Facultad de Ingeniería

Universidad de la República

Tesis presentada en la Universidad de la República
para obtener el título de Magíster en Ingeniería Matemática.

Director: Gonzalo Tornaría.

CRITERIOS DE ESTABLECIMIENTO DE CLAVES PARA UNA COMUNICACIÓN PUNTO A PUNTO

MODELOS DE USO Y ESQUEMAS DE REALIZACIÓN

Juan Escanellas.

11 de julio de 2013

Montevideo, Uruguay

RESUMEN. El objetivo de este trabajo es determinar criterios para el establecimiento de claves en una comunicación punto a punto. De un análisis preliminar de la seguridad de la comunicación, que involucra el canal, los mensajes y los usuarios participantes, se deduce que es necesario establecer una relación de equivalencia que permita distinguir a los usuarios. Esta relación está asociada al concepto usual de identidad. Se propone entonces un modelo que define qué atributos de identidad son necesarios para lograr el objetivo planteado. Se destaca de esta forma, a la vez, la importancia central de la identidad en la solución y la de establecer una comunicación adecuada de los requerimientos prácticos que tienen las hipótesis de los esquemas criptográficos disponibles, tanto para los usuarios como para los administradores de una solución final.

En el primer capítulo se indican qué aspectos del problema son importantes a la hora de seleccionar un esquema de establecimiento de claves. En el segundo capítulo se realiza una breve descripción de conceptos matemáticos a ser referidos en el capítulo tercero, que analiza los esquemas y las demostraciones de seguridad correspondientes.

Índice general

Capítulo 1

Establecimiento de claves

En este capítulo se describen los requerimientos del problema planteado y se analizan las condiciones y limitaciones inherentes. Se propone un modelo y criterios que permitan seleccionar los esquemas adecuados según el caso de uso. En los capítulos subsiguientes se describirá la seguridad de estos esquemas.

1.1. Introducción

La red telefónica tradicional garantiza una alta disponibilidad para establecer una comunicación. Agregando un dispositivo al teléfono es posible establecer una conversación segura aprovechando la calidad y la extensión de dicha red.

Como la voz consiste en variaciones de energía a distintas frecuencias en un rango limitado, midiendo la energía ocho mil veces por segundo se obtiene una secuencia numérica. A partir de esta es posible recuperar la conversación original.

Cifrando esa secuencia numérica con una clave secreta compartida, es posible restringir el acceso a la información de la conversación.

Luego de haber realizado un prototipo experimental a partir de componentes estándar disponibles en el mercado, surgió la necesidad de establecer criterios para determinar la clave compartida de manera segura.

Es necesario modelar como procesos aleatorios tanto los pasos del establecimiento de claves como las amenazas existentes y determinar cómo limitar la probabilidad de éxito de un atacante a un valor insignificante.

Para establecer una clave compartida no es suficiente lograr su transporte seguro, debe definirse "de quién" y "con quién" se comparte la clave. Estas "identidades" no corresponden a identidades reales, sino a condiciones que deben permitir establecer las restricciones deseadas sobre la comunicación. *Para establecer una clave es necesario determinar previamente en qué consiste la identidad de los usuarios.*

La capacidad de distinguir usuarios en un conjunto, corresponde a partir el conjunto en partes que se consideran "identidades" diferentes[1].

Esta partición del conjunto de usuarios podría basarse en una serie de condiciones que permitan asignar a cada usuario una parte del conjunto, por ejemplo el color de ojos, el tono de voz o por algo que posean o que conozcan. Cada subconjunto resultante será una "identidad", pero estos subconjuntos podrían contener más de un integrante. Por ejemplo, si dos usuarios quieren mantener una conversación confidencial, es suficiente restringir la conversación a un subconjunto de dos integrantes. Otros casos, en cambio, requieren poder definir particiones con más "precisión", por ejemplo para poder

[1] Matemáticamente la identidad es una relación de equivalencia que permite establecer la partición deseada en el conjunto (ver [Jud94] por más detalles)

distinguir el autor de una información compartida. En ese sentido también una identidad es un criterio de "medida" con mayor o menor capacidad de "separación" entre de los usuarios [2].

En este trabajo se propone un modelo de identidad compatible con las prácticas de identificación tradicionales y las nuevas técnicas que han surgido a partir de la criptografía moderna. Se clasifican posibles casos de uso para el establecimiento de claves y las condiciones que permitan seleccionar un esquema adecuado.

En este primer capítulo se presentarán los criterios que permiten seleccionar un esquema adecuado según el caso de aplicación. En el segundo capítulo se resumen los fundamentos matemáticos y las primitivas criptográficas citadas. Finalmente, en el tercer capítulo se describen los esquemas y las demostraciones de su seguridad.

Como se verá en detalle más adelante, para determinar el esquema más adecuado a una situación particular, los factores determinantes a tener en cuenta propuestos aquí serán: la cantidad de usuarios, la relación entre el tamaño de la clave y la cantidad de información numérica cifrada (el *"largo" de vida de la clave*) y la posesión de la información de la conversación (es decir, quién es el dueño de la información).

A continuación se definen las propiedades básicas de la seguridad de la información que se utilizan a lo largo de todo este trabajo.

Integridad: consiste en que la información no se modifique. En la práctica, alcanza con verificar si la información es la original.

Confidencialidad: se espera que la información no sea expuesta a extraños. Cuando la información viaja por un canal inseguro, debe ser encubierta mediante alguna transformación para que sea prácticamente imposible distinguirla. El cifrado simétrico permite con una única clave compartida, cifrar y descifrar su contenido entre quienes la conocen. La clave debe ser distribuída adecuadamente.

Disponibilidad: la información debe estar al alcance para su uso en el momento deseado.

Autenticidad: consiste en la garantía de que la información proviene de la fuente que se declara. Implica una prueba de identificación.

No repudio: es posible probar el autor de un mensaje aunque el este pretendiese rechazarlo.

Posesión: indica el dueño de la información y afecta el establecimiento de la clave, ya que este debe poder recuperar las claves involucradas en su información.

1.1.1. Desafío de la criptografía moderna.

La aparición de la criptografía asimétrica ha provocado un cambio a la hora de considerar los aspectos de mayor impacto en la seguridad de una comunicación. Al no requerirse un canal seguro para el acuerdo de la clave, es posible extender las aplicaciones de la criptografía. Sin embargo, sigue siendo necesario autentificar la información pública transmitida por el canal inseguro. La autentificación pasa a ser un aspecto trascendente, mientras que antes era un aspecto trivial determinado por la existencia misma del canal seguro. Es posible ofrecer más y mejores soluciones, pero aparece un nuevo problema: la autentificación requiere la capacidad de poder asociar la identidad a la información a autentificar.

[2] Así como la capacidad de separación que tiene un telescopio, por ejemplo.

Aparece así la necesidad de un proceso de identificación que permita verificar la identidad involucrada. Si bien es posible transformar la información de un mensaje reduciéndola a números, la identidad es un problema difícil de determinar directamente ya que requiere métodos convencionales que no es posible "digitalizar". Deben aplicarse procedimientos de registro de la identidad que cumplan con normas escritas y aceptadas por todos los involucrados en el ámbito de aplicación.

En los esquemas del modelo se requieren primitivas criptográficas como cifrar o firmar. Cuando se quiere lograr confidencialidad en la comunicación de la información (ya sea un documento, una conversación o una clave) es necesario disponer de un par de funciones (cifrar, descifrar) que permitan modificar y recuperar el mensaje.

Como se verá a continuación, para asegurar la exclusividad a un único usuario, las funciones de cifrado y descifrado deberán permitir restringirse a un único individuo y por lo tanto deberán depender de dos claves distintas. Es necesario así disponer de esquemas que utilicen cifrado *asimétrico* utilizando un par de claves (clave pública, clave privada), que actúan como candado y llave en analogía al acceso a una puerta. Estas funciones que cumplen la función de "escotillón, trampilla" (en inglés *trapdoor*), actúan como puertas secretas en una pared o piso de tal forma que su uso esté restringido al que no conozca el mecanismo de acceso.

1.2. Modelo propuesto: restricción de acceso e identidad

Es necesario establecer un modelo que permita representar la identidad. En primer lugar se analizará el problema de las restricciones de acceso necesarias, sus características y qué tipo de soluciones serían adecuadas según las condiciones del caso. Luego se analiza el problema de la autenticidad y la identificación, donde se presenta un modelo de identidad aplicable. Se obtiene un modelo que surge de las condiciones del problema sin hacer referencias a las tecnologías disponibles.

1.2.1. Restricción de la comunicación. En esta sección se analiza el problema de la comunicación a partir de las restricciones necesarias para el establecimiento de claves. Como se describe en la introducción es posible desplegar un canal digital a través de la línea telefónica. Para lograr la identificación a través de este canal, debe distinguirse una cadena de bits generada por una persona en particular. Si esa cadena de bits viajase por un canal inseguro podría ser reproducida. Por lo tanto: *debe existir un conocimiento secreto entre las partes que no viaje por el canal inseguro y que permitirá reconocer la identidad.*

A continuación se considerarán entidades que crean, modifican o leen mensajes y que desean comunicar los mensajes entre sí.

Definición 1. Sea $\mathcal{U}$ es el conjunto de usuarios que pueden acceder a un canal. Se clasifican los usuarios según su capacidad de acceso en *socios*, *rivales*, *autores* e *intérpretes*.

- $\mathcal{S}$ es el subconjunto de *socios* que pueden leer mensajes.
- $\mathcal{R}$ es el subconjunto de *rivales* que no pueden leer mensajes.
- $\mathcal{A}$ es el subconjunto de *autores* que pueden leer, crear y modificar mensajes.
- $\mathcal{I}$ es el subconjunto de *intérpretes* que solo pueden leer mensajes.

