Nombre del alumno:

Ignacio Ivan Sanchez Pantoja

Número de matrícula:

18108365

Nombre del profesor:

Israel Alejandro Herrera Araiza

Nombre del curso:

Controles Criptograficos De Seguridad

Actividad:

Fase 1 Actividad de clase Cifrados clásicos y RSA.

Fecha:

24/05/2024

Introduccion:

En el ámbito de la criptografía, los algoritmos simétricos y asimétricos desempeñan un papel crucial en la seguridad de las comunicaciones. Los algoritmos simétricos, como AES y Triple DES, son eficaces para la comunicación de 1 a 1 debido a su eficiencia en el cifrado y descifrado de datos. Sin embargo, presentan un reto significativo: la distribución segura de las claves. La seguridad de estos métodos depende en gran medida del proceso de intercambio de claves, lo que resalta la importancia de los protocolos criptográficos para garantizar un transporte seguro.

Por otro lado, los algoritmos asimétricos, como RSA, ofrecen una solución al problema de la distribución de claves mediante el uso de un par de claves públicas y privadas. RSA, a pesar de su longevidad, sigue siendo fundamental en la criptografía moderna debido a su robustez y versatilidad. Sin embargo, su seguridad depende de prácticas rigurosas y su capacidad de adaptación a posibles avances como la computación cuántica. Además, es esencial una implementación correcta para evitar vulnerabilidades derivadas de la relación entre el mensaje y el criptograma, donde la aleatorización y el uso de padding son vitales.

Otro avance destacado es el uso de las curvas elípticas, que ofrecen una seguridad comparable a RSA pero con claves de menor tamaño, haciéndolas eficientes y seguras. Las curvas elípticas se basan en operaciones complejas y problemas matemáticos difíciles de resolver, como el problema del logaritmo discreto, proporcionando una alternativa moderna y eficiente en la criptografía.

Finalmente, los protocolos como Diffie-Hellman permiten un intercambio seguro de claves sobre canales inseguros, facilitando la creación de claves compartidas sin la necesidad de que las partes se conozcan previamente. Este protocolo, junto con las mejoras que implican las curvas elípticas, subraya la continua evolución y adaptación de los métodos criptográficos para enfrentar las necesidades de seguridad en un mundo digital cada vez más interconectado.

Algoritmos simetricos

son útiles para métodos de comunicación 1 a 1 pero el problema es el traslado de las claves, la principal limitación de estos métodos de cifrado es el traslado de forma segura de estas claves, la seguridad siempre dependerá de la forma en la cual se realizo el proceso de intercambio de claves, en ese punto radica la importancia de los protocolos de comunicación criptográficas, los algoritmos mas comunes empleados en este apartado son AES y triple DES, el primer algoritmo de clave simétrica que se creó a lo largo de la historia fue el algoritmo de venam one time pad, sin embargo este algoritmo involucraba más inconvenientes que los actuales algoritmos simétricos, primero porque la calve debe de ser del mismo tamaño que el mensaje a cifrar, además al momento de realizar una comunicación por cada mensaje cifrado se debe seguir un proceso de intercambio de clave para poder realizar el envió de esta información en muchos documentos el paradigma o los algoritmos asimétricos constituyen una pieza necesaria para poder distribuir las

contraseñas empleadas por los algoritmos simétricos que pese a ser mas eficientes tienen este defecto.

