse a partir de la firma.

3. PROBLEMAS DE SEGURIDAD EN LA WEB

En este capitulo se expone el marco legal de la legislación colombiana sobre los conceptos relacionados con firma digital, certificados digital y entidades certificadoras, y los aspectos relacionados con los problemas de seguridad que se presentan al realizar transacciones a través de la Web.

3.1. MARCO LEGAL

El congreso de Colombia, aprobó el uso de las firmas digitales como elemento probatorio y reglamentó su uso mediante la **ley 527 de 18 de agosto de 1999**, "por medio de la cual se define y reglamenta el acceso y uso de los mensajes, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación".

En apartes de la ley se hacen las siguientes definiciones, reglamentaciones y aclaraciones:

- ✓ En el capitulo I se **definen las firmas digitales** como:

"Se entenderá como un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje permite determinar que este valor se ha obtenido

exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación"[12].

✓ "Artículo 7º. **Firma**. Cuando cualquier norma exija la presencia de una firma o establezca ciertas consecuencias en ausencia de la misma, en relación con un mensaje de datos, se entenderá satisfecho dicho requerimiento si:

- Se ha utilizado un método que permite identificar al iniciador de un mensaje de datos e indicar que el contenido cuenta con su aprobación.

- Que el método sea tanto confiable como apropiado para el propósito por el cual el mensaje fue generado o comunicado.

Lo dispuesto en este artículo se aplicará tanto si el requisito establecido en cualquier norma constituye una obligación, como si las normas simplemente prevén consecuencias en el caso de que no exista una firma."[13]

✓ En la parte III "**Firmas digitales, Certificados digitales y Entidades de certificación**", afirma:

Artículo 28. Atributos jurídicos de una firma digital. Cuando una firma digital haya sido fijada en un mensaje de datos se presume que el suscriptor de aquella tenía la intención de acreditar ese mensaje de datos y de ser vinculado con el contenido del mismo.

[12] Literal c) del artículo 2 de la ley 527 de 1999

[13] Artículo 7 de la ley 527 de 1999

Parágrafo. El uso de una firma digital tendrá la misma fuerza y efectos que el uso de una firma manuscrita, si aquélla incorpora los siguientes atributos:

1. Es única a la persona que la usa.
2. Es susceptible de ser verificada.
3. Está bajo el control exclusivo de la persona que la usa.
4. Está ligada a la información o mensaje, de tal manera que si éstos son cambiados, la firma digital es invalidada.
5. Está conforme a las reglamentaciones adoptadas por el Gobierno Nacional.

✓ Define la **Entidad de Certificación** como:

"Es aquella persona que, autorizada conforme a la presente ley, está facultada para emitir certificados en relación con las firmas digitales de las personas, ofrecer o facilitar los servicios de registro y estampado cronológico de la transmisión y recepción de mensajes de datos, así como cumplir otras funciones relativas a las comunicaciones basadas en las firmas digitales"[14].

✓ En el Capítulo II, Entidades de Certificación, establece las características de una **Entidad Certificadora:**

Articulo 29. Características y requerimientos de las entidades de certificación. Podrán ser entidades de certificación, las personas jurídicas, tanto públicas como privadas, de origen nacional o extranjero y las cámaras de comercio, que previa solicitud sean autorizadas por la Superintendencia de Industria y Comercio y que cumplan con los requerimientos establecidos por el Gobierno Nacional, con base en las siguientes condiciones:

[14] Literal d) del artículo 2 de la ley 527 de 1999

- Contar con la capacidad económica y financiera suficiente para prestar los servicios autorizados como entidad de certificación.

- Contar con la capacidad y elementos técnicos necesarios para la generación de firmas digitales, la emisión de certificados sobre la autenticidad de las mismas y la conservación de mensajes de datos en los términos establecidos en esta ley.

- Los representantes legales y administradores no podrán ser personas que hayan sido condenadas a pena privativa de la libertad, excepto por delitos políticos o culposos; o que hayan sido suspendidas en el ejercicio de su profesión por falta grave contra la ética o hayan sido excluidas de aquélla. Esta inhabilidad estará vigente por el mismo período que la ley penal o administrativa señale para el efecto.

✓ En el **Artículo** 32, Deberes de las Entidades de Certificación, se establecen los deberes de dichas entidades tales como:

- Emitir certificados conforme a lo solicitado o acordado con el suscriptor.

- Implementar los sistemas de seguridad para garantizar la emisión y creación de firmas digitales, la conservación y archivo de certificados y documentos en soporte de mensaje de datos.

- Garantizar la protección, confidencialidad y debido uso de la información suministrada por el suscriptor.

- Garantizar la prestación permanente del servicio de entidad de certificación.

- Atender oportunamente las solicitudes y reclamaciones hechas por los suscriptores.

- Efectuar los avisos y publicaciones conforme a lo dispuesto en la ley.

- Suministrar la información que le requieran las entidades administrativas competentes o judiciales en relación con las firmas digitales y certificados emitidos y en general sobre cualquier mensaje de datos que se encuentre bajo su custodia y administración.

- Permitir y facilitar la realización de las auditorías por parte de la Superintendencia de Industria y Comercio.

- Elaborar los reglamentos que definen las relaciones con el suscriptor y la forma de prestación del servicio.

- Llevar un registro de los certificados.

3.1.1. Regulación En Colombia [15]

Resumiendo las leyes que han aportado a la regulación de las Firmas Digitales y las Entidades de Certificación, se pueden mencionar:

- ✓ Ley 527 de 1999. Comercio Electrónico.
- ✓ Decreto Reglamentario 1747 de 2000. Reglamenta L.527- ENTIDADES DE CERTIFICACIÓN
- ✓ Título V Capítulo 8 de la Circular Única de la SIC
- ✓ Resolución 26930 del 2000. Estándares autorización Entidades de certificación.
- ✓ Resolución 36904 de 2001- Complementa 26930.

- ✓ Circular Externa No. 23 de 2002.
- ✓ Circular Externa No. 02 de 2002.
- ✓ Circular Externa No. 19 de 2002.

3.1.2. Entidades De Certificación[15]

En Colombia se encuentran autorizadas para ejercer esta función:

- ✓ **CERTICÁMARA, S.A.**

Avenida Calle 26 No. 68D - 35 Piso 5, Bogotá D.C.

Autorizada mediante resolución No. 1007 del 24 de enero de 2002.

Actualmente presta los siguientes servicios:

- ➢ **Certificados de Firma**
  - Certificados de Representación Empresa/Entidad.
  - Certificados de Pertenencia Empresa/Entidad.
  - Certificados de Profesional Titulado.
  - Certificados de Titular de Función Pública.
  - Certificados de Persona Natural.

- ➢ **Certificados de Empresa**
  - Certificados de Servidor Seguro.
  - Certificados para Firma de Código.
  - Certificados de VPN / Intranet.

- ✓ **AERONÁUTICA CIVIL**

Autorizada mediante resolución No. 17257 del 31 de mayo de 2002, modificación de cambio de nombre mediante resolución No. 28171 del 29 de agosto de 2002.

- ✓ **INSTITUTO COLOMBIANO DE CODIFICACIÓN Y AUTOMATIZACIÓN COMERCIAL**

Av. El Dorado No. 68B-85, torre II Piso 6, Bogotá D.C.
Autorizada mediante resolución No. 25352 del 31 de agosto de 2002.

- ✓ **BANCO DE LA REPÚBLICA**

Carrera 7 No. 14-78, Bogotá D.C.
Autorizada mediante resolución No. 6372 del 28 de Febrero de 2003.

- ✓ **A TODA HORA S.A.**

Carrera 13 No. 27 - 47 Piso 13, Bogotá D.C.
Autorizada mediante resolución No. 29844 del 22 de octubre de 2003.

3.2. DESCRIPCIÓN DE LOS PROBLEMAS DE SEGURIDAD

Al navegar a través de la Web un usuario se enfrenta a posibles fraudes como son:

- ✓ Clonación Servidor.
- ✓ Suplantación del Cliente.
- ✓ Suplantación de Mensaje.

[15] Tomado de Bernate & Gamboa Abogados

Esto da lugar a desconfianza para realizar operaciones que involucren información de alta confidencialidad llevando al usuario a tomar decisiones drásticas como aislarse de cualquier tipo de transacción por medio de la Web.

Una medida de protección es configurar el navegador para que verifique la "confiabilidad" de los sitios Web a los cuales se ingresa. Los datos que se transmiten al utilizar la interfaz Web (incluyendo el e-mail y la contraseña del usuario) viajan de forma segura a través de la red cifrándolos con una clave secreta contenida en el certificado de seguridad. Éste no es comercial y por lo tanto no es reconocido de forma automática por los navegadores Web. Aceptar este certificado es seguro y la confidencialidad de sus datos es tan alta como la de los datos cifrados utilizando un certificado comercial.

3.2.1. Correo Electrónico

Hay varios aspectos de seguridad relacionados con el correo electrónico que se deben conocer:

✓ Los mensajes de correo electrónico que se envían pasan a través de muchas computadoras dentro de la Web. Cualquiera de estos sistemas puede permitir la lectura del correo que pasa a través de él.

Para evitar esto, el mejor método es cifrar los mensajes. La forma más popular para cifrar correo es utilizar programas como PGP[7] o Gnu Privacy Guard (GnuPG), éstos ofrecen diversas opciones para cifrar archivos.

✓ Los anexos (attachments) del correo pueden ocultar virus. En la mayoría de los casos, éstos son mal intencionados e instalan virus en el computador.

Como posible solución a esta problemática se recomienda instalar un antivirus. Pero si lo que se quiere es no correr riesgo se debe borrar el correo que contenga anexos de tamaño elevado y de procedencia dudosa.

✓ Un correo puede ser falsificado para que parezca enviado por alguien de confianza cuando en realidad ha sido remitido por un usuario malicioso. Este correo falsificado puede solicitar un cambio de configuración o información para que el intruso pueda comprometer el sistema de una manera más fácil.

Un error frecuente es suponer que un sistema no va sufrir ningún ataque debido a la "*poca importancia de la información que se maneja*". Si el sistema está conectado a una red puede ser de interés para un intruso, ya sea porque puede utilizarlo para atacar a otra víctima desde el computador o sólo por un ataque indiscriminado.

3.2.2. Productos Software

Cualquier producto de software multiusuario en un entorno seguro, corriendo bajo cualquier plataforma, programado en cualquier lenguaje, debe cumplir tres premisas básicas de seguridad:

- ✓ Debe validar los datos que introduce el usuario.

- ✓ En caso error, no debe dar información detallada al usuario de lo que ha salido mal.