Para preservar la confidencialidad de los mensajes entre los socios es suficiente que todos los socios sean autores: $\mathcal{S} = \mathcal{A}$. En ese caso para todos los socios la restricción de la comunicación es la misma en ambos sentidos de la comunicación, por lo que se dirá que es una *restricción simétrica*.

Para preservar los derechos de autor entre los socios se requiere una restricción más fuerte que permita distinguir quiénes envían (autores) y quiénes reciben (intérpretes). En este caso se dirá que es una *restricción asimétrica*.

EJEMPLO 1.2.1. La Criptografía permite a un autor transformar un mensaje con una función de *cifrado* de tal forma que solo quienes posean la función para descifrar puedan leer el mensaje. Para simplificar la administración y el análisis de seguridad, estas funciones quedan determinadas por números enteros llamados *claves*.

DEFINICIÓN 2. Cuando las funciones de cifrar y descifrar utilizan la misma clave, todo lector es autor, por lo que resulta una restricción o *cifrado simétrico* de la comunicación.

Para lograr una restricción asimétrica se debe separar los autores de los intérpretes y distinguir así la acción de crear y modificar un mensaje (función para cifrar), de la acción de leer (función para descifrar). Si bien la función de descifrar debe permitir recuperar el mensaje original a partir del mensaje cifrado, no debería ser fácil deducir la función de cifrado a partir de la función de descifrado.

Por lo tanto, la función de cifrar deberá ser una función *flechada (one–way)* con un *acceso secreto (trap door)* cuya posesión permita utilizarla. Ese secreto se representa como una clave privada «a» que determina la función de cifrado del autor Ana. La función de descifrado correspondiente deberá tener determinado el acceso a través de una clave pública «α» que permita recuperar el mensaje cifrado para su interpretación.

DEFINICIÓN 3. Cuando las funciones de cifrar y descifrar utilizan dos claves distintas, resulta una restricción o *cifrado asimétrico* de la comunicación.

Una ventaja de utilizar claves para realizar restricciones asimétricas es que el análisis del uso de las funciones puede reducirse al uso de las claves, en particular, para el cifrado asimétrico debería ser difícil obtener la clave privada «a» a partir de la clave secreta «α».

1.2.2. Requerimientos del cifrado. A los efectos de cifrar un mensaje la información cifrada no debería aportar información sobre el mensaje original [Sha49].

Privacidad: es una restricción que separa "socios" de los *terceros* "rivales".

Autenticidad: es una restricción que separa al "autor" de un *par* "intérprete".

Aleatoriedad: indica que las claves se seleccionan del *total* de claves y no de un subconjunto de estas. Si a partir de la no aleatoriedad de las claves, el adversario obtiene información que permite reducir las claves posibles, aumenta su probabilidad de éxito en un ataque por ensayo y error (por «fuerza bruta»).

EJEMPLO 1.2.2. El cifrado simétrico no permite distinguir entre las entidades que poseen la clave. Se puede pensar que así como un instrumento óptico tiene un límite en su capacidad para separar o distinguir dos objetos, el "poder" de separación del cifrado simétrico es hasta grupos de dos o más entidades.

El cifrado asimétrico, en cambio, permite distinguir cualquier entidad y separar el autor del intérprete.

1.2.2.1. Características de las claves. Las claves permiten simplificar la utilización de funciones de cifrado y descifrado y establecer modelos más simples para medir la seguridad. También facilitan la realización de un sistema de administración y comunicación que alcance sus objetivos más eficientemente.

La aleatoriedad del mensaje para un adversario una vez aplicada la transformación de restricción (*cifrado*), depende de la aleatoriedad de la clave. Si la clave no es aleatoria será más fácil para el adversario (rival) obtener información de la clave o el mensaje.

La clave se representa (como información y para su procesamiento numérico) por una cadena de bits de longitud w. La cantidad de claves correspondiente es 2^w (cada bit permite duplicar las claves disponibles). De la misma forma la cantidad de mensajes posibles depende de la longitud en bits enviados. Si la cantidad de claves a disposición fuera igual a la cantidad de mensajes posibles y las claves se eligiesen de manera aleatoria, sería posible cifrar de tal forma que dado un mensaje cifrado, su origen haya podido ser cualquiera de todos los mensaje posibles. Se deduce que el resultado de la relación entre la longitud en bits de un mensaje cifrado y la longitud en bits de la clave, debería ser uno. Sin embargo, es muy difícil manejar claves de longitud comparable al de los mensajes enviados. En la práctica se establece un compromiso entre la facilidad de uso y la seguridad utilizando técnicas de cifrado a partir de claves de longitud acotada. En consecuencia, para mantener la relación entre el largo de los mensajes y el largo de la clave lo más bajo posible, debe cambiarse de clave con la frecuencia marcada por el crecimiento de esta relación.

En sentido figurado se utiliza la expresión *tiempo o largo de vida* para referirse al tipo de uso de una clave. Una clave de "*larga vida*" será una clave con la cual se espera cifrar poca información, mientras que una clave de "*corta vida*" será una clave que cifra mucha información [3].

1.2.3. Autenticidad y autentificación.

Definición 4. *Autenticidad* es la propiedad de ser genuino, verificable y confiable. (Confiable en el sentido de la validez de una transmisión, un mensaje o el origen de un mensaje).

Definición 5. *Autentificador* es el medio usado para confirmar la identidad del usuario, proceso o dispositivo. [NIS11]

Si una contraseña no viaja cifrada no es posible garantizar la autentificación. Si la contraseña viaja cifrada con clave simétrica la autentificación es parcial. Cuando en un dispositivo testigo (en inglés *token*) se utiliza cifrado asimétrico, es posible lograr una autentificación que brinde no repudio.

[3] Esto también es válido cuando se consideran claves para cifrar que sean fáciles de recordar, llamadas por eso "contraseñas" (*password* en inglés). Sin embargo usualmente las password para autentificación en un sistema (en inglés *login*) no se utilizan para cifrar la información del usuario, por lo que el análisis de su uso merece un enfoque distinto al realizado aquí.

1.2.4. Identidad. Para acordar la clave a través de un canal no confidencial de comunicación, es necesario intercambiar cierta información pública. Esta información debe enviarse de tal manera que impida a un tercero cualquiera no involucrado obtener la información secreta de la clave. Debe definirse un modelo aplicable de identidad que permita lograr este objetivo.

DEFINICIÓN 6. Según [NIS11] por identidad se entiende:

1. El *nombre completo* de tal forma que corresponda a un único individuo.
2. Las *características físicas y de comportamiento* por el cual un individuo es únicamente reconocible.

En inglés por *identity binding* se refiere a la acción de establecer esta relación entre el conjunto de individuos y el conjunto de sus nombres [4]. A los efectos del establecimiento de claves es necesario distinguir el usuario con quien se pretende establecer la comunicación de un adversario. Las condiciones que debería cumplir la *identidad* determinan la siguiente definición, así como el objetivo a modelar.

DEFINICIÓN 7. *Identidad* es la información invariante en el tiempo de una entidad que permite distinguirla de otra cualquiera. Parte de la información de identidad debe ser *inimitable*, de lo contrario otra entidad podría reproducir y asumir la identidad de otra, es decir *usurparla*.

1.2.4.1. Identificación. La identificación consiste en autentificar la identidad de una entidad determinada en el momento, mientras que la firma de un documento permite que sea autentificado a futuro.

Para probar la identidad usualmente se exige:

- características de comportamiento o atributos físicos ("lo que se es"),
- documentos o credenciales ("lo que se posee"), o
- "lo que se conoce" como ser contraseñas, información personal, etc.

Todo protocolo de acuerdo de claves requerirá la autentificación de la información intercambiada. Los datos necesarios para lograr la identificación corresponderán a la información necesaria para distinguir a un interlocutor de cualquier otro participante en el canal. Los datos de identificación son datos brindados por una fuente que se asume confiable durante la fase de *presentación* de la identidad.

La identificación, como toda toma de decisión, debe fundamentarse en criterios de discriminación objetivos. Un criterio objetivo permite determinar el resultado independientemente de quién realiza la evaluación. En la práctica esto permite establecer una correspondencia bien definida entre entre los criterios utilizados y los resultados.

EJEMPLO 1.2.3. El reconocimiento personal no es objetivo si depende de criterios no establecidos o de habilidades no transferibles: no es fácil determinar reglas claras para discriminar modalidades individuales de expresión: "forma de hablar", "gestos", etc. Lo mismo se puede decir de criterios de discriminación como "simpatía" o "afinidad". La

[4] Matemáticamente corresponde a establecer una función *inyectiva* entre el conjunto de individuos y sus nombres. Una función es inyectiva si a cualquier par de individuos (distintos) les corresponde un par de nombres (distintos).

falta de definición objetiva permite la aplicación de criterios "implícitos" que pueden ser manipulados [5].

1.2.4.2. Descripción del modelo de identidad.

DEFINICIÓN 8. Se llamará *plantilla* a información que (en el contexto de aplicación) sea inimitable (intransferible por medios externos), invariante en el tiempo y que represente una característica exclusiva de cada individuo.

EJEMPLO 1.2.4. En los sistemas tradicionales de autentificación se espera que el estilo de grafía personal cumpla la función de *plantilla*. También se utiliza como plantilla personal la propia yema del dedo para registrar la huella digital. En el sistema de cifrado asimétrico la plantilla corresponde a un número secreto llamado clave privada que no es "imitable".

Otro componente necesario en la información de la identidad debe ser *declarable* sin dar por ello indicios que permitan reproducir la *plantilla*.

DEFINICIÓN 9. Se llamará *muestra* a la parte declarable de la identidad asociada a la plantilla.

EJEMPLO 1.2.5. La rúbrica de una firma es una muestra (declaración del estilo de firma personal) comparable a la marca estampada de un sello o a la huella de tinta dejada en el papel de un documento de certificación. En el cifrado asimétrico la *muestra* corresponde a la clave pública, mientras que la *plantilla* es la clave privada. Se supone que la clave pública no brinda información de la clave privada. Esta es una hipótesis que será considerada con más detalle en los capítulos siguientes.