El cifrado RSA a pesar de tener 47 años desde su invención sigue siendo un pilar fundamental en la criptografía moderna debido a su robustez y versatilidad. Sin embargo, su seguridad depende de implementaciones adecuadas y prácticas rigurosas de manejo de claves, especialmente en un entorno donde los ataques son cada vez más sofisticados. El futuro de RSA está marcado por su adaptación frente a posibles avances en computación cuántica que podrían cambiar el paradigma de la criptografía actual, sin embargo hasta ese momento se deberá de considerar el cambiar de criptosistema, si bien el cifrado RSA es seguro es necesario contar con personal capacitado para implementar de forma segura estos algoritmos en los sistemas seguros, al ser RSA un criptosistema asimétrico es decir que (utilizando claves públicas y privadas para el cifrado y la firma digital) como se describió en las actividades de clase, este cifrado basa su funcionamiento en la complejidad de factorización de números primos requiriendo la necesidad de tener 2 números primos para generar las claves públicas o privadas, como expone Galbraith que RSA utiliza el problema de trapdoor one-way permutation, en palabras simples "son funciones que son fáciles de calcular en una dirección, pero difíciles de invertir sin una clave secreta. Son fundamentales en la criptografía de clave pública y en la generación de firmas digitales seguras."(Galbraith, S. D. (2012)), Galbraith al momento de definir el cifrado RSA menciona que hay múltiples consideraciones al momento de implementar RSA, consideraciones que contemplan a su vez múltiples ataques a los criptosistemas, mencionado que un criptosistema que se considera seguro teóricamente convirtiéndose en un estándar criptográfico obtiene la denominación **IND-CCA, este término denota que un criptosistema debe ser seguro ante cualquier ataque del mundo real**.

Ahora bien los principales ataques que todo criptosistema debe de enfrentar son:

Ataques Criptográficos Directos:

- **Ataques de Mensaje Elegido (Chosen Ciphertext Attack, CCA)**: Permiten a un atacante elegir un texto cifrado y obtener su descifrado. Sin medidas de padding adecuado, como OAEP, estos ataques pueden comprometer la seguridad de RSA.
- **Ataques de Texto Plano Elegido (Chosen Plaintext Attack, CPA)**: El atacante puede cifrar mensajes de su elección y utilizar los resultados para intentar descifrar otros mensajes cifrados con la misma clave pública.

Las vulnerabilidades de RSA al mencionar que radican en la implementación nos referimos al hecho de que es necesario forzosamente que el mensaje a cifrar supere en tamaño a la clave utilizada es decir que de alguna forma se aplique un periodo criptográfico, esto es porque suele haber una relación entre el mensaje y el criptograma y esta relación para poder ser destruida es necesario aplicar mecanismos de tanto generación de paddings es decir generación de bytes "basura" con el fin de agrandar el mensaje para destruir la relación anteriormente citada, además de ser necesario aleatorizar el proceso de cifra de los datos, al ser RSA un algoritmo determinista (es decir que dada una entrada al aplicar esta misma entrada con las mismas variables producirá el mismo resultado) es imperativo la aleatorización.

Otro criptosistema es Curvas elípticas el cual como se menciona en (Azad, 2015) es el creado por Neal Koblitz y Victor Miller el cual será explicado mucho mas a fondo en su sección correspondiente.

En general podemos mencionar que casi siempre los algoritmos asimétricos utilizan 2 claves separadas y en general utilizan los problemas como curvas elípticas, logaritmos discretos y el problema de la factorización, Azad menciona que todos los algoritmos de cifrado asimétricos son generalmente utilizados para autenticar datos

Sin embargo siempre hay un problema, el cual es como completar verificar la identidad del personal que enviara los datos, entre esta y muchas otras cuestiones se ven desarrolladas en el concepto de ANI (Autenticación, no repudio y Integridad) de los datos

Azad menciona que la autenticación puede ser realizada por medio de las firmas públicas