- ✓ No debe facilitar el acceso a información sensible que pueda permitir a un usuario no autorizado conocer los mecanismos internos del software.

Si el servidor devuelve demasiada información, el usuario tendrá una buena oportunidad para crear una cadena de texto malformada que le permitiría seguir investigando el problema, o incluso, el acceso a información sensible.

3.2.3. Problemas Fundamentales

Existe un número básico de requerimientos legales que obliga a las partes comprometidas en una transacción y hacen que los documentos legalmente exijan cumplir lo pactado. Para cumplir éstos, en el mundo digital la transacción debe tener las siguientes características:

3.2.3.1. Confidencialidad

Usada para guarda el contenido de la información para todos aquellos que estén autorizados. Confidencialidad es un término sinónimo de privacidad. Son

numerosas las formas de proporcionar confidencialidad, desde protección física hasta algoritmos matemáticos que proporcionan datos incompresibles.

3.2.3.2. Integridad de Datos

Garantiza la no autorización de alteraciones de datos. Para asegurar la integridad de datos se debe tener la capacidad de detectar cambios por partes no autorizadas. La manipulación de datos incluye la inserción, borrado y sustitución.

3.2.3.3. Autenticación

Usada para identificar. Esta función aplica a entidades y a la información misma. Dos partes dentro de una comunicación deben identificarse entre sí. La información enviada sobre un canal debe ser autenticada para los datos de origen, tiempo de envío, contenido de datos, etc. Este aspecto de la criptografía es usualmente divido en dos clases mayores: autenticación de entidad y autenticación de datos de origen.

La autenticación de datos de origen implica proporcionar datos de integridad (por si un mensaje es modificado, el código también debe haber cambiado).

3.2.3.4. No Repudio

Evita a una entidad negación previa de acciones o compromisos. Por ejemplo, una entidad puede autorizar una compra y después negar tal orden. Una forma de resolver esta disputa involucra incluir a una tercera parte que sirva de certificador.

3.2.4. Posibles Soluciones

Para la solución a los problemas que se presentan cuando existe intercambio de información a través de la Web se pueden plantear soluciones como:

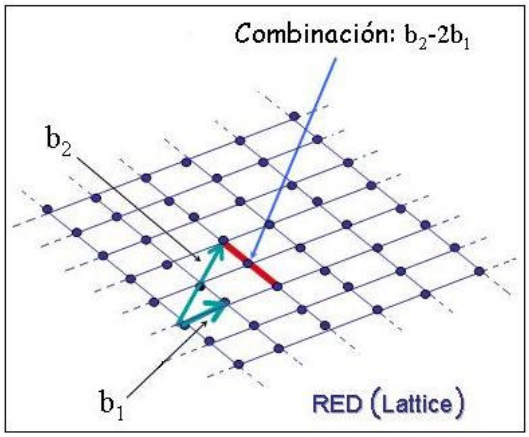
- ✓ **Criptografía de Clave Pública**
  - Uso de Firma Digital
- ✓ **Políticas de Sitios Web**
  - Remover interpretadores que no se necesiten en absoluto y que puedan representar un agujero de seguridad.
  - Chequear regularmente tanto los registros del Web como los del sistema, para detectar actividades sospechosas.
  - Revisar continuamente la información acerca de los nuevos errores encontrados, ataques y riesgos en los sistemas del servidor Web.

4. MODELO FIRMA DIGITAL CON LATTICE

En el capítulo anterior se mostraron los aspectos relacionados con los problemas de seguridad que se presentan al realizar transacciones a través de la Web y el marco legal de la legislación colombiana sobre los conceptos de firma digital, certificados digitales y entidades certificadoras. El presente capítulo comienza con las definiciones teóricas del concepto de Lattice y sus problemas relacionados, buscando consolidar las bases para exponer el modelo de firma digital basado en el problema de reducción de Lattice.

4.1. LATTICES (REDES)

Fig 7. Ejemplo de un Lattice en dos dimensiones



Son objetos geométricos usados para resolver muchos problemas en matemáticas y en ciencias de la computación. Se puede describir geométricamente como un conjunto de intersecciones de puntos de una cuadricula regular n dimensional

(pero no necesariamente ortogonal).

Una definición formal de un Lattice es la siguiente:

Sí $B=\{b_1,b_2,\ldots,b_n\}$ es un conjunto de vectores linealmente independientes en $\mathbb{R}^n$, el Lattice generado por B, que usualmente se denota por $L(B)$, es el conjunto de todas las combinaciones lineales con coeficientes enteros de los vectores base B, es decir

$$L(B) \overset{def}{=} \left\{ \sum_i k_i b_i : k_i \in \mathbb{Z} \text{ para todo } i \right\}$$

En este caso decimos que B es una base de $L(B)$ y que $L(B)$ tiene dimensión n.

Se toma una base para un Lattice $\mathbb{R}^n$ como una matriz B no singular de $n \, x \, n$, en la cual las columnas son los vectores de la base. De esta forma, el Lattice generado por B es el conjunto

$$L(B) = \left\{ Bv : v \text{ es un vector entero, } v \in \mathbb{Z}^n \right\}$$

el vector Bv es conocido como un vector-Lattice (o punto Lattice).

Fig 8. Ejemplo de una Base para un Lattice en seis dimensiones

Posición 0	Posición 1	Posición 2	Posición 3	Posición 4	Posición 5
0	9	7	5	-1	-1
-1	6	-4	-2	6	-9
-2	-7	9	9	-5	5
-6	-3	6	3	6	6
9	-8	-2	-7	-9	11
1	-1	7	-6	-1	-7

Existen muchas bases para un Lattice L. Por ejemplo, si el conjunto $B=\{b_1,b_2,\ldots,b_n\}$ genera algún Lattice entonces tomando cualquier vector $b_i \in B$ y adicionando a él cualquier combinación lineal entera de los otros vectores se obtiene una base diferente para el mismo Lattice. Un hecho importante sobre los Lattice es que todas las bases de un Lattice tienen el mismo determinante. Esto ocurre debido que hay una matriz entera T tal que $BT=C$ y otra matriz T^{-1} tal que $CT^{-1}=B$.

Los Lattices proporcionan problemas que no pueden ser resueltos en tiempo polinomial (NP-hard), que permiten crear funciones de una vía o funciones tramposas; uno de ellos es el problema del vector más corto (SVP) y otro es el del vector más cercano (CVP) en L (Lattice).

4.1.1. Lattice Dual

Si $B=\{b_1,b_2,\ldots,b_n\}$ es una base para algún Lattice $L(B)$ en $\mathbb{R}^n$ (donde B es una matriz de $n\ x\ n$ cuyas columna son los $b_i{}'s$) entonces el Lattice dual de $L(B)$ es el generado por las filas de la matriz B^{-1}.

4.1.2. Base Ortogonal

Cualquier base B puede ser transformada en una base ortogonal para el mismo espacio vectorial usando el método de ortogonalización de Gram-Schmidt.

Si se tienen los vectores $\vec{b}_1,\ldots,\vec{b}_n \in \mathbb{R}^{m\ x\ n}$, no necesariamente ortogonales (o incluso linealmente independiente), que generan un espacio vectorial $V=span(B)$,

siempre se puede encontrar una base ortogonal $B^* = \left[\vec{b}_1^* \middle| \ldots \middle| \vec{b}_n^* \right]$ para V de la siguiente manera:

$$\vec{b}_1^* = \vec{b}_1$$

$$\vec{b}_2^* = \vec{b}_2 - \mu_{2,1}\vec{b}_1^* \text{ donde } \mu_{2,1} = \frac{\left\langle \vec{b}_2, \vec{b}_1^* \right\rangle}{\left\langle \vec{b}_1^*, \vec{b}_1^* \right\rangle}$$

$$\vec{b}_i^* = \vec{b}_i - \sum_{j<i} \mu_{i,j}\vec{b}_j^* \text{ donde } \mu_{i,j} = \frac{\left\langle \vec{b}_i, \vec{b}_j^* \right\rangle}{\left\langle \vec{b}_j^*, \vec{b}_j^* \right\rangle}$$

Las columnas de B^* son ortogonales $\left(\left\langle \vec{b}_i^*, \vec{b}_j^* \right\rangle \text{ para todo } i \neq j \right)$ por lo tanto las columnas (no cero) de B^* son linealmente independiente y forman una base para el espacio vectorial $span(B)$. Sin embargo, ellas generalmente no son una base para el Lattice $L(B)$, aunque $span(B) = span(B^*)$ en general $L(B) = L(B^*)$ no tiene validez.

4.1.3. Defecto de Ortogonalidad

Sea B una matriz no singular de $n \, x \, n$, el defecto de ortogonalidad de B es definido como

$$orth-defect(B) \overset{def}{=} \frac{\prod_i \|b_i\|}{|\det(B)|}$$

donde $\|b_i\|$ es la norma euclidiana de las $i-esimas$ columnas de B.

$orth-defect(B)=1$ sí y sólo sí las columnas de B son ortogonales unas a otras, y $orth-defect(B)>1$ de otra manera.

4.1.4. Defecto de Ortogonalidad Dual

Sea B una matriz no singular de $n\ x\ n$, el defecto de ortogonalidad dual de B se define como:

$$orth-defect^{*}(B) \overset{def}{=} \prod_i \frac{\|\hat{b}_i\|}{|\det(B^{-1})|} = |\det(B)| \bullet \prod_i \|\hat{b}_i\|$$

donde $\hat{b}_i$ son las $i-esimas$ filas en B^{-1}.

4.1.5. Base Reducida

Una base $B=(\vec{b}_1,\ldots,\vec{b}_n) \in \mathbb{R}^{mxn}$ es reducida δ si tiene las siguientes propiedades:

1. (longitud reducida) $|\mu_{i,j}| \leq \frac{1}{2}$ para todo $i > j$.