DEFINICIÓN 10. Se llamará *identidad virtual* al par (plantilla, muestra) para representar en este modelo a las características inimitables y declarables que permiten distinguir una identidad.

EJEMPLO 1.2.6. La identidad virtual es una representación objetiva en el modelo de los criterios usados habitualmente para reconocer a una persona, el rostro puede representar la plantilla y su fotografía la muestra. También el dedo pulgar y su huella pueden constituir una identidad virtual.

DEFINICIÓN 11. Llamamos *declaración de identidad* del usuario U a la información en bits formada a partir del par (nombre, muestra):

$$\text{“U”} \parallel \text{ver}_U,$$

donde

- “U” representa una cadena de bits asociada al nombre único o identificación nominal, consistente en el nombre y datos que aseguren su unicidad,
- ver_U representa una cadena de bits asociada a la muestra (por ejemplo, la clave pública) de U y

[5] No solo en referencia al necesario rigor científico sino para dejar un marco claro del cumplimiento de las normas. La *ingeniería social* manipula los efectos de los *prejuicios* de los individuos sobre su interpretación de lo que "se *debía* hacer".

- $\|$ representa la operación de concatenación de bits.

Para verificar la asociación entre la identidad virtual y la declaración de identidad sin que sea necesario revelar la plantilla, es necesario un mecanismo de verificación. Esta *verificación* puede brindarla un agente confiable que conociendo la identidad de la entidad la presente como tal. El agente brindará las garantías necesarias para una identificación rigurosa justificable en el contexto de aplicación.

Según las condiciones definidas en un acuerdo establecido previamente entre las partes, el agente confiable o autoridad de confianza asignará un mecanismo de *verificación* a la *declaración de identidad* correspondiente, permitiendo así determinar lo que llamaremos *identidad relativa* (Ver Figura 1.2.1).

Definición 12. Llamamos *identidad relativa* al par formado por la *declaración de identidad* y un mecanismo de verificación de su autenticidad.

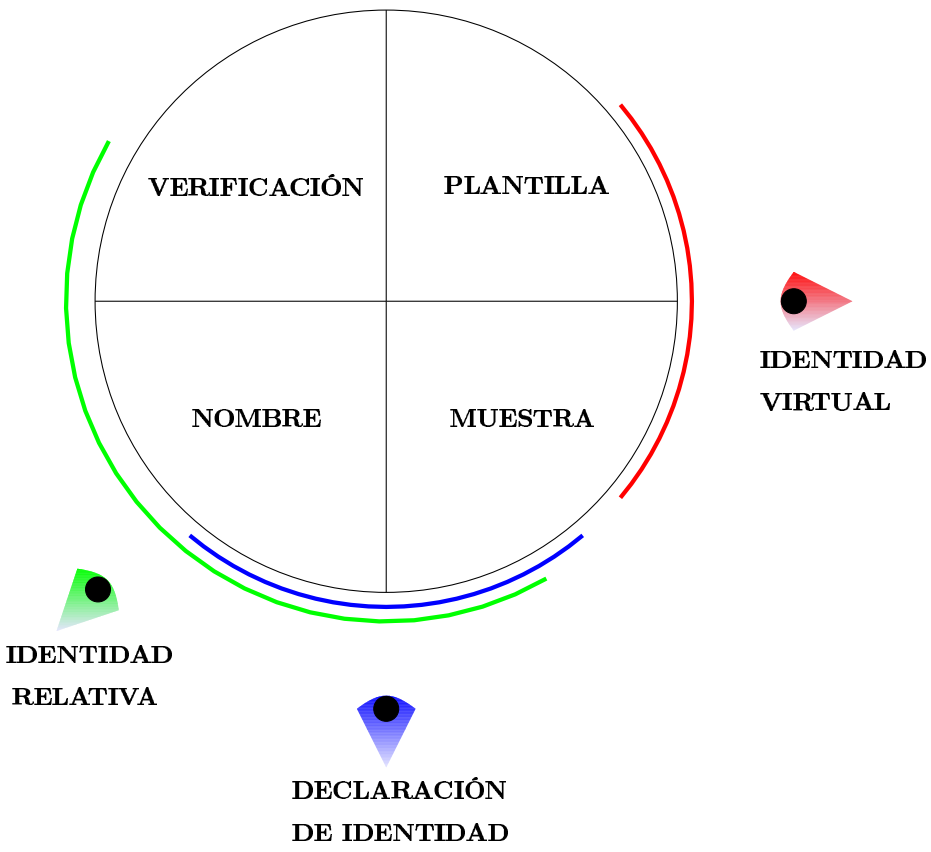

Figura 1.2.1. Modelo de identidaad.

Ejemplo 1.2.7. Un mecanismo de verificación usualmente aceptado consiste en que un agente confiable y reconocido (TA) presenta la declaración de identidad en un documento aplicando su firma. En la medida en que todos los usuarios puedan *reconocer* la firma del TA será posible realizar la verificación.

Definición 13. Para emitir un *certificado digital* (que se notará como Cert_U para un usuario U) se requiere un proceso confiable de un agente externo llamado TA especificado en un contrato. En primer lugar se toma registro de la declaración de

identidad, donde el nombre es un conjunto de datos que identifican únicamente al usuario y la muestra corresponde a su clave pública. Luego se emite el certificado adjuntando la firma del TA de la declaración de identidad. En el acto del registro, los usuarios reciben del TA su muestra. A partir de ese momento la muestra del TA permitirá verificar su firma de las declaraciones de identidad de todos los usuarios registrados.

En conclusión, la identidad en este modelo se compone de la identidad relativa y de la identidad virtual. La identidad relativa y la identidad virtual tienen en común la muestra.

Definición 14. En un ataque *Man In the Middle* (MIM) una entidad se interpone en un canal de comunicación asumiendo las identidades de cada extremo, presentando a cada una, los correspondientes pares (nombre, muestra). Esto ilustra la necesidad de un mecanismo de verificación de la relación entre la *identidad virtual* y la *declaración de identidad*. En la descripción del esquema KAS STS (ver 3.6.1) se muestra un ejemplo de este ataque.

Ejemplo 1.2.8. Un ejemplo de identificación tradicional es el carné o tarjeta de identificación, donde un agente registra cada usuario asociando el nombre y la muestra que puede ser la fotografía del rostro o la huella digital.

Ejemplo 1.2.9. En una solución de clave asimétrica, el par de claves (pública, privada) constituye una identidad virtual. La clave pública es la muestra y la clave privada la plantilla. Sin embargo la identidad virtual podría ser asociada a cualquier nombre si no se dispone del mecanismo de verificación de la identificación relativa.

1.2.5. Necesidad de certificación. Para que una entidad certifique la asociación entre una muestra y una identidad debe establecerse una relación de confianza. Una vez definido un modelo de identidad adecuado a la situación real cuya solución debe realizarse, aparece naturalmente el rol de la presentación, es decir, cómo aprendemos las nuevas identidades. Quienes cumplen el rol de presentar identidades nuevas deben gozar de la propiedad de confianza. Sin embargo, la confianza es una propiedad difícil de establecer de manera general. Existen soluciones que pretenden ser universales pero aplicando procedimientos administrativos que requieren una importante infraestructura o estableciendo criterios más flexibles de presentación que pueden ser cuestionables en cuanto a su confiabilidad. No existe una solución perfecta para la confianza a la hora de la presentación de una nueva identidad. Para cada caso debe pensarse con cuidado que solución de confianza se elige y si esta se ajusta adecuadamente a los requerimientos.

Es posible establecer distintos niveles de *autoridad de confianza*. Las TA pueden firmar certificados en un dominio, pero requerir de una firma de un TA superior para reconocimiento en un dominio más amplio de usuarios. Por ejemplo un TA de un país y un TA internacional. Cuando más alto esté el TA en este árbol jerárquico, mayor será su autoridad de confianza. Una entidad de confianza superior puede presentar otras entidades de menor nivel de confianza.

Definición 15. En el TA, la responsabilidad de realizar los procedimientos convencionales de verificación de identidad de los usuarios recae sobre la *autoridad de registro* (RA, en inglés *Registration Authority*).

Una vez realizado el registro, la *autoridad certificadora* (CA, en inglés *Certification Authority*) recibe del usuario su clave pública y junto con otra información de aplicación y administrativa procede a firmarla (con la clave privada de la autoridad certificadora).

Cuando corresponde, la clave pública de la autoridad certificadora se emite en un certificado de una autoridad de certificación superior o es firmada por sí misma, siendo entonces un certificado *certificado por sí y disponible para todos los usuarios*.

Resumiendo, la autoridad de registro debe contar con un mecanismo convencional de identificación de los participantes, de tal forma que permita protocolos de verificación de la identidad (autentificación). Se pretende mediante un contrato, que al emitir las claves o los certificados, estos correspondan a la identidad pretendida. La utilización de una clave pública para cifrar o firmar, solo verifica la correspondencia con su clave privada, pero no la identidad de su propietario. Mediante un certificado del TA es posible verificar la correspondencia entre la declaración de identidad y la clave privada. La emisión del certificado requiere un procedimiento de verificación convencional de la identidad de quien declara ser propietario de la clave pública.

La estructura de confianza también juega un rol fundamental. Como vimos debe permitir un procedimiento que es posible auditar. Esta confianza puede delegarse a una entidad o formarse por los propios usuarios pero siempre estableciendo un protocolo de registro. El TA en general se encarga de los procedimientos de registro y de emisión de certificados, que consisten en documentos digitales que unen indivisiblemente la clave pública a información de identificación mediante la firma digital del TA. Aquí, la clave pública del TA debe adquirirse mediante un mecanismo de confianza en el acto de registro.