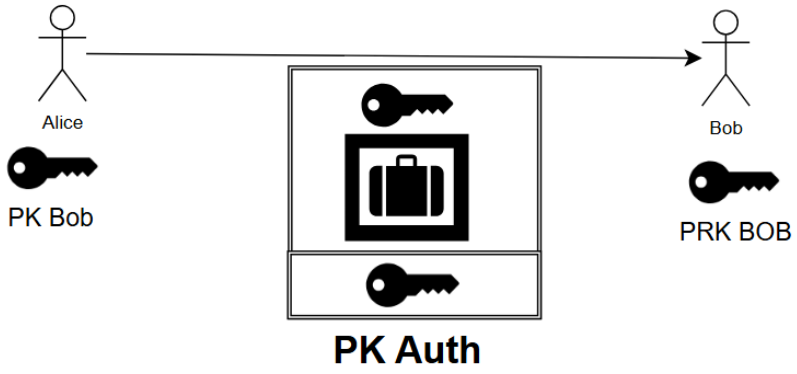
Así mismo con el caso del no repudio Azad menciona que "un emisor no puede bloquear la transmisión de un mensaje si dicho mensaje se encuentra firmado"

El concepto de integridad simplemente consiste en la no alteración de los datos mientras que viajen en un medio inseguro

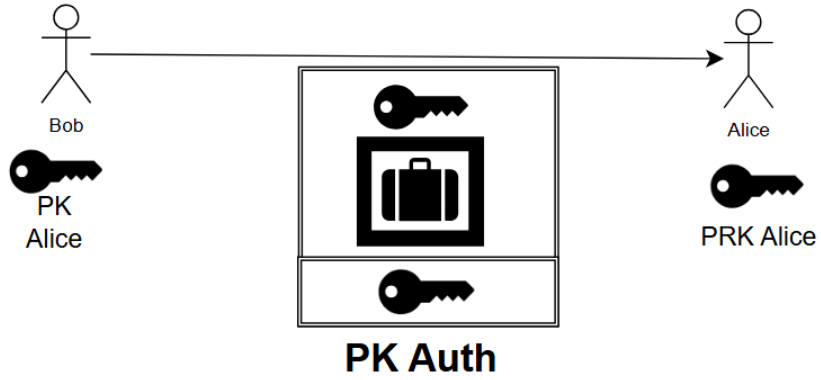
Las claves privadas en los cifrados asimétricos funcionan para la firma de los mensajes mientras que las claves publicas sirven para el descifrado de los datos, Azad pospone una técnica que no implementa necesariamente un protocolo criptográfico de firma, sin embargo funciona muy bien para poder explicar el funcionamiento del proceso de firmado de claves:

1) Azad pospone que es necesario contar con 1 par de claves compartida por ambos actores es decir (una clave publica y privada) a este par de claves se le conocera como las claves de autenticación
2) Un actor determinado puede enviar los mensajes al actor secundario haciendo uso de su clave privada para el cifrado de datos

Las siguientes figuras explican el funcionamiento de la autenticación con RSA



Alice envia informacion a bob haciendo uso de su clave publica para cifrar los datos, y bob descifra los datos con su clave privada, la clave de autenticación que ambos poseen permite autenticar que el mensaje no haya sido alterado



Alice envia informacion a bob haciendo uso de su clave publica para cifrar los datos, y bob descifra los datos con su clave privada, la clave de autenticación que ambos poseen permite autenticar que el mensaje no haya sido alterado

El funcionamiento consistiría en utilizar la clave de autenticación A_k para poder firmar los mensajes para posterior a su firma enviar los datos a la clave Publica utilizada para el cifrado de los datos, es necesario siempre descifrar los datos en el orden en el cual se firmaron es decir si primero se aplico la clave privada de autenticación (PRK) primero se tiene que descifrar los datos con la clave privada del receptor y después con la clave de autenticación por ejemplo con alice $PRK_{alice}(PRK_{auth}(c))$ donde c es el criptograma

Otro enfoque popular es hacer uso de las curvas elípticas las cuales como menciona Azad poseen un tamaño de clave publica/privada menor en relación a su contraparte RSA pero aun así mantienen la seguridad de los datos.

La NIST aconseja un tamaño de claves de 163 bits a comparación con el tamaño de claves usado por RSA que es de 1024 bits supone una ventaja en cuanto al almacenamiento de claves notoria.