2. Para cualquier par de vectores consecutivos $\vec{b}_i, \vec{b}_{i+1}$, se tiene

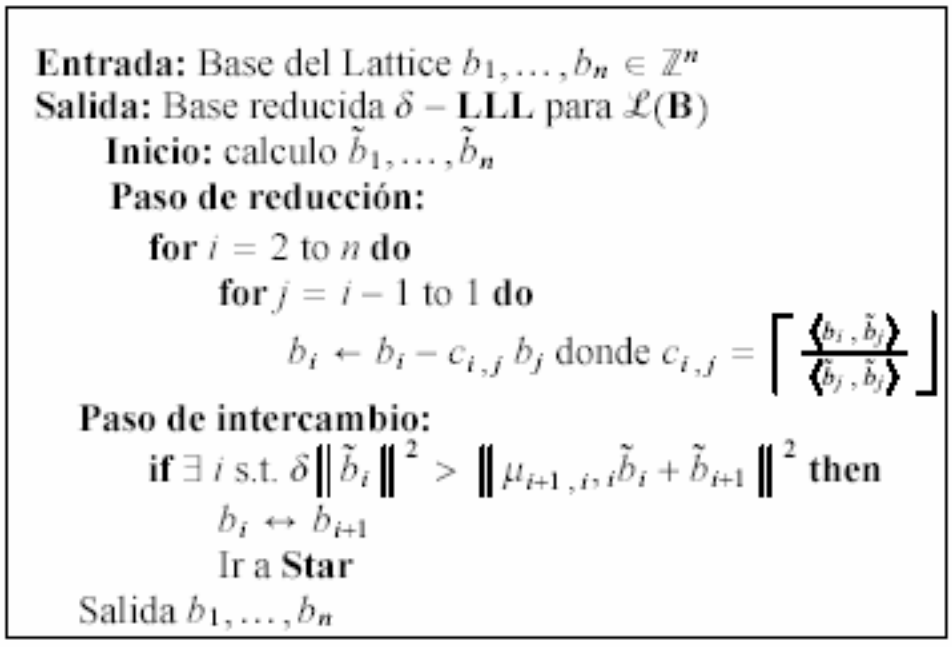
$$\delta \left\| \pi_i \left(\vec{b}_i \right) \right\|^2 \leq \left\| \pi_i \left(\vec{b}_{i+1} \right) \right\|^2$$

o equivalente $\delta \left\| \vec{b}_i^* \right\|^2 \leq \left\| \vec{b}_{i+1}^* + \mu_{i+1} * \vec{b}_i^* \right\|^2$.

4.1.6. Algoritmo LLL

La reducción de base LLL produce vectores que son más cortos con un factor $2^{\frac{n}{2}}$.
El algoritmo LLL de reducción en un Lattice se puede formular según **Fig**. 9.

Fig 9. Algoritmo LLL



[16]

[16] μ es el coeficiente de Gram-Schmidt, definido como $\mu_{i,j} = \frac{\langle b_i, \tilde{b}_j \rangle}{\langle \tilde{b}_j, \tilde{b}_j \rangle}$

El paso de intercambio toma en cuenta la segunda propiedad de una base reducida. El paso de reducción toma en cuenta la primera propiedad, en éste la base Gram-Schmidt no cambia (por lo tanto los vectores $\tilde{b}_1,\ldots,\tilde{b}_n$ no necesitan ser recalculados). Está sujeto a que sólo se ejecuten operaciones columnas de la forma $b_i \leftarrow b_i + ab_j$ para $i > j$ y $a \in \mathbb{Z}$. Estas operaciones no cambian la ortogonalización de Gram-Schmidt.

Este algoritmo funciona de manera similar a Gram-Schmidt pero con el coeficiente $\mu_{i,j}$ redondeado al entero más cercano.

4.2. PROBLEMAS RELACIONADOS

Existen algunos problemas relacionados con Lattice que se consideran intratables computacionalmente debido al tiempo que necesitan para ser solucionados.

4.2.1. SBP[17]. Problema de la Base Más Pequeña

Dada una base B para un Lattice en $\mathbb{R}^n$, el objetivo es encontrar la base "más pequeña" B' para el mismo Lattice. Existen muchas variantes del problema dependiendo del significado exacto de "la más pequeña".

Una manera de interpretar “la más pequeña” es teniendo en cuenta el defecto de ortogonalidad, en este caso se debe considerar la variante en la cual se busca la base B' de $L(B)$ que tenga el defecto de ortogonalidad más pequeño. No se conoce un algoritmo que en tiempo polinomial solucione el problema; existen

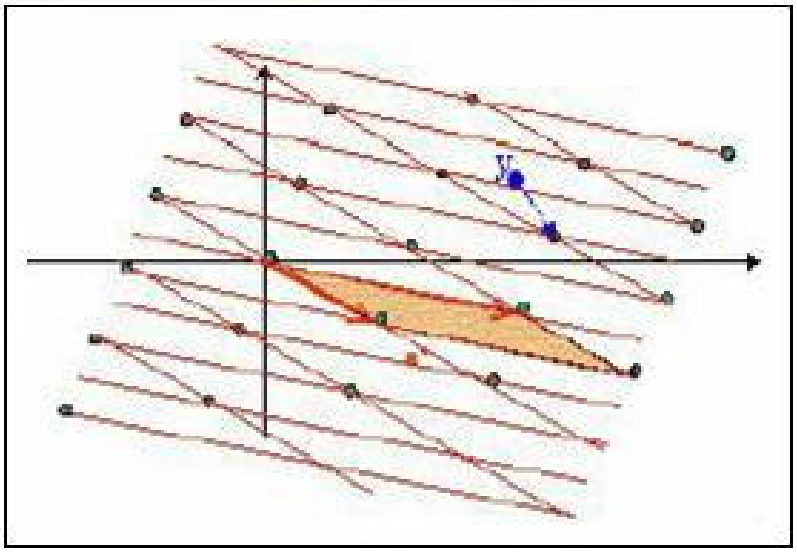
[17] Smallest Basis Problem. Problema de la base más pequeña.

algunas variantes de los algoritmos de LLL que alcanzan un porcentaje de aproximación de $2^{O(n^2)}$ en el peor caso para **SBP** en $\mathbb{R}^n$.

4.2.2. CVP[18]. Problema del Vector Más Cercano

Dado un Lattice $L(B)$ en $\mathbb{R}^n$ y un vector objetivo $\vec{t_0} \in \mathbb{R}^n$, hallar un punto de $L(B)$ tal que $\left\|\vec{t} - \vec{t_0}\right\|$ sea mínimo, es decir hallar $\vec{t} \in L(B)$ de manera que $\left\|\vec{t} - \vec{t_0}\right\| \leq \left\|\vec{w} - \vec{t_0}\right\|$ para todo $\vec{w} \in L(B)$.

Fig 10. Ejemplo del CVP en dos dimensiones



Se simplifica este problema probando encontrar un punto dentro de un cierto paralelepípedo en $\mathbb{R}^n$.

[18] Closet Vector Problem. Problema del vector más cercano.

4.2.2.1. Encontrando el punto Lattice más cercano

Se muestra en **Fig.** 11 un algoritmo que permite encontrar un vector entero x de manera que $B\vec{x}$ esté dentro de $\vec{t_o} + P\left(B^*\right)$:

Fig 11. Algoritmo CVP

Paso 0. $i := n$

Paso 1. $x_i := \left\lfloor \dfrac{\left\langle \vec{t}, \vec{\mathbf{b}}_i^* \right\rangle}{\left\langle \vec{\mathbf{b}}_i^*, \vec{\mathbf{b}}_i^* \right\rangle} \right\rceil$

Paso2. $\vec{t} = \vec{t} - x_i \vec{\mathbf{b}}_i$

Paso3. $i := i - 1$, sí $i \geq 1$ Ir al Paso 1.

La operación $\lfloor x \rceil$ denota la elección del entero más cercano a x

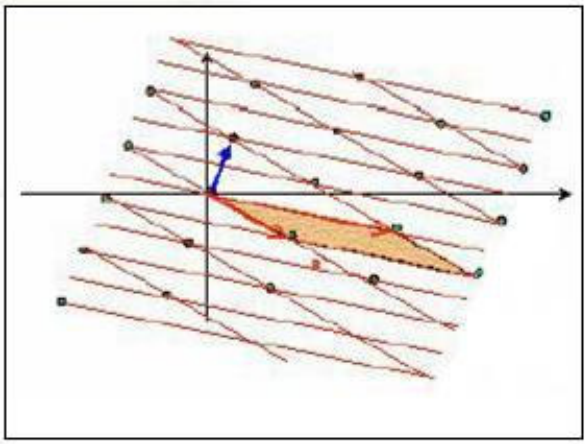
En caso de empate se escoge el más pequeño.

Los mejores algoritmos en tiempo polinomial para aproximación son los basados en LLL **[LEN82]** y sus variantes. Babai **[BAB86]** probó que el CVP en $\mathbb{R}^n$ puede aproximarse en tiempo polinomial con un factor de $2^{\frac{n}{2}}$. Sin embargo, estos límites se refieren a los peores casos, y los algoritmos se ejecutan "usualmente" mucho mejor que el límite mencionado anteriormente.

4.2.3. SVP[19]. Problema del vector más corto

Dado un Lattice $L(B)$ hallar el vector no nulo de $L(B)$ más corto (respecto a una norma $\|.\|$[20]), es decir dado $L(B)$ hallar $\vec{t} \in L(B) \setminus \{\vec{0}\}$ talque $\|\vec{t}\| \leq \|\vec{w}\|$ para todo $\vec{w} \in L(B) \setminus \{\vec{0}\}$.

Fig 12. Ejemplo SVP en dos dimensiones



La solución al SVP depende de la norma que se esté usando. Cuando se utilizan bases reducidas el primer vector es aproximadamente el más corto en el Lattice.

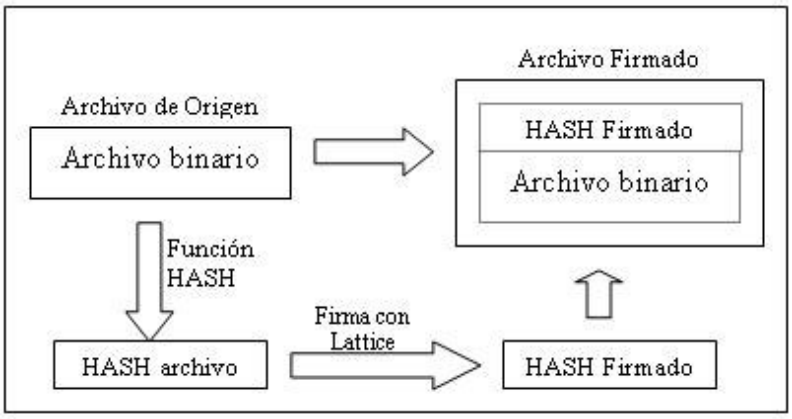
4.3. FIRMA DIGITAL CON LATTICE

Para realizar este proceso se debe aplicar una función resumen al mensaje a

[19] Shortest Vector Problem. Problema del vector más corto.
[20] Es una norma. Por lo general se utiliza la norma euclidiana definida como $\|\vec{x}\| = \sqrt{\langle \vec{x}, \vec{x} \rangle} = \sqrt{\sum_{i=1}^{n} x_i^2}$.

firmar en busca de obtener una cadena de longitud fija (HASH archivo). Luego se firma con Lattice este resumen obteniendo un HASH Firmado. En **Fig** 13 se muestra el esquema general de firmado.