1.2.6. Emisión de certificados digitales.

Definición 16. Un certificado (de clave pública) [NIS11] es una representación digital de información que por lo menos:

1. identifica la autoridad certificadora que lo emite,
2. nombra o identifica al suscriptor,
3. contiene la clave pública del suscriptor,
4. identifica el período de validez, y
5. está firmado de forma digital por la autoridad de certificación que lo emite.

Para la emisión de los certificados:

1. Se establece la identidad de manera convencional, determinando una cadena de caracteres con la información de identificación.
2. Se determina el par de claves (firma/privada y verificación/pública), donde la clave de firma/privada queda en poder del usuario.
3. El TA genera la firma de la cadena de caracteres formado por la información de identificación y clave de verificación (pública). A partir de la información anterior, el certificado consiste en la terna, (nombre, clave de verificación, firma del TA).

1.2.7. PKI. Una infraestructura de clave pública (en inglés *Public Key Infrestructure*, PKI) consiste en una infraestructura que permite proveer servicios de comunicación segura, control de acceso y arquitectura de privacidad mediante la administración

de certificados. Debe proveer los mecanismos para poder realizar la emisión de los certificados, su revocación, etc.

Además de brindar una solución a la confianza necesaria para determinar la autenticidad de la declaración de la identidad, sin la cual, como vimos, la criptografía asimétrica no puede establecerse, esto debe dar un marco para permitir otros controles de aplicación.

Introducir una PKI en un entorno o en una organización determinada, requiere una cuidadosa planificación y profunda comprensión de las relaciones con otros sistemas automáticos involucrados.

DEFINICIÓN 17. Una infraestructura de clave pública (PKI) facilita la disposición de productos y servicios de integridad y autenticidad para soluciones digitales que históricamente utilizaban papel. Estas soluciones digitales dependen de la integridad y la autenticidad de la información, que pueden realizarse asociando una única firma digital a un individuo y evitando su falsificación. Además es posible brindar privacidad cifrando la información.[KHPC01]

DEFINICIÓN 18. Una autoridad de certificación (en inglés *Certification Authority*, CA) es una entidad confiable que emite y revoca certificados de clave pública. También es responsable de cumplir estrictamente con la política de la PKI.

DEFINICIÓN 19. Autoridad de registro (en inglés *Registration Authority*, RA) es una entidad confiable que establece y responde por la identidad de un suscriptor al proveedor de credenciales de identificación (en inglés *Credential Service Provider*). El RA puede ser parte o ser independiente al proveedor de credenciales, pero está siempre en relación a este. Es la organización responsable de definir la función de identidad (identity binding).

DEFINICIÓN 20. La lista de certificados revocados (en inglés *Certificate Revocation List*, CRL) es una lista creada y firmada por una CA que indica los certificados que han perdido validez antes de su vencimiento.

La administración de certificados debe incluir:

Registro: consiste en las tareas administrativas tradicionales para determinar la identidad, verificando documentos, información presencial, realizadas por la RA.

Administración de claves: debe controlarse la generación, asignación y distribución de las claves.

Respaldo: los procedimientos para respaldo en caso de pérdida de las claves privadas deben ser definidos y cumplir con los requerimientos del caso.

Emisión de certificados: es el procedimiento mediante el cual se habilita un certificado que ha sido solicitado para su aprobación.

Recepción de certificados: es el procedimiento de ingreso de las solicitudes de certificados, para su creación o renovación.

Actualización: acción de renovación de un certificado.

Recuperación: acción de recuperación ante la eventual pérdida de la clave privada. (Es un servicio opcional: el manejo de la clave privada por otra parte que no sea su dueño requiere garantías para no socavar los fundamentos del modelo de identidad).

Revocación: acción por la cual se da de baja a un certificado y se lo incluye en la CRL.

Expiración: fin del período de validez del certificado.

Historia de claves: procedimiento que permite la verificación de información firmada o cifrada con certificados que han expirado o han sido revocados.

Almacenamiento de claves: definición del procedimiento por el cual se define el lugar y método de acceso a las claves según el caso.

1.2.8. Funciones de la entidad administradora (TA). La TA es la entidad encargada de distribuir la información previa para establecer la comunicación entre las partes.

La administración de las claves requerirá:

Almacenamiento: de las claves con acceso restringido.

Respaldo: de aquellas claves para su eventual recuperación.

Distribución: de las claves a los participantes según sea requerido.

Control: de validez por:

- Expiración: por política del TA, se limita el tiempo de validez de una clave para controlar su exposición teniendo en consideración el contexto, por ejemplo ante el riesgo de un ataque pasivo consistente en observar el texto cifrado para deducirla.
- Revocación: en cualquier momento, por ejemplo a solicitud de un usuario, se suspende la validez de una clave por pérdida o robo.

También deberá cuidar la información manejada teniendo en cuenta:

Posesión: de la información del canal y por lo tanto de las claves.

Integridad: de la información almacenada.

Autenticidad: de la información de identificación que determinará las identidades y su asociación con certificados y claves.

Disponibilidad: de las claves para establecer una sesión.

No repudio: de un trámite de solicitud de certificado o clave.

A medida que crece el número de claves se requerirán más recursos para su administración.

Las tareas del TA, según las necesidades y conveniencia del caso, podrían ser realizadas por los propios participantes, por una parte de ellos o ser delegadas a una entidad independiente.

1.2.9. Validación de certificados.

1. Verificar la integridad y autenticidad del certificado verificando la firma del TA.
2. Verificar que el certificado no expiró.
3. Verificar que el certificado no ha sido revocado.
4. Verificar que el certificado corresponde a lo especificado en campos opcionales.

1.2.10. Mecanismos de control de revocación. A los efectos de permitir el control a los usuarios de los certificados que hayan sido revocados, es posible mantener disponible una lista de números de serie de los certificados revocados. La preparación, firma, publicación y actualización de esta lista (en inglés: *Certificate Revocation List*,

CRL) es responsabilidad del TA. Dado que el tamaño de las listas puede llegar a ser muy grande, es posible mantener un *repositorio* de la lista y las últimas modificaciones.

Otra técnica utilizada es utilizar un "protocolo de estado de certificados en línea" (OSCP), donde un servidor responde las consultas sobre un certificado consultando la CRL.

1.3. Modelos de confianza

Cuando existen más de un TA entre dos usuarios, los TA deben ser también identificados y por lo tanto disponer de identificación firmada por otro TA de igual o mayor autoridad de confianza. Un TA que no dispone de firmas de otro TA se llama raíz, y un TA que firma el certificado de otro, establece una relación de orden entre ellos. Este orden puede ser estricto, en cuyo caso se establece un árbol jerárquico estricto entre TA o de lo contrario puede ser *radial* (en inglés: *hub and spoke*). Un usuario debe establecer un camino, según el orden anterior, entre su TA y su usuario par, además de verificar que las condiciones del camino están de acuerdo con la arquitectura del modelo, de tal forma que en un modelo jerárquico estricto, no es aceptable la firma por parte de un TA de jerarquía inferior a un TA superior.

NOTA: Un aspecto a considerar es que un TA cuando firma el certificado de otro, en principio firma su identidad, no con esto asegurando que los TA inferiores actúen adecuadamente.

1.3.0.1. Modelo de confianza jerárquico estricto. En una jerarquía estricta el TA raíz es llamado *ancla de confianza* (en inglés *trust anchor*) y es el encargado de emitir certificados a los TA de menor nivel. Cada TA puede emitir certificados a los suscriptores. El modelo tiene una estructura de árbol basado en una relación de confianza (ver la Definición 44).

1.3.0.2. Modelo de confianza en red. En el modelo de confianza en red los TA se certifican entre sí. Pueden tomar dos formas:

- *Configuración en malla* en que los TA se firman los certificados entre si.
- *Configuración radial* (en inglés *Hub and Spoke*) una TA central (Hub) certifica el resto de las TA .

En el modelo de confianza en red, la cantidad de certificados a emitir entre las n autoridades de confianza participantes será:

- proporcional a n en el modelo radial,
- proporcional a n^2 en el modelo en malla.

1.3.0.3. Modelo de confianza basado en un navegador de Internet. El programa que se utiliza para la navegación por Internet contiene una lista de TA, y el usuario confía en el proveedor del navegador en incluir TA válidas. Su desventaja consiste en que no posee un servicio adecuado de revocación de TA y cuando una conexión no tiene certificado válido, se da la opción al usuario de darlo por válido de todas maneras, lo que pone en cuestión el fundamento en sí del sistema de seguridad de los certificados.

1.3.0.4. Modelo de confianza PGP. El sistema de criptografía PGP [Ass00] es híbrido ya que combina criptografía asimétrica y criptografía simétrica. Para verificar la validez de la asociación entre el destinatario y la declaración de la identidad (su nombre y clave pública), se establece un sistema de certificación basado en firmas confiables del par (nombre, clave pública).

En el esquema PGP se definen tres niveles de confianza (*Completa*, *Marginal* y *Ninguna*) y tres niveles de validez (*Totalmente válido*, *Marginalmente válido*, *Sin validez*).

La confianza se establece mediante el modelo de "presentación", según el cual se delegan a personas o entidades la capacidad de presentar un certificado como válido, cumpliendo así el rol de CA. Cada presentador puede tener un nivel de confianza: *Completa* cuando su firma es suficiente para dar validez total a un certificado o *Marginal* cuando apenas puede brindar validez marginal. Se requieren dos entidades con confianza marginal o una entidad con confianza total para que un certificado sea *Totalmente válido*.

1.3.1. Cifrado basado en identidad. El sistema de cifrado basado en identidad (en inglés *Identity Based Cryptography*, IBC o *Identity Based Encription*, IBE) tiene varias similitudes pero también diferencias importantes respecto al cifrado por clave pública tradicional. En el sistema de cifrado IBC los usuarios se registran ante el TA para obtener un conjunto de parámetros públicos.