Curvas Elípticas

Las Se basan en la geometría de curvas algebraicas y se definen por ecuaciones de la forma $y2 = x3 + ax + by\text{^}2 = x\text{^}3 + ax + by2 = x3 + ax + b$.

Estas curvas permiten realizar operaciones complejas que son computacionalmente difíciles de invertir, lo cual las hace ideales para criptografía de manera similar como ocurre con RSA.

El modo de funcionamiento de curvas elípticas es muy similar en cuestión de requerir números primos para poder crear las claves públicas y privadas, sin embargo en este caso es necesario un numero primo p y 2 parámetros para ajustar la curva elíptica denominados a y b, en este sentido no todas las curvas elípticas serán compatibles para la criptografía, la criptografía solo hace uso de una curva elíptica con propiedades específicas, Azad menciona que existen 2 tipos de curvas elípticas **las singulares** y **no singulares**, las no singulares o aquellas que no tienen raíces cuadradas en su forma, son usadas por el cifrado de curvas elípticas, ahora bien para generar los puntos que conformaran la curva elíptica existen 2 caminos a seguir:

1) Utilizando números primos
2) Realizando una curva binaria utilizando el galous field

Siendo solo las primeras admisibles de ser desarrolladas en un software, en resumen podemos mencionar que la criptosistema basado en curvas elípticas se fundamenta en la dificultad de resolver problemas matemáticos específicos, como el Problema del Logaritmo Discreto en una curva elíptica (ECDLP, por sus siglas en inglés).

Las curvas elípticas a grandes rasgos involucran una serie de pasos para poder ser implementadas

1. **Definición Matemática**: una curva eliptica debe forzosamente cumplir la condición de : $(4a^2 + 27b^2 \neq 0$).
2. **Grupo de Puntos**: Los puntos en la curva, junto con un "punto en el infinito" (punto neutro), forman un grupo abeliano bajo una operación de suma de puntos. Esta estructura es esencial para la criptografía, ya que permite definir operaciones como la multiplicación de un punto por un entero, los grupos abelianos son caracterizados debido a que permiten realizar operaciones sin importar el orden de los factores.

Ahora bien en específico de donde proviene la seguridad de las curvas elípticas?

1) **Operación de Suma**: La suma de dos puntos P y Q en la curva genera otro punto R. Si los puntos son iguales (P= QP = QP=Q), la operación se llama duplicación. La complejidad de esta operación en curvas elípticas contribuye a la seguridad del criptosistema.
2) **Problema del Logaritmo Discreto**: Dado un punto P y otro punto Q=kPQ = kPQ=kP, donde k es un número entero secreto, es extremadamente difícil encontrar k incluso si se conocen P y Q. Esta propiedad se aprovecha en los algoritmos de intercambio de claves y firmas digitales los cuales se explicaran mas adelante.

En la practica la forma de implementar estos algoritmos es haciendo uso de la infraestructura de clave publica (PKI) donde una autoridad generalmente conocida como CA emite los certificados y una entidad debe confiar en la autenticidad de estos certificados el CA generalmente incluyen datos como un numero serial para la identificación de quien se va a autenticar.

En general la forma para poder realizar y firmar los documentos utilizando una clave publica, los CA son en cierta forma organizados en base a si son privados o públicos mientras que los CA privados son prácticamente organizaciones como universidades o incluso CA dentro de una compañía, estos tipos de certificados son limitados a un contexto determinado mientras que los CA públicos son aquellos que se encargan de asegurarse que las comunicaciones o más bien las transacciones con determinados servidores sean seguras en el contexto de la red global.

Protocolo de Intercambio de Claves Diffie-Hellman

El protocolo Diffie-Hellman es un método para el intercambio seguro de claves a través de un canal inseguro. Permite a dos partes establecer una clave compartida, que puede ser utilizada para cifrar la comunicación posterior, sin necesidad de que previamente se conozcan. Esto se logra mediante el uso de un secreto privado y un número público acordado entre las dos partes.