Fig 13. Esquema general de firmado con Lattice



Para poder enviar la información se concatenan el resumen firmado con el archivo binario creando un paquete, buscando que cuando llegue a su destino y se verifique la validez de la firma, se pueda extraer el archivo original (binario).

Todo el proceso de firma con Lattice se muestra para el usuario como una elección de un archivo fuente, tipo de resumen (MD5 o Sha1), clave privada o clave pública y ruta de archivo destino. De manera que la complejidad del problema para firmar archivos queda totalmente oculta para el usuario.

Para firmar archivos con Lattice se requiere contar con un juego de claves, la privada y la pública, las cuales se obtienen como se muestra en el apartado 4.3.1.

4.3.1. Generación de Claves

Este proceso se debe realizar para obtener las claves pública (B) y privada (R), las cuales corresponden a las bases de los Lattices a utilizar en el proceso.

Las bases B y R son representadas por matrices de $n\ x\ n$ donde los vectores bases son las columnas de éstas.

4.3.1.1. Base Privada

Se crea con base en un paralelepípedo. En particular, se construye a partir de una matriz R' que se distribuye en $\{-l,\ldots,+l\}^{n\ x\ n}$ y se utiliza para obtener R mediante $R \leftarrow R' + k \bullet I$, donde k es un entero y I es la matriz identidad.

Para garantizar la calidad de la base, antes de finalizar el proceso de creación se aplica una reducción LLL de manera que se obtenga un conjunto de vectores linealmente independiente que formen una base para el Lattice.

4.3.1.2. Base Pública

Una vez se cuente con la base privada R, se debe escoger la base pública B según una cierta distribución del Lattice $L(R)$.

Para crear la base pública se multiplica R por algunas matrices unimodulares "aleatorias" para obtener B, particularmente $B = R \bullet T_1 \bullet T_2 \bullet \ldots T_n$. Cada una de estas

matrices de transformación unimodular se escoge como un producto de un matriz triangular superior y una matriz triangular inferior, $T_i = L_i U_i$, donde las entradas de la diagonal en L_i, U_i son ± 1, las otras entradas de L_i, U_i son $\{-1, 0, +1\}$.

4.3.2. Esquema De Firma Digital Con Lattice

Al igual que los esquemas de firma digital existentes, la firma con Lattice se realiza por medio de dos procesos, uno de firma y otro de verificación. En cada uno de ellos se llevan a cabo procedimientos que aplican el problema de reducción de Lattice.

Se propone un esquema de firma con mensaje recuperable.

4.3.2.1. Proceso de Firma

Requiere conocer el Lattice B (clave pública).

1. Se le aplica al mensaje M (mensaje a firmar) una función Hash que reduce su longitud a un mensaje $h(M)$ de 128 o 160 bits, dependiendo el tipo de función que el usuario escoja (MD5 o SHA-1), lo cual permite trabajar cualquier archivo como una cadena de tamaño constante y garantiza que no ocurrirán alteraciones durante el envío.

2. $h(M)$ se somete a un proceso de cifrado aplicando Lattice.

Se crea un vector e (error o ruido) y un vector v (vector de información).

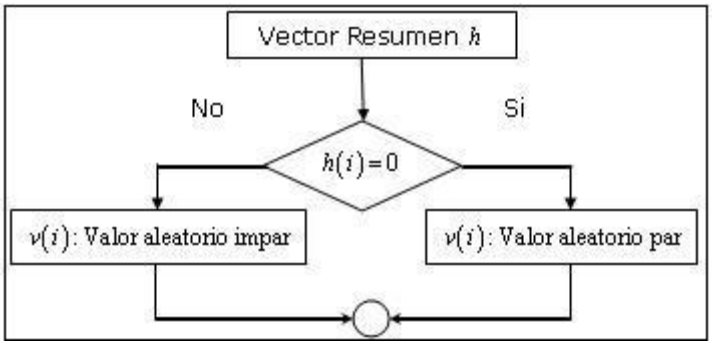
- **Vector** e

Se crea escogiendo valores entre $-\sigma$ y σ de manera aleatoria (entre $-\text{Máxima norma de } R \quad y \quad \text{Máxima norma de } R$) asignándolos a cada componente del vector, donde σ se toma como $\sigma \leq \text{Máxima norma de } R$.

- **Vector** v

A partir del resumen obtenido del archivo $h(M)$ se crea un vector que contiene valores aleatorios pares e impares dependiendo del contenido del mismo.

Fig 14. Creación del vector de información

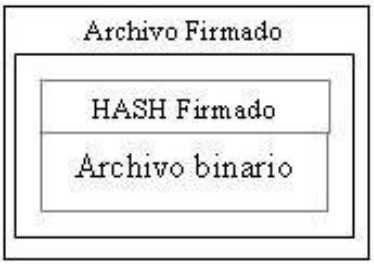


3. Se realiza el cifrado del vector v obteniendo un vector c mediante la operación $c = Bv + e$.

4. Se envía el mensaje firmado S[21]

[21] S está formado por la concatenación del HASH Firmado y el Archivo binario.

Fig 15. Estructura del mensaje Firmado S



4.3.2.2. Proceso de Verificación

Requiere conocer el Lattice R (clave privada).

1. Quien recibe el mensaje firmado S aplica la función de verificación que depende de la clave privada de quien se dice propietario del mensaje.

Teniendo en cuenta la definición

$$\mathbf{T} \stackrel{def}{=} \mathbf{B}^{-1}\mathbf{R}$$

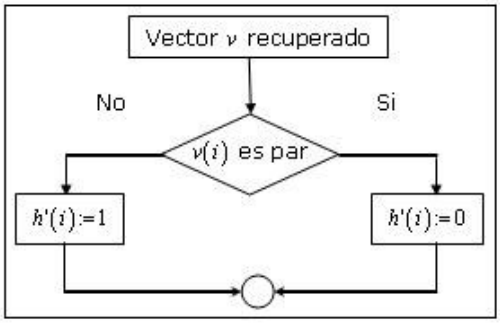
Se recupera el vector v mediante la aplicación de

$$\mathbf{v} \leftarrow \mathbf{T}\lceil \mathbf{R}^{-1}\mathbf{c} \rfloor$$

La función mostrada anteriormente, representa a c como una combinación lineal de las columnas de R y redondea sus coeficientes a los números enteros más cercanos para obtener un punto del Lattice. La representación de este punto como combinación lineal en las columnas de B es el vector v.

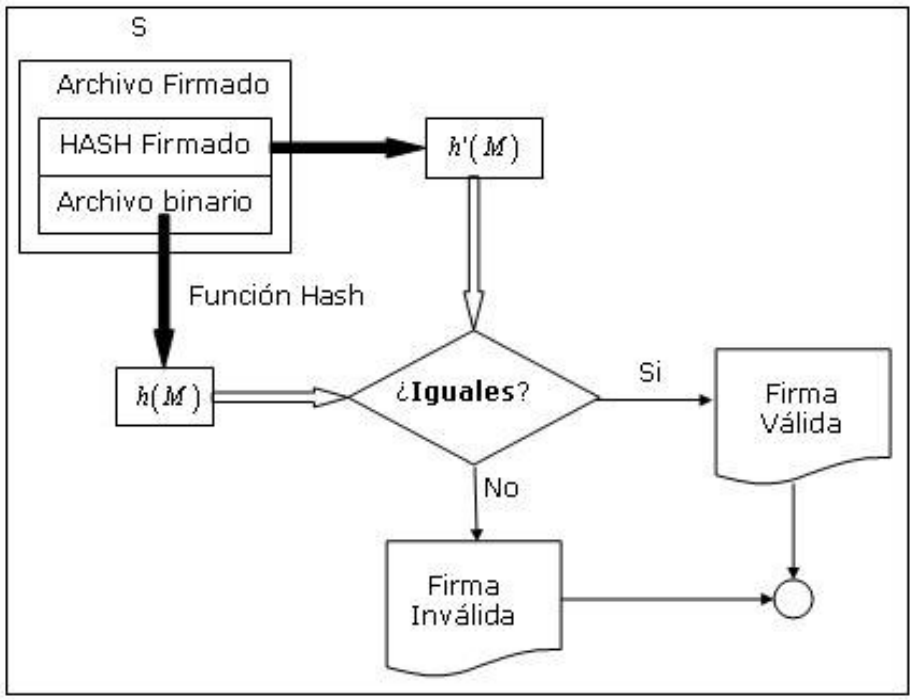
2. Luego de recuperado el vector v se realiza un proceso que recobra el resumen almacenado en él, como se muestra en **Fig.** 16.

Fig 16. Recuperación del Resumen $h'(M)$



3. Se compara lo recuperado ($h'(M)$) con el resumen del archivo $h(M)$ contenido en S. Si coinciden, quiere decir que el archivo firmado es válido y puede ser aceptado.

Fig 17. Verificación de un archivo firmado



5. RESULTADOS

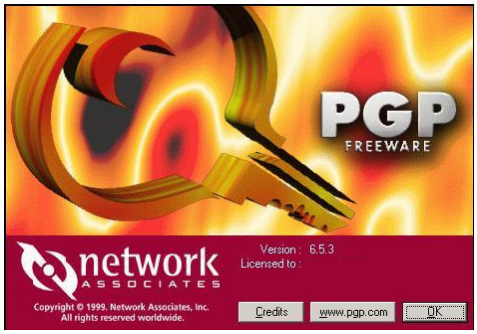
En el capítulo anterior se definieron conceptos teóricos de Lattice y sus problemas relacionados, finalizando con la explicación del esquema de firma digital propuesto (basado en Lattice). En el presente capítulo se realiza una comparación entre los software PGP 6.5.3 y el prototipo de "Firma Digital con Lattice" que aplica el esquema de firma planteado en el capitulo anterior. Se comienza con una breve reseña de PGP, luego se exponen paralelamente los procesos de generación de claves, firma y verificación de archivos, concluyendo con un análisis de resultados obtenidos de la comparación de las aplicaciones probadas.

5.1. VALIDACIÓN SOFTWARE PGP Vs FIRMA DIGITAL CON LATTICE

5.1.1. Reseña del PGP (Pretty Good Privacy)

Es un programa de cifrado de datos que incluye múltiples funciones de seguridad y de gestión de claves.

Fig 18. Software PGP



PGP fue creado por Phillip Zimmermann como un medio que permitiera a una persona protegerse de la inseguridad del correo electrónico. En un principio generó gran controversia, debido a diversos problemas legales, lo cual contribuyó a aumentar su popularidad y extender su uso a nivel internacional. Actualmente el uso de PGP es completamente legal, a excepción de algunos estados con regímenes totalitarios en los que el uso de criptografía está perseguido y en países como Francia que cuenta con leyes muy restrictivas sobre este tema.