Con estos parámetros el usuario puede calcular la clave pública asociada a cualquier nombre de identificación. Esto permite una aproximación diferente ya que aquí un usuario puede preparar un nombre que incluya una serie de condiciones y determinar la clave pública correspondiente aplicando una función *hash* (ver sección 2.5) que permite resumir la identificación del usuario junto a parámetros públicos del sistema.

El destinatario de la información cifrada se autentifica ante el generador de clave privada (PKG, *Private Key Generator*) que es la parte del TA. Para determinar la clave privada la PKG usa información propia secreta llamada *clave maestra* (en inglés *master secret*) combinada al nombre del usuario para calcular la clave privada y se entrega al usuario autorizado.

Los algoritmos necesarios en un esquema IBC son: *establecimiento*, *extracción*, *cifrado* y *descifrado*.

El establecimiento: inicializa los parámetros requeridos, incluyendo el secreto maestro que la PKG utiliza para calcular las claves privadas.

La extracción: es el algoritmo que calcula la clave privada a partir de los parámetros del establecimiento, junto con el nombre de la identidad del usuario, usando para esto la clave maestra de la PKG.

El cifrado: se realiza con la clave pública IBC. La clave pública es determinada a partir de los parámetros públicos del establecimiento y el nombre de la identidad del usuario.

El descifrado: se realiza con la clave privada IBC obtenida de la PKG.

EJEMPLO 1.3.1. En IBC es posible cifrar información médica reservada con destino a un rol "doctor" como parte del nombre de identificación de la identidad. Aquellos que cumplan con estas condiciones de identificación podrán tramitar su clave privada. Cuando una organización tiene una infraestructura basada en roles, IBC permite cifrar la información reservada para ser descifrada por alguien que cumpla ciertas combinaciones de información de identidad que correspondan a dicho rol.

1.3.1.1. Conclusiones sobre el cifrado IBC. Cuando la organización es propietaria de la información a cifrar, IBC presenta ventajas por su bajo costo y gran facilidad

de uso respecto al cifrado con clave pública tradicional ([Lut08]), ya que el TA conoce la clave privada de los usuarios. Esto permite que la organización pueda recuperar las claves privadas cuando la falta de un empleado no puede implicar la falta de la información que este maneja. (Sin embargo esto impide el no repudio).

Aún así debe mantenerse cuidadosamente el sistema de identificación (nombres de identificación, etc.) así como la revocación y la expiración de las claves. La clave maestra del TA no debe poder determinarse a partir de las claves de los usuarios, ya que esto permitiría la falsificación del TA. Para la generación de la clave maestra el TA determina un par (clave pública, clave privada) y utiliza una función pública que permite incluir detalles de identificación del TA así como parámetros del sistema.

Los algoritmos de clave pública nos permiten comunicar de forma segura con otros sin haber intercambiado la clave previamente. Esta ventaja implica asumir hipótesis adicionales. En el caso de los algoritmos de clave pública tradicionales, se utiliza un certificado digital para administrar la clave pública de los usuarios y es necesario establecer una relación de confianza en el TA y la PKI. Allí se generan los certificados con el rigor correspondiente a la seguridad prometida. Si el TA comete un error (propio o provocado maliciosamente por un tercero) y asocia un nombre incorrecto a la clave pública de un usuario, es posible cifrar un mensaje con la clave incorrecta o que una firma no represente a quien realmente representa. Además si las realizaciones de clave pública tradicional archivan copias de las claves privadas de los usuarios, se debe tener una confianza total en cuanto a los servicios de seguridad brindados, en cuanto a que esas claves no terminen en manos de usuarios no autorizados.

En el caso de IBC, los supuestos necesarios son distintos. Cualquier usuario puede calcular una clave pública a partir del nombre de identidad del usuario y los parámetros públicos correctos, pero debe asumirse que los usuarios reciben los parámetros públicos. Si se brinda a un usuario parámetros incorrectos, fácilmente se puede descifrar sus mensajes cifrados. También se debe suponer que la PKG IBC autentifica los usuarios apropiadamente antes de asignarles sus claves privadas y que ciertos problemas sean inviables.

1.4. Esquemas de establecimiento de claves

Una clave de larga vida puede ser distribuida previamente a los usuarios por el TA o, si es de corta vida, ser distribuida en cada instancia de sesión requerida. Alternativamente la clave puede ser acordada sin la participación activa del TAque eventualmente participaría distribuyendo certificados previamente, pero no durante el establecimiento de la clave. Así, las opciones de establecimiento de claves se clasifican en esquemas de distribución previa de claves (KPS, en inglés *Key Predistribution Scheme*), esquemas de distribución por sesión (SKDS, en inglés *Session Key Distribution Scheme*) y esquemas de acuerdo de claves (KAS, en inglés *Key Agreement Scheme*). Estos esquemas se caracterizan por:

KPS: el TA distribuye información de claves anticipadamente a todos los participantes que, en el momento de requerirlo pueden utilizarla para cifrar una comunicación. Esto permitirá a cada par de usuarios determinar la clave correspondiente a una sesión de comunicación entre ellos, a partir de la información que el TA distribuyó a cada usuario del par.

SKDS: el TAelige a demanda claves de sesión y los distribuye mediante un protocolo interactivo. Se supone que el período de validez de una clave de sesión es relativamente corta. Las claves de sesión se cifran con claves establecidas anticipadamente entre el TA y los usuarios del esquema.

KAS: para acordar una clave de sesión, los usuarios emplean un protocolo interactivo. Este protocolo puede estar basado en esquemas de criptografía simétrica o asimétrica y no requieren la participación de un TA durante la ejecución del protocolo.

1.4.1. Seguridad en la distribución y acuerdo de claves. Consideremos dos participantes Ana y Ben que desean establecer una clave. Deben considerarse las amenazas y objetivos de un posible adversario Omar y las acciones que podría intentar para lograrlos.

Dado un esquema de distribución o acuerdo de claves, el adversario puede intentar:

1. modificar un mensaje,
2. almacenar un mensaje para uso futuro,
3. usurpar la identidad de un usuario.

Para lograr

1. hacer que Ana o Ben acepten una clave inválida,
2. hacer creer a Ana y Ben que establecieron una clave cuando no,
3. obtener alguna información sobre la clave establecida.

Dada la dificultad de evaluar la seguridad de un esquema, disponer de una demostración de su seguridad brinda una clara definición de los supuestos y de sus objetivos. Luego deberá verificarse el cumplimiento de los supuestos y si los objetivos corresponden a las necesidades del modelo y a la solución que se pretende con este. Una demostración no asegura que un esquema no pueda ser atacado con éxito bajo cualquier condición, sino que permite reducir el problema a ciertas hipótesis que permiten un mejor análisis del riesgo involucrado al implementar una solución. Una vez conocido el riesgo de esas hipótesis, la demostración permite deducir exactamente el riesgo del esquema. En la práctica el problema de factorizar números muy grandes o la solución del logaritmo discreto permiten establecer criterios de evaluación aplicados por estándares a nivel internacional. Sin embargo basar la seguridad en la probabilidad de un complot en un contexto particular, es quizás más difícil de justificar.

1.4.2. Comparación de esquemas KPS. Si bien los esquemas de KPS por acotación de complot son incondicionalmente seguros (es decir, no dependen de una conjetura que supone que un problema es difícil de resolver), desde el punto de vista de la aplicación del modelo, es recomendable depositar la confianza en la dificultad de resolver un problema matemático, estudiado universalmente, que en la dificultad de realizar un complot, a menos que se disponga de información justificable objetivamente.

1.4.3. Establecimiento de claves de sesión. El establecimiento de claves de sesión, permite disminuir:

- la vida de las claves,
- la cantidad de claves del sistema,
- las claves que cada participante debe almacenar,

Para su realización existen dos alternativas, la *distribución* y el *acuerdo* de claves de sesión.

1.4.4. Distribución de claves de sesión SKDS. Es recomendable utilizar esquemas de distribución de claves de sesión (SKDS [Sti06]) cuando el dueño de la información no participa de la sesión o cuando se prefiera utilizar criptografía simétrica. En SKDS cada participante deberá establecer en cada sesión un canal seguro con el TA mediante el acuerdo previo de una clave de larga vida o el uso de certificados.

La cantidad de claves de larga vida por usuario se minimiza, mientras que el TA debe almacenar una cantidad proporcional a la cantidad de participantes de claves de larga vida. El TA genera las claves de cada sesión a demanda de los participantes previo a la comunicación entre ellos. Por lo tanto:

1. cada participante almacena una clave de larga vida,
2. el TA almacena las claves de cada participante,
3. el TA genera las claves y las distribuye para cada sesión mediante el canal seguro establecido; puede usarse para esto criptografía simétrica o asimétrica.

1.4.5. Acuerdo de claves de sesión (KAS). En el acuerdo de claves de sesión (KAS) los participantes pueden determinar la clave de sesión a partir de información establecida previamente sin que el TA participe activamente durante el establecimiento de las claves. El TA se encarga de la distribución de los certificados requeridos por los esquemas para permitir la autentificación de las claves. Cada usuario puede determinar su clave independientemente: *la clave de sesión no tiene que ser transmitida.*

En 3.6 se trata la seguridad de los esquemas de acuerdo de claves.

1.4.6. ZRTP. El protocolo ZRTP [Bre07] es un protocolo usado para acordar claves por canales de voz. No requiere certificados y usa claves (de corta vida: efímeras) determinadas por Diffie–Hellman. Una vez establecida la primer clave segura, se combina parte de la clave anterior con la siguiente para evitar ataques *MIM* (ver la Definición def:mim) subsiguientes. El acuerdo de la primer clave, se compara entre ambos extremos leyendo el resultado de aplicar una función que permite obtener un resumen característico de la clave. Se debe recordar que de todas maneras, para establecer una clave se requiere información de identificación previa. Por más detalles prácticos sobre la investigación de la seguridad de ZRTP, consultar [BB10]. En ZRTP se supone que la información necesaria para el reconocimiento mutuo es suficiente. De lo contrario, sería fácil realizar un ataque *MIM* sustituyendo primero la identidad del extremo y luego la clave.