El proceso se basa en la dificultad de resolver el problema del logaritmo discreto en grupos de gran tamaño. Para mejorar la seguridad del protocolo Diffie-Hellman, se emplean curvas elípticas (ECDH, por sus siglas en inglés), que hacen más difícil para un atacante determinar la clave compartida, incluso si tiene acceso a todos los datos intercambiados públicamente.

El protocolo Diffie-Hellman es uno de los primeros métodos para el intercambio seguro de claves que permite a dos partes establecer una clave compartida sobre un canal inseguro sin que ningún observador externo pueda interceptarla. Fue introducido por Whitfield Diffie y Martin Hellman en 1976 y representa un avance crucial en la criptografía moderna, ya que proporciona una base para la seguridad de las comunicaciones en redes públicas.

Funcionamiento del Protocolo Diffie-Hellman

El objetivo principal de Diffie-Hellman es permitir que dos partes, comúnmente llamadas Alice y Bob, acuerden una clave secreta común que puede usarse para cifrar mensajes entre ellos. Esta clave se negocia de tal manera que un atacante que esté escuchando no pueda deducirla, incluso si conoce todos los datos intercambiados públicamente.

Su funcionamiento consiste en el uso de grupos Cíclicos asi como el problema del logaritmo discreto. En su forma más simple, opera en el grupo multiplicativo de enteros módulo un primo grande p.

Aplicaciones Comunes

- **VPNs y Protocolos de Seguridad en Internet**: Como IPSec y TLS, donde se requiere un intercambio seguro de claves para establecer conexiones cifradas.
- **Mensajería Segura**: Utilizado en aplicaciones de mensajería cifrada como Signal y WhatsApp.

Conclusiones:

La evolución de los algoritmos y protocolos criptográficos refleja la constante necesidad de asegurar la comunicación y proteger la información en un entorno digital en constante cambio. Los algoritmos simétricos, como AES y Triple DES, ofrecen rapidez y eficiencia en la encriptación, pero presentan desafíos en la distribución segura de claves. Los algoritmos asimétricos, como RSA, han revolucionado la criptografía al resolver este problema, permitiendo la autenticación y el intercambio seguro de claves mediante pares de claves públicas y privadas.

Sin embargo, RSA y otros sistemas asimétricos no están exentos de vulnerabilidades, ya que su seguridad depende de implementaciones correctas y del uso de técnicas como el padding y la aleatorización para mitigar posibles ataques. Las curvas elípticas emergen como una alternativa poderosa, combinando alta seguridad con un menor tamaño de clave, lo que las hace especialmente adecuadas para dispositivos con recursos limitados.

Los protocolos como Diffie-Hellman ejemplifican el avance hacia métodos que permiten el intercambio seguro de claves sin la necesidad de un canal seguro previo, estableciendo la base para muchas aplicaciones modernas, desde VPNs hasta mensajería segura. En conjunto, estos algoritmos y protocolos no solo protegen la confidencialidad y la integridad de los datos, sino que también aseguran la autenticidad y el no repudio, pilares fundamentales de la seguridad informática.

A medida que la criptografía avanza, es esencial mantenerse actualizado y adaptar las implementaciones a las nuevas amenazas, como la computación cuántica, que podrían cambiar radicalmente el panorama actual. La continua innovación y la adecuada formación en criptografía seguirán siendo clave para garantizar la seguridad de la información en un mundo cada vez más digital y conectado.

Referencias

Azad, A.-S. K. (2015). *PRACTICAL CRYPTOGRAPHY.* Taylor Francis Group.

LOPEZ, M. J. (2011). *Criptografia y Seguridad en Computadores.* Andalucía: UNIVERSIDAD DE JAEN.

Galbraith, S. D. (2012). Mathematics of Public Key Cryptography. Cambridge University Press.

Schneier, B. (1996). Applied cryptography: Protocols, algorithms, and source code in C (2nd ed.).

John Wiley & Sons