Hasta principios de 2001 la política de distribución de PGP se fundamentaba en permitir su uso gratuito para fines no comerciales y en publicar su código fuente; en febrero de 2001, luego del abandono de la empresa por parte de Zimmerman (su creador) dejó de publicarse.

Actualmente PGP se ha convertido en un estándar internacional, lo cual ha dado lugar a la aparición de múltiples productos PGP que brindan facilidades, desde el cifrado de correo electrónico hasta la codificación de particiones enteras del disco duro (PGPDisk), pasando por la codificación automática y transparente de todo el tráfico TCP/IP (PGPnet).

5.1.1.1. Funcionamiento

PGP funciona con criptografía asimétrica permitiendo una gran facilidad al usuario a la hora de gestionar sus claves públicas y privadas.

El empleo de algoritmos asimétricos obliga a poseer las claves públicas de todos sus interlocutores, además de la clave privada propia. PGP facilita el manejo de

clave por medio de un concepto de anillo (o llavero), que es el lugar para que el usuario guarde todas las claves que posee; es un único archivo en el que se pueden efectuar operaciones de extracción e inserción de claves de manera sencilla, además proporciona un mecanismo de identificación y autentificación.

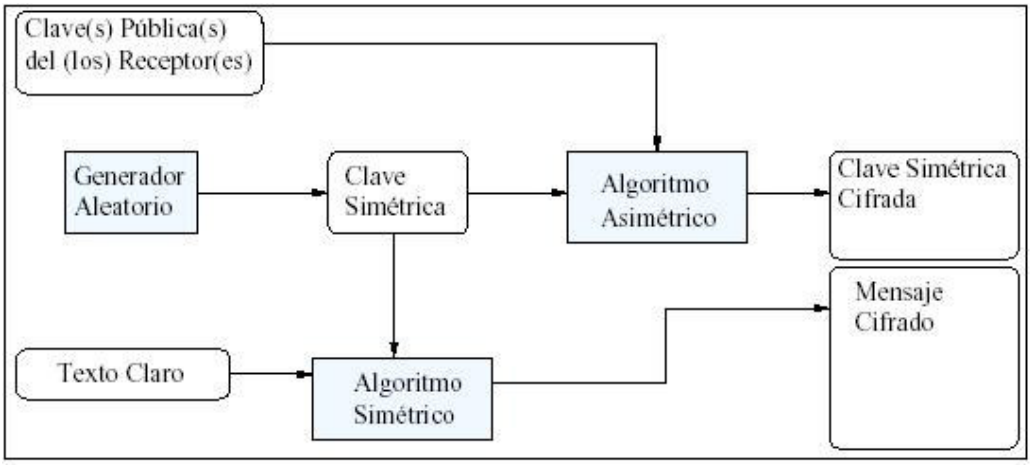
La familia de versiones 2.x.x fue la que alcanzó una mayor popularidad, y sigue siendo utilizada por muchas personas actualmente. Los PGP 2.x.x emplean únicamente los algoritmos IDEA, RSA y MD5.

Uso

Los algoritmos simétricos de cifrado son más rápidos que los asimétricos. Por esta razón, PGP cifra primero el mensaje empleando un algoritmo simétrico con una clave generada aleatoriamente (clave de sesión) y luego cifra la clave haciendo uso de la llave pública del destinatario, la cual es extraída del anillo de claves públicas a partir del identificador suministrado por el usuario; todo esto es transparente, sólo se debe indicar el mensaje a codificar y la lista de identificadores de los destinatarios.

Para descifrar el mensaje, PGP busca en la cabecera las claves públicas con las que está cifrado y pide una contraseña que servirá para abrir el anillo de claves privadas y comprobar si se tiene una clave que permita recuperar el mensaje. Siempre que se quiera hacer uso de una clave privada se debe suministrar la contraseña correspondiente, lo que permite asegurar que aún si el anillo de claves privadas quedara comprometido, un atacante tendría que averiguar la contraseña para descifrar los mensajes.

Fig 19[22]. Codificación de un mensaje PGP



La mayor parte de la seguridad de PGP descansa en la calidad del generador aleatorio que se emplea para calcular las claves de sesión; si alguien logra predecir la secuencia de claves que se usan, podrá descifrar todos los mensajes independientemente de los destinatarios a los que vayan dirigidos. Por esta razón, PGP protege mediante criptografía la semilla que necesita para la generación de números seudoaleatorios. Se considera sensible al archivo que contiene dicha semilla, y por lo tanto se recomienda evitar que quede expuesto.

5.1.1.2. Firma Digital

PGP obtienen en primer lugar el resumen MD5 o SHA-1, que posteriormente se cifra empleando la clave privada RSA o DSA.

[22] Tomado de **[LUC00]**, página 173.

La firma digital puede ser añadida al archivo (firma con mensaje recuperable) u obtenida en otro aparte (firma con apéndice).

5.1.1.3. Gestión de Claves

PGP almacena las claves en unas estructuras denominadas anillos, cada usuario tendrá dos, uno para las claves públicas (PUBRING.PKR) y otro para las privadas (SECRING.SKR). Cada una de las claves, además de la secuencia binaria del algoritmo que se emplee, poseen un identificador del usuario que la emitió, la fecha de expiración, la versión de PGP con que fue generada y la huella digital (resumen, hash).

La huella digital es bastante útil, se trata de una secuencia hexadecimal lo bastante larga como para que sea única (o difícil de encontrar una igual), y lo suficientemente corta como para que pueda ser escrita en un papel. Un ejemplo es:

9E2B 9D14 CBCE FE12 16A8 C103 48B2 5161 69AB 5784

Para verificar la autenticidad de una clave basta con llamar al autor y pedirle que lea el valor de la huella digital (resumen) de su clave.

Cuando una clave queda comprometida puede ser revocada por su autor. Este proceso requiere generar y distribuir un certificado de revocación que informará a todos los usuarios la invalidez de esa clave. Para generarlo se necesita la clave privada, por lo que en muchos casos se recomienda generar con cada clave su certificado de revocación y guardarlo en lugar seguro, de tal forma que si se olvida o pierde la clave privada se pueda revocar. Las últimas versiones de PGP

permiten nombrar revocadores de claves, que son usuarios capaces de invalidar a un usuario sin hacer uso de su llave privada.

El uso inadecuado de PGP puede convertirlo en una protección inútil.

5.1.2. Generación de Claves

Este proceso es fundamental en cualquier Criptosistema de clave pública, consiste en generar una clave pública y una privada a partir del problema matemático sobre el cual descansa su seguridad.

5.1.2.1. PGP

Permite generar firmas digitales mediante el esquema RSA y DSS, para lo cual utiliza números primos y logaritmo discreto respectivamente. Las claves generadas tienen una estructura similar que permite exportarlas al correo electrónico y otras aplicaciones que puedan validar su contenido.

Fig 20. Ejemplo de clave pública con PGP

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGPfreeware 6.5.3 for non-commercial use <http://www.pgp.com>