1.4.7. Resguardo compartido de una clave. Cuando un TA administra una clave secreta, es posible mejorar la confiabilidad compartiendo la responsabilidad de acceso a la clave secreta. Para resguardar una clave cuyo acceso es sensible, se puede distribuir información parcial de esta entre varios participantes de tal forma que a partir de cierto valor *umbral* t (en inglés *threshold*) sea posible su recuperación. En el esquema de resguardo compartido de claves de Shamir, (ver [Sti06] capítulo 13), el propietario de la clave (que no participa en el esquema) distribuye las “partes” a los participantes. Solo a partir de un acuerdo entre t de estos participantes es posible recuperar la clave.

1.5. Características determinantes del modelo

En esta se sección se indican las variables del modelo a tener en cuenta para determinar el esquema de distribución de claves más adecuado al caso de aplicación.

- Número de usuarios ν,
- Número de claves γ,
- Tiempo de validez τ,
- Facilidades de encuentro entre usuarios para acordar claves,
- Uso de contraseñas o claves por parte de usuarios,
- Propietarios de la información a intercambiar,
- Relaciones de confianza,
- Valor de la información,
- Costo de un TA,
- Grado de exposición de las claves.

1.5.1. Largo de vida de una clave. Como se indica en la sección 1.2.2.1, el largo de vida de una clave depende de la exposición del texto cifrado, ya que por Shannon (Communication Theory of Secrecy Systems [Sha49]) si el largo del texto plano es mayor que la clave, queda expuesta información al adversario que eventualmente podría obtener. Es recomendable entonces cifrar el texto plano de la comunicación con claves de sesión (donde podría incluso haber sesiones de tiempo limitado, y haber varias sesiones por conversación).

Esta consideración permitiría clasificar el establecimiento de claves según:

- distribución previa de claves (*de larga vida*) o,
- distribución o acuerdo de claves (*de corta vida*).

1.5.2. Posesión de la información. Otro aspecto a considerar es la conveniencia o no de la participación de un agente confiable en el establecimiento de la clave, centralizando la administración y distribución de estas. Esto depende de que la información sea propiedad del agente confiable y deba mantener control sobre la información cifrada o porque las entidades estén dispuestas a compartir la propiedad de la información cifrada confiando en su servicio como facilidad para sus operaciones.

Esto determina la elección de un esquema de distribución previa de claves de larga vida o de distribución de claves de sesión (de corta vida), donde el agente confiable o de confianza participa directamente en la generación de las claves a distribuir.

En caso contrario, ya sea por innecesario o inconveniente, puede optarse por un método donde el establecimiento de las claves se realice sin la participación directa de un agente confiable: un esquema de acuerdo de claves. En esta clase de esquema, el TA podrá participar brindando un servicio de certificación sin poder acceder a la información de las claves acordadas.

1.5.3. Cantidad de claves. La cantidad de claves a asignar a los participantes varía según la restricción de la comunicación es simétrica o asimétrica.

Distribución previa de claves (KPS): a la hora de asignar claves simétricas a ν usuarios, como se requiere una clave para cada uno de los $\binom{\nu}{2}$ pares de usuarios, la distribución previa de claves simétricas requiere un número de claves proporcional a ν^2.

Distribución de claves por sesión (SKDS): una alternativa para que el número de claves sea proporcional a ν es asignar una figura responsable que actúe como autoridad de confianza (TA), que distribuya una clave a cada uno de los usuarios. Cuando un usuario desea establecer una sesión de comunicación solicita una clave al TA. El TA genera una clave aleatoria y la entrega al par de usuarios correspondiente.

Esquema KAS STS: no requiere participación del TA durante el acuerdo de las claves, solo debe emitir los certificados. Pero requiere que ambas partes ejecuten los pasos del protocolo para determinar la clave.

En KPS Trivial: es incondicionalmente seguro y no requiere realizar cálculos para determinar la clave (deberá buscarse en una tabla de $\nu - 1$ entradas), pero el total de claves del sistema será γ proporcional a ν^2, por lo que el esfuerzo de administración también crece en ese orden.

KPS D–H: γ es proporcional a ν, el TA distribuye certificados.

ZRTP: no se requiere certificados, pero la seguridad depende de un primer reconocimiento de la voz seguro entre las partes.

SKDS Bellare–Rogaway: el TA genera la clave a demanda y la distribuye. Los usuarios tienen una clave de larga vida para comunicarse con el TA: la ventaja es que el cifrar con clave de sesión deja la clave menos expuesta.

KAS STS (estación a estación): el TA solo certifica claves públicas de los usuarios.

IBC: no hay certificados. El TA determina la clave privada que corresponde a su identidad, durante el registro. Esto requiere mayor confianza depositada en el TA.

KAS con contraseña: los usuarios pueden memorizar las claves, pero como en KPS-Trivial, las contraseñas crecen según ν^2.

1.6. Resumen

Los esquemas propuestos han sido seleccionados por su eficiencia y propiedades de seguridad demostrables matemáticamente. A grandes rasgos, estas resultan ser la distribución previa de claves trivial (KPS trivial), la distribución previa de claves Diffie–Hellman (KPS D–H), la distribución de claves por sesión Bellare–Rogaway (SKDS B–R), el acuerdo de claves estación a estación (KAS STS) y el acuerdo de claves cifrado con contraseña (KAS D–H con contraseña).

En el esquema KPS trivial, cada par de participantes debe acordar una clave de larga vida ya sea entre sí o a través de una entidad centralizada llamada autoridad confiable (TA) que las distribuya. Como la cantidad de pares crece proporcional al cuadrado del número de usuarios, la administración de las claves limita la utilización de este esquema a un número pequeño de usuarios. También requiere el cambio periódico de las claves de acuerdo a su utilización.

En el esquema SKDS B–R un TA genera las claves de cada sesión entre dos usuarios distribuyendo estas a demanda. Para ello deben contar también con una clave de larga vida con el TA, pero su uso es mucho más limitado, por lo que el período de cambio de claves puede ser más extendido. Como hay una clave por cada usuario, las claves a administrar crecen proporcionalmente al número de usuarios.

En estos dos esquemas, cuando el TA distribuye las claves, tiene la capacidad de acceder a la información y por lo tanto está en condiciones de ser su dueño.

El esquema KPS D–H, consiste en la distribución previa de certificados por parte del TA para transmitir la "parte pública" del acuerdo de claves Diffie–Hellman. El número de claves es proporcional al de usuarios y la clave de cifrado resultante es de larga vida.

En el esquema KAS STS, no se requiere la participación del TA durante el acuerdo de las clave para una conversación. Este esquema utiliza cifrado asimétrico, en el que cada participante dispone de un par (clave pública, clave privada). La clave privada será un secreto de cada usuario, pero cada usuario deberá registrar su clave pública ante el TA, que a su vez permitirá verificar al resto de los usuarios que la clave pública es auténtica, es decir que realmente corresponde al usuario supuesto.

En el esquema KAS STS al permitir que la clave privada sea un secreto de cada usuario permite que la información sea propiedad exclusiva de los interlocutores. Sin embargo, si el TA administrase las claves privadas, también será potencial propietario de la información de las conversaciones. Como en SKDS el número de claves es proporcional al número de usuarios, pero en KAS STS la administración de las claves públicas, requieren una infraestructura de clave pública adecuada para brindar documentos que certifican la autenticidad de las claves públicas que manejan los usuarios del sistema.

Si es necesario garantizar la posesión y disponibilidad de la información para un tercero (su dueño), las claves deben permanecer a su alcance. En este caso puede ser conveniente utilizar un esquema de distribución de claves de sesión SKDS en lugar de KAS (ver secciones 1.4.4 y 1.4.5).

En cambio, cuando la posesión de la información sea exclusiva de las partes en comunicación puede ser más conveniente un esquema KAS.

En el esquema KAS D–H con contraseña, la clave acordada es de corta vida, pero se requiere administrar una contraseña por cada par de usuarios, por lo que las contraseñas crecen proporcionalmente al cuadrado del número de usuarios.

1.7. Casos de uso

A la hora de decidir el esquema a utilizar para un caso particular, las coordenadas fundamentales a tener en cuenta son, la propiedad de la información cifrada, la capacidad de almacenamiento de claves y su administración, la capacidad de procesamiento de los terminales y del TA. En general se optará por cifrar con claves de sesión, por lo que a la hora de determinar si usar SKDS o KAS, deberá tenerse en cuenta que SKDS es adecuado cuando el propietario de la información es el TA, y este distribuye las claves de sesión, manteniendo así el control de las claves y por lo tanto del contenido cifrado independientemente de los interlocutores involucrados. De lo contrario aun si no hay un tercer dueño de la información, si el procesamiento de los terminales supera la capacidad requerida para realizar cifrado asimétrico, deberá usarse SKDS por clave simétrica, para evitar el crecimiento exponencial de las claves en los terminales. Cuando el procesamiento de los terminales puede soportar cifrado asimétrico, este permitirá con un manejo adecuado de la clave privada de cada usuario y de un manejo confiable de las claves públicas, establecer una comunicación confidencial punto a punto.

1.7.1. El sistema de telefonía celular GSM. La telefonía celular GSM [ETS11] es un sistema de comunicación global para comunicación telefónica móvil.

Desde el punto de vista de la seguridad se disponen las siguientes facilidades:

1. Autentificación de la identidad del usuario.
2. Confidencialidad de la identidad del usuario.
3. Confidencialidad de los datos de señalización.
4. Confidencialidad de los datos del usuario.