mQENA0RVOv4AAAEIANz3RA3a48LbFjcUIpDRg9wLN6Oo6Bvi/umcvpSRNvA/lei+Z
BX/1M8TtG4HS+S5HvNXPr3nDMjjUCB8aNd7SSWgNgPkkDGZ+Pgh13Uk7xw37JFOB
SYaCB/EYQVRsdF64dsxWhpnASZFJjUTg8iP2uE68eOB/Im+Bt+aWpvZaxwxxLZG7BR
jc6b7q6U79XTWC8ELI27Eg50Rgm2hLb77fl2yPRckwcwYu8ps1DwTbKbXnsTGrMm/F
Cx6Zoxz5TTzhHbo5uNa4UKOFn4/x4XwRZ9TtjXsFUizwGr2JpUyyDWlR66oir9W4zJq
maYkTK6CdOopCQcttmzcDU8EE9pGnUABRG0Hmp1YW5HYWJyaWVsIDxqdWFuQ
GhvdG1haWwuY29tPokBFQMFEERVOv5wNTwQT2kadQEBcCgIAMvO/V9wQIdbkEq
oJSvtyFFkM8bBTRpHnxZsg182UCBP2z3wb2dAj43CB1ChENHS6arz58XBnMgBRPcA+
aSc1Vxlj7QxDASVJ6nie5iuOHjFwisvL3UpmG041lMwkBB9UKk6g0f82PB8KBhsxCIbi3
RU8AYrTbY0PUVa4IXTCy9D0QbkXxOqVFMOUHuPgvegOneSEc9z90kYGf/+Z10qK
CnPFv5+sitJBGpbnRogExgbsUfnqEKkZmw8K6XbnRi8eS2rPPraXyS9FezKcv2zC4TSU5
jsd7UEOGRMT/dMmymTIBt5up2pD80IBiy9MIozRNPsQu2uR8yQbdEUJAHxMQKM=
=/6v0
-----END PGP PUBLIC KEY BLOCK-----
```

Paso 1

El proceso para la generación de claves comienza con el suministro del nombre completo (full name) y el correo electrónico (e-mail) por parte del usuario. No es necesario que la dirección de correo sea la real, pero se recomienda que lo sea para que los que se quieran comunicar sepan que la clave es real y pertenece a esa dirección de e-mail.

Fig. 21. Generación de claves con PGP. Paso 1

Paso 2

Se debe elegir el tipo de cifrado que se utilizará. Las opciones son Diffie y Hellman junto con la Digital Signature Standard (representado como DH/DSS) y el RSA. Dependiendo del tipo de elección la seguridad descansará en el problema del logaritmo discreto o en la factorización de números primos.

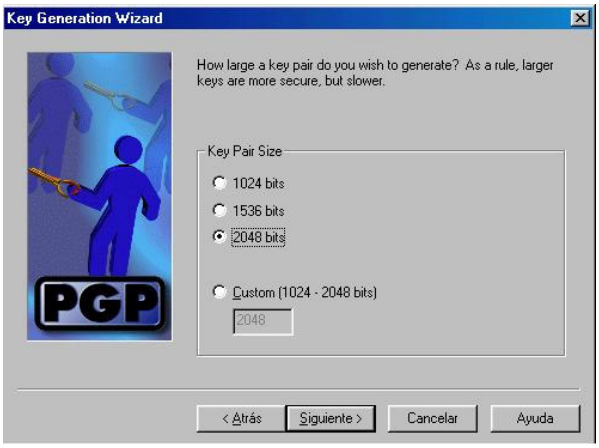
Fig 22. Generación de claves con PGP. Paso 2

Paso 3

Se debe elegir el tamaño de las claves a generar (pública y privada). Si se escogen claves de longitud distinta a los valores que se proponen, el tiempo

necesario para generarlas es mucho mayor. Se recomienda usar una clave de 2.048 bits.

Fig 23. Generación de claves con PGP. Paso 3



Paso 4

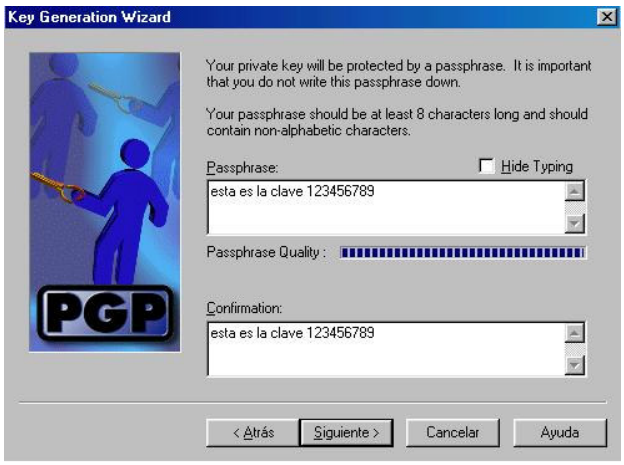
El usuario tiene la opción de escoger si las claves generadas expiran o no.

Fig. 24. Generación de claves con PGP. Paso 4

Paso 5

Debido a las grandes longitudes de las claves, el usuario debe definir una frase secreta para cifrar su clave privada con el resumen de ésta y guardarla en el anillo de claves, de tal forma que cuando se quiera firmar o verificar un documento sólo se digite la frase secreta, se calcule su resumen y se descifre su clave privada. La inclusión de criptografía simétrica se hace para fortalecer la seguridad, sino se utilizará el sistema quedaría en manos del usuario, quien debería proteger su archivo de clave privada.

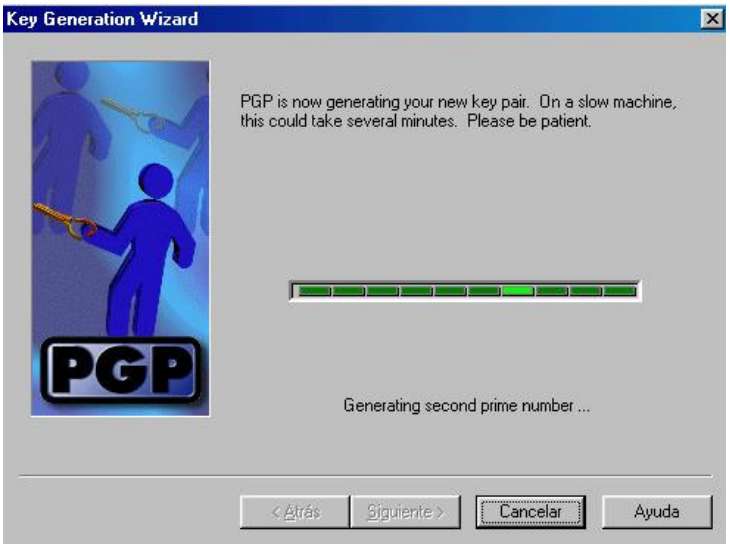
Fig. 25. Generación de claves con PGP. Paso 5



Paso 6

Se generan las claves y se almacenan en el anillo definido por el usuario. Toda clave después de creada se puede exportar a un archivo plano para facilitar la portabilidad entre aplicaciones.

Fig. 26. Generación de claves con PGP. Paso 6



Paso 7

Se tiene la opción de publicar en un servidor de claves, la llave pública mediante el envío de la misma con sólo seleccionar la caja de chequeo.

Fig. 27. Generación de claves con PGP. Paso 7

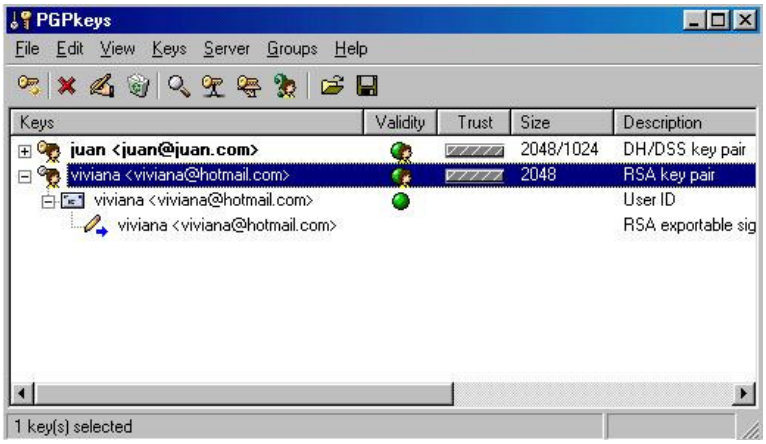
Paso 8

Se muestra el resultado final del proceso.

Fig. 28. Generación de claves con PGP. Paso 8

En **Fig.** 29 aparece el visor de claves de PGP donde se muestran los usuarios registrados con su respectiva información.

Fig 29. Visor de Claves PGP



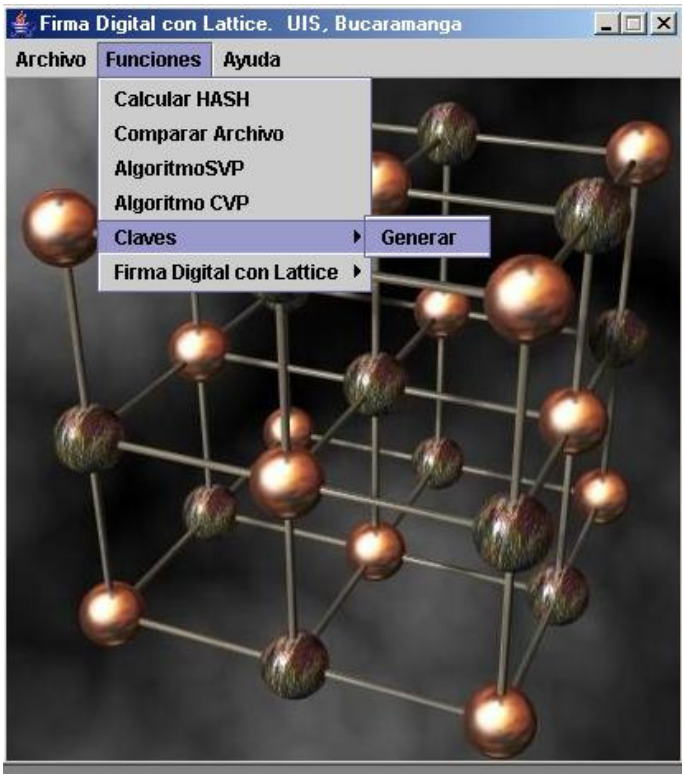
5.1.2.2. Lattice

La generación de las claves con Lattice consiste en la creación de dos archivos (*.lat) que contienen las bases del Lattice privado y el público, los cuales se almacenan en la ruta especificada por el usuario, siendo responsabilidad de éste su manejo y protección.

Paso 1

Se debe ejecutar la aplicación “Firma Digital con Lattice”. Ir al menú Funciones, submenú Claves y seleccionar la opción Generar. Esta secuencia de pasos invoca al programa encargado de generar las bases del Lattice.

Fig 30. Firma digital con Lattice. Opción generar Claves



Paso 2

El proceso de generación de las bases de los Lattices se hace según se explicó en el Capitulo 4. Para el usuario toda la complejidad se convierte en transparente, sólo debe elegir el "Tamaño de la Lattice" a partir de una lista (de 2 a 40), el "Directorio Destino" que será ruta donde se guarden los archivos generados y el "Nombre de Clave Privada" y "Nombre de la Clave Pública" sin ninguna extensión; el programa al momento de crear les coloca la extensión lat.

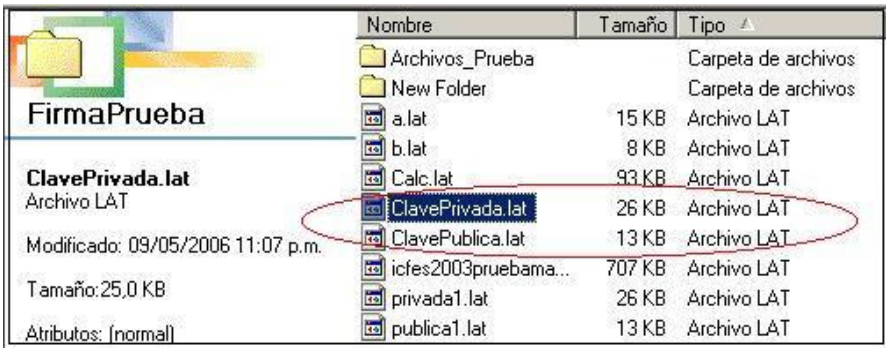
Fig 31. Generación de Claves

Paso 3

Se genera un mensaje de éxito en el proceso de generación de claves. Como resultado se crean dos archivos en el directorio destino como se muestra en **Fig** 33.

Fig 32. Resultado de la generación de Claves

Fig 33. Resultado de la generación de Claves



5.1.3. Firma digital

Al momento de realizar la firma el usuario debe conocer la clave pública del receptor del mensaje.

La firma digital en PGP se realiza siguiendo los pasos:

Paso 1

Se debe seleccionar la opción PGPtools para visualizar la barra de herramientas, en la cual se puede seleccionar la acción a realizar entre las que se encuentran Encrypt Sign, PGPKeys, Encrypt, Sign, Decrypt/Verify.

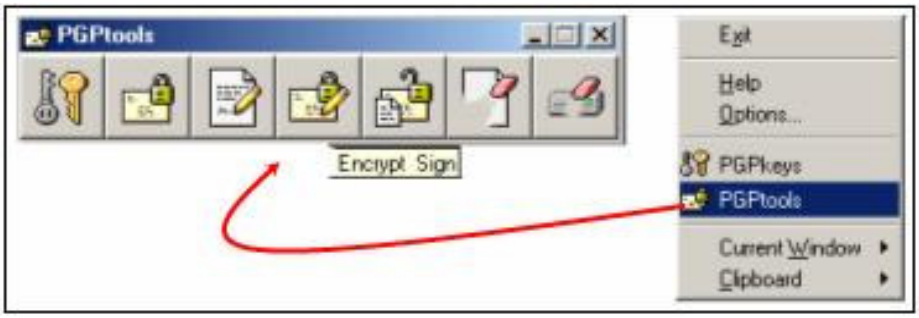
Dependiendo del tipo de firma que se quiera realizar se debe escoger en la barra de herramientas:

✓ Encrypt Sign. Realizar la firma digital con mensaje recuperable.

✓ Sign. Firma digital con apéndice.

El tipo de firma a utilizar (RSA, DSS) depende de la clave seleccionada para el proceso de cifra.

Fig 34. Barra de herramientas de PGP



Paso 2

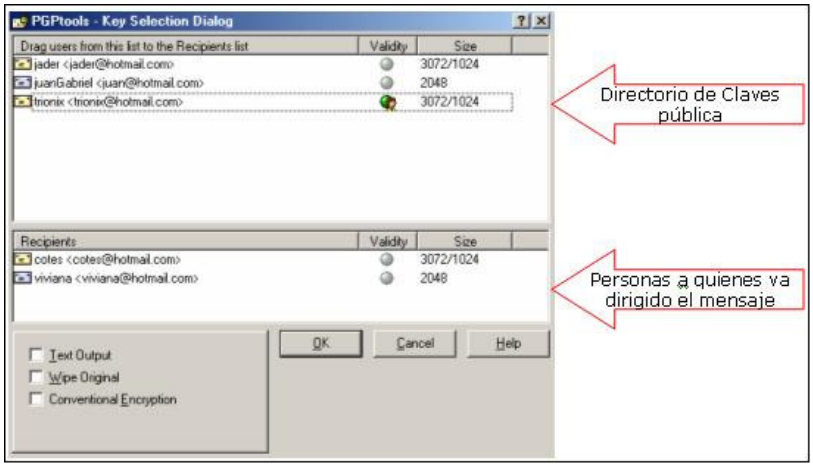
Seleccionar el archivo a procesar como se muestra en **Fig** 35.

Fig 35.Selección de archivo a cifrar y firmas

Paso 3

Se deben seleccionar los usuarios destinatarios del mensaje a firmar; se puede escoger uno o todos dependiendo del alcance que se quiera dar.

Fig 36.Selección de los destinatarios del mensaje a firmar



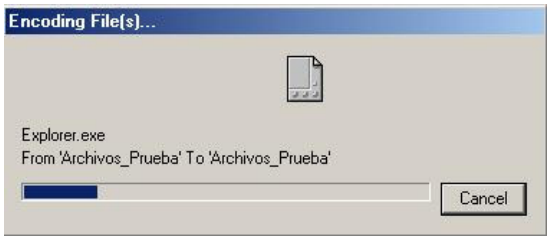
Paso 4

Se solicita la clave de sesión del firmante para verificar su identidad, en caso de no ser válida el proceso quedará nulo.

Fig 37.Confirmación de la identidad del usuario firmante

Luego de realizados los pasos anteriores de manera satisfactoria, se obtiene un archivo firmado y cifrado, almacenado en la misma carpeta del archivo de origen.

Fig 38.Proceso de cifrado del archivo con PGP



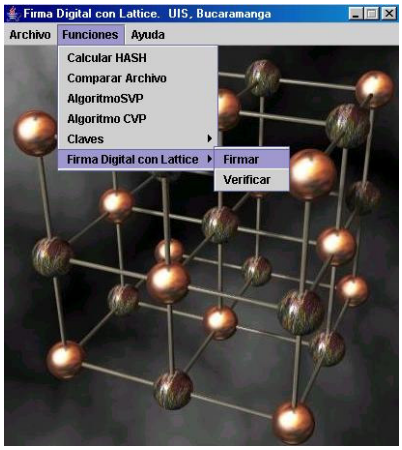
5.1.3.1. Lattice

La firma digital con Lattice se realiza mediante los siguientes pasos:

Paso 1

Con el programa "Firma Digital con Lattice" en ejecución, se debe ir al Menú Funciones, submenú Generar Firma con Lattice y seleccionar Firmar.

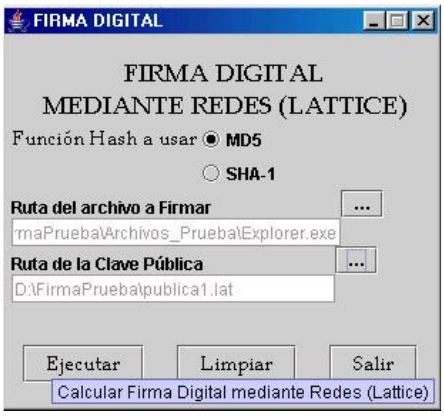
Fig 39. Selección de la opción Firmar (Firma Digital con Lattice)



Paso 2

Se escoge la función Hash a utilizar, el archivo a Firmar y la Ruta de la Clave Pública.

Fig 40. Elección del tipo opciones de Firma Digital con Lattice



Al dar clic en ejecutar se procede a la firma, generando como resultado un archivo firmado con Lattice (*.lat). El proceso finaliza con el mensaje mostrado en **Fig** 41.

Fig 41. Mensaje de finalización Firma con Lattice exitosa

5.1.4. Verificación de la Firma Digital

Requiere que el usuario ingrese la clave que valide la firma aplicada al mensaje.

5.1.4.1. PGP

La verificación de la firma se realiza mediante la siguiente secuencia de pasos:

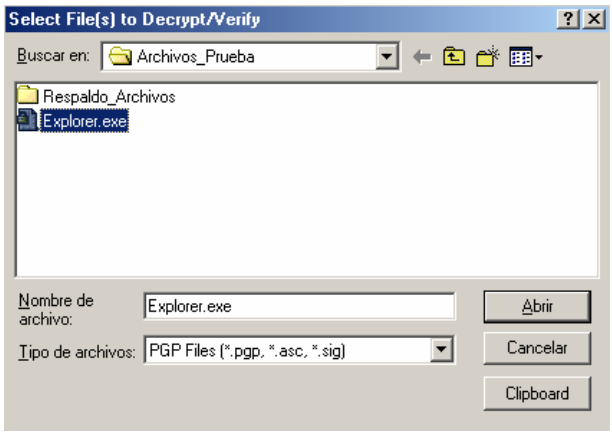
Paso 1

Se debe seleccionar el archivo firmado, lo cual se puede realizar haciendo clic sobre él o seleccionando la opción en la barra de herramienta Decrypt/Verify.

Fig 42.Selección del proceso Decrypt/Verify

En caso de acceder mediante la barra de herramientas es necesario seleccionar el archivo objetivo con la ayuda de la ventana de exploración que se muestra en **Fig.** 43.

Fig. 43.Selección del archivo firmado



Paso 2

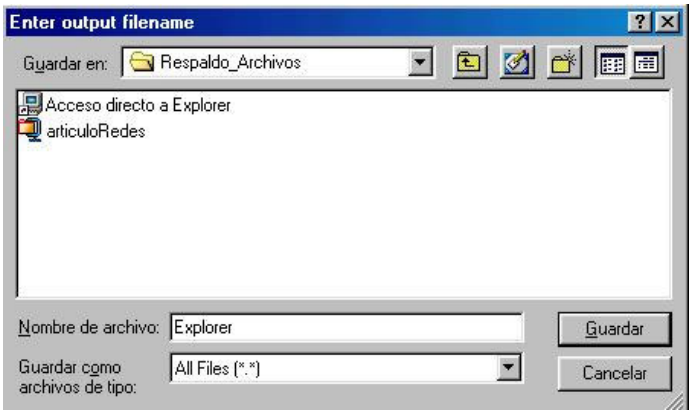
Escribir la clave de sesión del usuario receptor del mensaje, la cual debe corresponder a alguno de los usuarios que aparecen como posibles receptores.

Fig. 44. Selección del usuario receptor del mensaje

Paso 3

Se escoge la ruta y el nombre del archivo de salida que se va a recuperar. El programa por defecto coloca el nombre original y la ruta donde se encuentra el archivo firmado.

Fig. 45. Selección de la ruta y nombre del archivo obtenido con PGP



Luego de esta secuencia de pasos, en caso de resultar satisfactoria, se obtiene el mensaje original que se encontraba firmado.

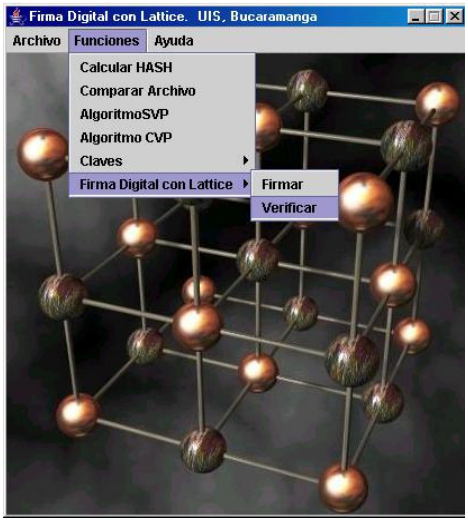
5.1.4.2. Lattice

La verificación de un archivo firmado con Lattice se mediante los siguientes pasos:

Paso 1

Con el programa “Firma Digital con Lattice” en ejecución, se debe ir al Menú Funciones, submenú Generar Firma con Lattice y seleccionar Verificar.

Fig 46. Selección de la opción Verificar (Firma Digital con Lattice)



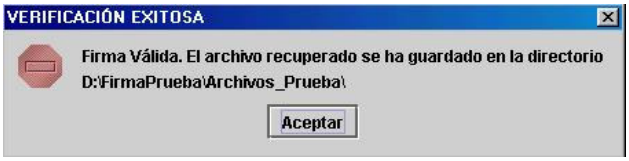
Paso 2

Se debe seleccionar la ruta del archivo firmado, la ruta de la clave privada y la de pública, y dar clic en ejecutar.

Luego de realizado este proceso se retorna el resultado de firma exitosa o firma inválida, dependiendo de la validación de las claves y el archivo firmado. En el caso que la firma se exitosa, como se muestra la **Fig** 48, el archivo obtenido se guarda en la misma ruta que el firmado.

Fig 47. Opciones de Verificar Firma Digital mediante Lattice

Fig 48. Resultado de firma digital mediante Lattice válida



5.2. ANÁLISIS DE RESULTADOS

Luego de realizar varias pruebas de firma digital y verificación de archivos, se obtuvo la **Tabla 1**. Se aprecia que la firma digital con Lattice, a pesar probarse sobre un prototipo, tiene buenos tiempos de cómputo frente a otras alternativas como lo es PGP.

La ventaja más notoria en tiempo de computo la proporcionan los Lattices en el proceso de firmado para archivos grandes, donde aventaja en gran medida a la firma con RSA y DSS de PGP. Para archivos pequeños (menos de 600 Kb) los

Lattices funcionan más rápido que PGP debido al preprocesamiento que requiere éste para firmar un archivo (aplicación de compresión con zip).

La verificación de la firma con Lattice en archivos de gran tamaño se hace más lento que el proceso PGP debido a las operaciones con las bases (matrices) que se deben realizar, lo cual acarrea un alto tiempo de cómputo.

El prototipo software tiene ciertas limitaciones como son:

✓ **Tamaño del Lattice (Rango)**

Esta limitación se debe al tipo de dato del lenguaje en el cual se implementó el programa (double de 64 bits en Java), el cual al ser requerido en operaciones entre bases (matrices) del Lattice de grandes dimensiones (mayor que 40) se produce desbordamiento, impidiendo la verificación de la firma aplicada.

Aún con esta limitación, se ve que la Firma con Lattice se puede trabajar en cualquier dimensión siempre y cuando se cuente con un tipo de dato que soporte un almacenamiento de números de gran tamaño sin perdida.

✓ **Tamaño del archivo a cifrar**

Por ser implementado a manera de prototipo, el manejo de archivo en la aplicación "Firma Digital con Lattice" esta limitado en tamaño al trabajar los archivos en vectores de tipo Byte que proporciona el lenguaje de programación (Java).

El tamaño máximo del archivo que se puede firmar para garantizar que la firma digital y la verificación será satisfactoria es de 30 Mb.

Para eliminar esta limitación se debe cambiar la forma de manejar los archivos utilizando algún tipo de objeto que proporcione el lenguaje.

Debido a que el objetivo de este trabajo es mostrar la aplicación del concepto matemático del problema de reducción de Lattice SVP[3] y CVP[4] a la firma digital, el prototipo fue implementado para probar la validez del esquema de firma planteado asumiendo las limitaciones antes descritas, dejando abierta la posibilidad de ser superadas en futuros trabajos de investigación.

Tabla 1. Comparación de PGP frente a Firma con Lattice

Nombre del archivo	Tamaño Kb	PGP		Lattice	
		Tiempo de Firma (seg)	Tiempo de Verificación (seg)	Tiempo de Firma (seg)	Tiempo de Verificación (seg)
Instalador de Dreamweaver 4.exe	25.239	84	36	20	43
Sybex.Complete.Java.2.pdf	9.942	52	16	50	17
TesisLattice23Mayo2006.doc	1.855	7	4	5	6
articuloRedes.rar	576	4	2	2	1.5
EXPLORER.exe	176	5	4	1	1

6. CONCLUSIONES Y RECOMENDACIONES

6.1. CONCLUSIONES

La legislación no le da peso al concepto de firma digital ni a sus alcances, lo cual puede hacer que los usuarios no confíen en esta tecnología. Además, en muchos países la legislación acerca de este tema es poca y no existe uniformidad de las leyes, debido a que sus contenidos varían de un país a otro, lo cual dificulta su aplicación en un entorno global como Internet.

Un aspecto crítico en la firma digital es la garantía de ser firmado por quien dice haberlo hecho, evitando la posibilidad de repudio por su parte. También se debe tener la seguridad que lo que ha sido firmado sea lo que se quería avalar, es decir, que se mantenga la integridad.

Dependiendo de las necesidades de la organización se deben escoger los modelos de seguridad, sin olvidar que el desarrollo de la cultura organizacional en seguridad es un proceso continuo, debido a la gran rotación que presenta el mercado. En caso que no se de este proceso, puede llegar a quedar rápidamente obsoleto o ser desconocido por las nuevas personas que ingresan a la organización.