La seguridad de la comunicación se establece punto a punto entre cada abonado y un nodo de la red (MSC). La red consiste en operadores que despliegan sus MSC para establecer la comunicación entre sus abonados y la red. Al registrarse ante el operador, al abonado se le asigna una declaración de identidad (IMSI) y una plantilla simétrica (K_i). La autentificación del abonado corresponde al centro de autentificación del operador del abonado (CAu), que es un componente de la base de datos de registro de abonados del operador (HLR). Como no es necesario distinguir entre el abonado y el CAu, es posible utilizar una plantilla simétrica para la identificación del abonado ante la red.

El operador le entrega al abonado una tarjeta de abonado inteligente (SIM) y un equipo móvil (TM)[6]. La SIM contiene el PIN, el IMSI, el K_i y un algoritmo (de desafío y respuesta) que a partir de un desafío aleatorio (RAND) del CAu, permite calcular la respuesta SRES y la clave de sesión K_c.

El CAu contiene también una base de datos con una tabla (IMSI, K_i) y el mismo algoritmo para determinar la respuesta SRES y la clave de sesión K_c. Por lo tanto la autentificación es por desafío y respuesta y el establecimiento de claves corresponde a un esquema del tipo de acuerdo de claves simétrico, (porque la plantilla K_i es simétrica).

A los efectos de dificultar el seguimiento de la identidad del abonado a través de su comunicación con la red, una base de datos de abonados visitantes a la red (VLR), asocia una identidad temporal TMSI al IMSI.

La comunicación inalámbrica entre el teléfono móvil del abonado y la MSC se establece a través de una radiobase de la red. El equipo móvil obtiene la clave de sesión K_c de la SIM y la radiobase la obtiene del CAu del abonado. De esta forma la comunicación (de voz, datos y señalización) viaja cifrada a través del aire.

1. En el contrato se asocia una SIM con el registro de clientes del proveedor HLR.
2. El abonado tiene asociado un identificador MSI.
3. El terminal al conectarse consulta al registro de visitantes VLR.
4. El VLR envía el IMSI al HLR.

Ya sea la primera vez que realiza la conexión o por alguna razón excepcional que el VLR pierda los datos del cliente, una vez autentificado el cliente, se ejecutará un protocolo con la estación móvil.

1. SIM envía un TMSI por defecto al VLR.
2. VLR solicita el IMSI al SIM.
3. VLR realiza la autentificacón del MS.
4. VLR envía un TMSI por el canal cifrado.

El TMSI cambia en cada cambio de localización (LAI). De esta forma si cambia de VLR, el TMSI puede ser fácilmente determinado por el nuevo VLR.

1. SIM envía (LAI,TMSI) al nuevo VLR.

[6]El equipo móvil cuenta con una identificación propia (IMEI) que se usa por ejemplo para el caso de robo

2. El nuevo VLR deduce así el VLR anterior y le solicita el IMSI.

Si el usuario cambia de VLR, el nuevo VLR solicita el IMSI al VLR anterior que le transfiere las ternas sin uso al nuevo VLR.

En el Cuadro 1.7.1 se resume la relación entre los parámetros de seguridad en la red GSM.

SIM	TM	Radiobase	Registro
IMSI, K_i			IMSI, K_i
TMSI			TMSI
	K_c	K_c	

CUADRO 1.7.1. Distribución de parámetros de seguridad en la red.

1.7.2. Grupo de gerentes y un gerente general. Una empresa tiene un grupo de gerentes y un gerente general que responde ante el directorio. Utilizan conversaciones telefónicas para negociar y en algunos casos estas conversaciones no pueden quedar fuera del ámbito de los gerentes. Durante una conversación confidencial entre un gerente y el gerente general, el final de una negociación por una solicitud de inversión estratégica requiere no repudio, ya que el gerente general deberá evaluar los resultados de las negociaciones con cada gerente y presentar sus conclusiones al directorio a partir de estas. Dado que estas negociaciones pueden implicar decisiones de negocio que involucren medidas no fácilmente reversibles, se requiere que un planteo de un gerente al gerente general no pueda ser negado posteriormente. Por ejemplo que si el gerente justifica una solicitud con un argumento, no pueda luego negar haber sostenido tal argumento. Esto tanto por la posibilidad de que el gerente bajo presión no actúe honestamente, así como ante la situación de que se pueda demostrar que el gerente general no pudo confundir al gerente con otro, ya sea por accidente o incluso en una maniobra deshonesta por parte del gerente general.

Se considera que una conversación telefónica a través de un sistema cuyo software no se conecta nunca a Internet, cumple con ventajas los requisitos de seguridad necesarios planteados luego del análisis de riesgo realizado a tales efectos.

Durante una conversación mediante un botón «PRIV» se tiene la opción de pasar a una conversación confidencial entre los gerentes. Acordado el resultado del planteo, se decide dejar constancia, apretando otro botón «REG»: en ese estado se enciende una luz que indica grabación. Al indicarse fin (por ejemplo apretando nuevamente «REG»), se apaga la luz, se termina la grabación, se firma y se envía la grabación y la firma.

No se considera conveniente la privacidad de la conversación en el ámbito empresarial, por lo que para el estado «PRIV» se selecciona un esquema un esquema SKDS Bellare–Rogaway. El esquema SKDS Bellare–Rogaway cuenta con una demostración de seguridad y utiliza primitivas de criptografía simétrica, pero requiere para cada sesión un intercambio de mensajes con un TA.

El botón «REG» requiere un sistema de emisión de certificados para firmar la grabación, donde la clave privada sea de acceso exclusivo a cada gerente a los efectos de mantener las garantías del no repudio. La firma de esta parte decisiva de la conversación permite verificar la autenticidad y el no repudio.

Alternativamente, se decide que dado que existe una infraestructura de certificados para la firma, el establecimiento de claves pueda realizarse también por KAS STS,

que también tiene demostración de seguridad. El uso de criptografía asimétrica en el acuerdo de claves, permite que no sea necesario la interacción con un TA por cada sesión. Dependiendo de la situación, puede configurarse un aparato telefónico remotamente para que use KAS o SKDS. Por ejemplo en caso de auditarse un aparato por alguna razón excepcional. La empresa considera que la información de las conversaciones es de su propiedad, por lo que no se considera necesario una indicación del esquema utilizado en cualquier sesión de ese aparato telefónico.

En otro escenario posterior, debido al éxito y a la experiencia lograda con el producto, se da la oportunidad de brindar a grupos terceros un servicio de ese tipo. En ese caso la información de las conversaciones será privada para el proveedor por lo que la asignación de claves se configurará en los teléfonos únicamente por KAS STS.

Según cada caso el diseño de la PKI y los servicios que esta brinde, deberán ser cuidadosamente determinados. La verificación de revocación por los aparatos telefónicos (ver sección 1.2.10), así como la recuperación de una clave privada (por pérdida de un token, o de contraseña de acceso a esta), deberá considerarse con atención. En este último caso, quizás el acceso compartido requiriendo múltiples participantes, pueden aumentar la sensación de confianza. Sin embargo, siempre que la clave privada no sea propiedad exclusiva del usuario, es muy difícil cuantificar objetivamente el riesgo y las garantías que realmente puede brindar el sistema. La seguridad de la clave privada lleva siempre la responsabilidad y dificultad de su uso.

Capítulo 2

Primitivas criptográficas

En este capítulo se realiza una breve descripción de las primitivas utilizadas. Por más detalles, ver [Sti06], [Jud94] y [LN97].

2.1. Resumen de fundamentos matemáticos

Cuando dos enteros tienen el mismo resto en la división entera sobre m, se dice que son congruentes módulo m. Esto equivale a decir que dos números son congruentes módulo m si su diferencia es un múltiplo de m.

Definición 21. Si m es un entero positivo, se dice que dos enteros a y b son congruentes módulo m y se escribe $a \equiv b \pmod{m}$, cuando $b - a$ es múltiplo de m.

En el manejo habitual de los horarios, se trabaja considerando las horas módulo 24 o módulo 12 para el sistema "AM/PM" y se realiza la aritmética naturalmente. Análogamente se puede trabajar módulo cualquier entero positivo m. Por más detalles en la sección 1.1 de [Sti06] se brinda un resumen breve y en [Ste09] se desarrolla el tema con más detalle.

Definición 22. Se nota $\mathbb{Z}/(m)$ al conjunto de los restos módulo m: $\{0, \ldots, m-1\}$. Cuando para un elemento $a \in \mathbb{Z}/(m)$ existe un $b \in \mathbb{Z}/(m)$ tal que $ab - 1$ es múltiplo de m, se dice que a es *invertible* y que b es su *inverso multiplicativo* en $\mathbb{Z}/(m)$.

El conjunto de los invertibles módulo m, que se notará aquí como $\Phi(n)$, es igual al conjunto de los elementos de $\mathbb{Z}/(m)$ coprimos con m.

Ejemplo 2.1.1.

$$\Phi(6) = \{1, 5\}.$$

Definición 23. Una operación binaria $\cdot$ en un conjunto G es una función

$$(\cdot) : G \times G \longrightarrow G,$$

y se nota $g_1 \cdot g_2 = g_1 g_2 = (\cdot)(g_1, g_2)$.

Cuando la operación es conmutativa (que el orden de los elementos no afecta al resultado), suele usarse la notación $+$ para la operación. Por supuesto es un criterio convencional y cualquier símbolo puede ser utilizado para referirse a una operación.

Definición 24. Un *grupo* es un conjunto G no vacío con una operación binaria $(\cdot)$ que cumple las tres condiciones indicadas a continuación.

1. La operación $\cdot$ sobre G es asociativa, es decir, para cualquier $a, b, c \in G$,

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c.$$

2. Existe un elemento identidad e en G tal que para todo $g \in G$,

$$g \cdot e = e \cdot g = g,$$

3. Para cada elemento $g \in G$, existe un elemento inverso $g^{-1} \in G$ tal que

$$gg^{-1} = g^{-1}g = e.$$

Si el grupo también satisface

4. Para todo $a, b \in G$,

$$a \cdot b = b \cdot a,$$

entonces el grupo es llamado abeliano (o conmutativo).