Un factor importante que caracteriza los criptosistemas de clave pública es su alto nivel de “seguridad”. Los nuevos criptosistemas basan su seguridad en la complejidad computacional de algún problema matemático que desde el punto de vista teórico tiene solución pero en la práctica es “muy difícil” de resolver.

Los Lattices presentan una serie de propiedades que dan lugar a problemas computacionalmente “difíciles”, característica que los hace aplicable a la criptografía. El planteamiento de un esquema de firma digital basado en Lattice descansa en los problemas del vector más corto y el vector más cercano, los cuales presentan un grado de complejidad de cálculo alto al aumentar la dimensión del Lattice sobre la cual se trabaja.

El tiempo de cómputo que requiere un esquema de firma con Lattice para archivos pequeños (menos de 600 Kb) es bajo en comparación con alternativas como las firmas con RSA y DSS implementadas por PGP. Para archivos de gran tamaño (cerca de 30 Mb) el proceso de firma es más rápido que los requeridos por esquemas firma con RSA y DSS, aunque el proceso de verificación es lento debido a las operaciones que se requieren entre las bases (matrices) de los Lattices a fin de recuperar los vectores almacenados y aproximar los problemas del vector más corto y el más cercano.

Aunque los problemas de reducción de Lattice del vector más corto y el más cercano presentan complejidad computacional que les hace aplicables a la criptografía, no tiene igual acogida. El problema del vector más cercano es el más aplicado debido a la complejidad que implica su aproximación, además, el problema del vector más corto es un caso particular del más cercano cuando el vector objetivo es el cero.

6.2. RECOMENDACIONES

Debido a la evolución de los computadores y a la creación de nuevos algoritmos que resuelven algunos problemas matemáticos, que antes parecían imposibles o requerían muchos recursos, se recomienda seguir en la búsqueda de nuevas estructuras matemáticas que aumenten la complejidad del problema en el cual

descansa la seguridad de los criptosistemas y que amplíen su espacio de claves para impedir posibles ataques.

Los Lattices tienen muchos problemas asociados que permiten plantear criptosistemas, en este trabajo se estudiaron el problema del vector más corto y el del vector más cercano. Quedan aún problemas como el de la base más pequeña que podría ser interesante de aplicar para un cifrado de clave pública.

Al momento de escoger e implementar en un lenguaje de programación un criptosistemas se debe en cuenta características del lenguaje como tamaño de los tipos de datos, soporte de programación orientada a objetos, portabilidad y escalabilidad. En caso que los datos manejados sean muy grandes, se recomienda trabajar con tipos de datos definidos por el usuario, con la particularidad que se deben definir todas las operaciones (suma, resta, potenciación, entre otras) que afectan las variables definidas.

Se recomienda tener en cuenta el aporte realizado en este proyecto para futuros trabajos, ya sean de mejora a lo realizado o estudio de problemas no considerados.

BIBLIOGRAFÍA

[AJT97] AJTAI, Miklos and Dwork, Cynthia. A public key cryptosystem with worst case/average case equivalente. ACM Symposium on theory of computing. 1997.

[AND88] ANDREASSEN, Kart. Computer Criptology, Beyond decoder rings. Editorial Prentice. New Jersey. 1988. 268 p.

[ANG99] ANGEL, José de Jesús, Criptografía para principiantes Seguridad Data. 1999.

[BAB86] BABAI, L. On Lovász lattice reduction and the nearest lattice point problem. *In Combinatorica*, vol. 6, 1986, pp. 1-13.

[CEB00] CEBALLOS, Francisco. Java 2 Curso de Programación. Editorial Alfaomega Ra_ma. Mexico DF. 2000

[DWO98] DWORK, Cynthia. Lattices and Their Application to Cryptography, Stanford University, Spring Quatre. 1998.

[FIS00] FISCHLIN, Roger and SEIFERT, Jean Pierre. Tensor based trapdoors for CVP and their application to public key cryptography. Goethe university at Frankfurt, Germany, 2000.

[GOL99] GOLDREICH, Oded, Weizmann Institute of Science, ISRAEL, GOLDWASSER Shafi, HALEVI Shai, MIT, Laboratory for computer science, Public key cryptosystems from lattice reduction problems. 1997.

[JAC00] JACOBSON, Ivar, BOOCH, Grady and RUMBAUGH, James. El Lenguaje Unificado de Modelado. Ed. Addison Wesley. Madrid. 2000

[HCW80] H.C. Williams, A Modification of the RSA public-key encryption procedure, IEEE Transaction on Information Theory, No 26, pp 726-729 1980.

[LEN82] LENSTRA, H.W and LOV´ASZ, L.. Factoring polynomials with rational coefficients. *Mathematische Annalen* 261, 515-534 (1982).

[LUC00] LUCENA, Manuel José. Criptografía y seguridad de computadores. Segunda Edición. España, 1999.

[MEN97] MENEZES, Alfred, OURSCHOT, Paul and VANSTONE, Scout. Handbook of applied cryptography. Editorial CRC Press LLC. Boca Raton. 1997. 780 p.

[MIC99] MICCIANO, Daniele. Lattices in cryptography and cryptoanalisys. University of California. San Diego, 1999.

[MIC02] _____ and GOLDWASSER, Shafi. *Complexity of Lattice Problems: a Cryptographic Perspective*, volume 671 of *The Kluwer International Series in Engineering and Computer Science*. Kluwer Academic Publishers, Boston, Massachusetts, Mar. 2002.

[NASH02] NASH, Andrew, DUANE, William, JOSEPH, Celia and BRINK, Derek. PKI Infraestructura de claves públicas. Editorial McGraw-Hill. Bogota. 2002

[PFL89] PFLEEGER, Charles P. Security in computing. Editorial Prentice. 1989. 538 p.

[PIN97] PINO, Gil. Seguridad Informática: Técnicas Criptográficas. Editorial Alfaomega. México. 1997. 137 p.

[PRES93] PRESSMAN, Roger. Ingenieria del software, un enfoque practico. Editorial McGraw – Hill. Tercera Edicion. Mexico. 1993

[RAM05] RAMIÓ AGUIRRE, Jorge. Libro digital de Seguridad Informática y Criptografía. Madrid España 2005.

[SCH96] SCHNEIER, Bruce. Applied Cryptography : Protocols, algorithms and Source code in C. Editorial John Wiley. New York. 1996. 758 p.

[SEB89] SEBERRY, Jennifer and PIEPRZYK, Josef. Cryptography: An introduction to computer security. Editorial Prentice Hall. New York. 1989

[3W1] www.azom.com/details.asp?ArticleID=2123

ANEXOS

ANEXO 1. EQUIPO REQUERIDO

Para el buen funcionamiento del prototipo “Firma Digital con Lattice” y “PGP 6.5.3” se recomienda un equipo que cuente mínimo con las siguientes características:

Procesador Intel Pentium II 200 Mhz
128 Mb de memoria RAM
20 Gb en disco duro
Unidad de CD-ROM de 52X
Unidad de discos de 3 ½”

El software que se requiere instalado para la ejecución de las aplicaciones:

Microsoft Windows
JRE (Java Runtime Environment) 1.4.2 o superior
PGP 6.5.3 (Para la ejecución de PGP)

Todas las características descritas anteriormente con mínimas. Si el usuario cuenta con mejores condiciones, los programas tendrán un desempeño superior sin llegar en ningún momento a presentar incompatibilidades.