A veces se nota $a \cdot b$ simplemente como ab. La propiedad asociativa garantiza que una secuencia de operaciones sin paréntesis no es ambigua, ya que el lugar de los paréntesis no afecta el resultado.

DEFINICIÓN 25. Un grupo es finito si tiene un número finito de elementos. Se llama *orden* de grupo finito al número de sus elementos..

Se dirá que dado un elemento $\lambda \in G$ y un entero n,

$$\lambda^n = \prod_1^n \lambda.$$

EJEMPLO 2.1.2. El conjunto de los enteros forma un grupo con la operación de adición. El 0 es la identidad y el inverso de un entero cualquiera a es $-a$. El grupo de los enteros se nota como $\mathbb{Z}$.

DEFINICIÓN 26. Un subconjunto H del grupo G es un subgrupo de G si H es un grupo respecto la operación de G. Los subgrupos de G que no sean subgrupos triviales ($\{e\}$ y G) son llamados subgrupos no triviales de G.

DEFINICIÓN 27. Las potencias de un elemento λ de un grupo forman un subgrupo $\langle\lambda\rangle$. En ese caso λ es un generador de $\langle\lambda\rangle$ y se dice que $\langle\lambda\rangle$ es un grupo cíclico generado por λ. Si el grupo cíclico generado por λ es finito, su número de elementos se denomina *orden* de λ.

Un grupo cíclico puede tener más de un elemento generador. Por ejemplo el grupo aditivo $\mathbb{Z}$ tiene a 1 y a -1 como generadores.

EJEMPLO 2.1.3. $(\Phi(6), \cdot)$ es un grupo cíclico. En efecto $\Phi(6) = \Phi(5)$, ya que módulo 6, $5 \equiv -1 \pmod 6$.
$(\Phi(12), \cdot)$ no es un grupo cíclico. $11 \equiv -1 \pmod{12}$ y $5^2 \equiv 7^2 \equiv 1 \pmod{12}$
En $(\Phi(15), \cdot)$ que tampoco es cíclico, $\langle 2\rangle = \{2, 4, 8, 1\}$ y $\langle 7\rangle = \{7, 4, 13, 1\}$.

DEFINICIÓN 28. Un cuerpo $(F, +, \cdot)$ es un conjunto F, con dos operaciones binarias, tales que:

1. F es un grupo abeliano respecto la operación $\cdot$.
2. El conjunto de los elementos de F distintos de 0, $F^* = F \setminus \{0\}$, forma un grupo con la multiplicación $\cdot$.
3. $\cdot$ es conmutativa.
4. Se cumplen la ley distributiva; es decir, para todo $a, b, c \in F$, se cumple

$$a \cdot (b + c) = a \cdot b + a \cdot c.$$

Un ejemplo de cuerpo finito es el conjunto $\{0, 1, \ldots, p-1\}$ junto con la suma y el producto módulo p, *llamado cuerpo de Galois de orden* p y se nota F_p. Se destacan algunas propiedades a recordar.

PROPOSICIÓN 2.1.1. Si F es un cuerpo finito con q elementos, entonces todo $a \in F$ cumple $a^q = a$.

TEOREMA 2.1.1. *Para cada cuerpo finito* F_q *el grupo multiplicativo* F_q^* *de elementos no cero de* F_q *es cíclico.*

Así como es posible extender el cuerpo de los números reales $\mathbb{R}$, agregando un nuevo elemento que sea raíz del polinomio $x^2 + 1$ y obtener así el cuerpo de los números complejos, representable por $R \times R$, es decir, el plano complejo; es posible extender un cuerpo finito F_p con p primo, para lograr un cuerpo finito de p^m elementos, donde m es el grado de un polinomio sin raíces en el cuerpo F_p.

2.2. Logaritmo discreto y factorización

Ciertos grupos finitos cíclicos de orden muy grande[1], tienen la propiedad de que las potencias de un elemento λ no siguen un patrón reconocible, es decir, que dados el elemento λ y una potencia elegida al azar, no habría un algoritmo mucho mejor para encontrar el exponente correspondiente, que realizar una búsqueda exhaustiva, es decir recorrer todos los exponentes hasta encontrar la potencia en cuestión.

DEFINICIÓN 29. Sea $\lambda \in G$ donde $(G, \cdot)$ es un grupo. El *logaritmo discreto* de una potencia de λ es la función que permite determinar el exponente correspondiente.

El *problema del logaritmo discreto* consiste en calcular, dados un grupo cíclico $\langle\lambda\rangle$ y un elemento cualquiera de él α elegido al azar, el exponente $a \in \mathbb{Z}$ tal que $\alpha = \lambda^a$.

2.2.1. El problema computacional de Diffie–Hellman (CDHP). El *problema computacional de Diffie–Hellman* refiere a la situación modelada en el establecimiento de claves Diffie–Hellman. Dado un grupo cíclico $\langle\lambda\rangle$ ambas partes Ana y Ben determinan su propio exponente secreto elegido al azar y calculan su potencia correspondiente. Digamos que Ana elige el exponente a y determina $\alpha = \lambda^a$ y Ben elige el exponente b y determina $\beta = \lambda^b$. Para determinar la clave, Ana y Ben comparten sus potencias públicamente y calculan $\alpha^b = \beta^a$ que utilizan como clave[2].

DEFINICIÓN 30. Dado un grupo con operador multiplicativo y un elemento λ en él, sean dos potencias $\alpha = \lambda^a$ y $\beta = \lambda^b$, donde los exponentes son secretos.

El *problema computacional de Diffie–Hellman* $\mathrm{CDHP}(\lambda, \alpha, \beta)$ consiste en hallar la potencia λ^{ab}.

En un grupo aditivo y un elemento P en él, dados dos productos aP y bP el problema CDHP consiste en obtener abP.

Una forma obvia de resolver este problema es calculando el logaritmo discreto en el caso multiplicativo o los factores en el caso aditivo, para obtener a y b. Por lo tanto CDHP no es más difícil de resolver que el problema del logaritmo discreto.

[1] Un área de investigación que permite aumentar la disponibilidad de grupos cíclicos, es la de las curvas elípticas sobre cuerpos finitos.

[2] este no es un protocolo de establecimiento de claves seguro como veremos más adelante.

2.2.2. El problema de decisión Diffie–Hellman (DDHP). El *problema de decisión de Diffie-Hellman* consiste en obtener información parcial de la solución CDHP. Si el adversario pudiera, a partir de los tres parámetros de entrada, obtener varios bits del resultado, el establecimiento de claves Diffie–Hellman no sería hermético, ya que un adversario pasivo podría obtener información de la clave de los usuarios observando el intercambio de claves públicas.

Dado un grupo con operador multiplicativo y un elemento λ en él, sean dos potencias λ^a y λ^b. El problema de decisión DDHP consiste en que dada una potencia cualquiera elegida de $\langle\lambda\rangle$, determinar si es o no cierto que sea igual a λ^{ab}.

Cuando en la presentación de un esquema de seguridad se indica que está basado en el problema del logaritmo discreto, muchas veces se da por entendido la utilización de los problemas CDHP y DDHP.

2.2.3. El problema de factorización. Otro problema del cual se conjetura no existe una solución viable, es el problema de factorización de un número entero *compuesto*. En efecto, todo número entero es unidad (1 o -1), 0, primo o producto de primos. Sin embargo aún cuando un número sea el producto de solo dos primos, es posible seleccionarlos de tal forma que *se conjetura sería* inviable factorizarlos. El problema RSA, es un problema que está basado en la inviabilidad del problema de la factorización.

2.2.4. Definiciones.

Definición 31. *Texto original (plaintext)* es la información para la cual el cifrado provee privacidad. Un algoritmo de cifrado toma el texto original y una clave como entradas y produce un texto cifrado como salida.

Definición 32. *Texto cifrado (ciphertext)* es la salida de un algoritmo de cifrado.

Definición 33. *Cifrado (encryption)* toma texto original y una clave como entradas y produce texto cifrado como salida.

Definición 34. *Descifrado (decryption)* toma el texto cifrado y una clave como entradas y produce texto original como salida.

Definición 35. *Clave criptográfica* es un valor que define la operación de cifrado o descifrado. Los valores usados para todos los usuarios del sistema criptográfico se llaman parámetros. El cifrado IBC dispone de un conjunto de parámetros públicos.

Definición 36. *Clave asimétrica o pública* es un cifrado que usa dos claves relacionadas: una pública y otra privada, tal que dada la clave pública es inviable obtener la clave privada.

Definición 37. *Cifrado aleatorio* es uno que requiere un número aleatorio como entrada además del texto original y la clave.

TA: es la entidad confiable, responsable de la administración y de la distribución de información.

Ana: es la identidad de la primera usuaria del canal.

"Ana": es el nombre de Ana expresado como cadena de bits.

Ben: es la identidad del segundo usuario del canal.

"Ben": es el nombre de Ben expresado como cadena de bits.
Omar: es la identidad del atacante.
$\lceil x \rceil$: es el menor entero mayor que x.
$\Phi(n)$: es el conjunto de enteros positivos menores que n que son coprimos con n. Si p es primo $\Phi(p) = \{1, \ldots, p-1\}$.
$\varphi(n)$: es el número de elementos de $\Phi(n)$.
$e_K(m)$: cifrado de m con la clave K.
$d_K(c)$: descifrado de c con la clave K.
$mac_K(m)$: resumen (hash) cifrado con clave simétrica K del mensaje m.
$sig_U(m)$: firma del usuario U del mensaje m.
$ver_U(s)$: verificación de la firma s del usuario U.
ver_U: clave pública del usuario U.
KPS: (Key Predistribution Scheme), esquema de distribución previa de claves.
SKDS: (Session Key Distribution Scheme), esquema de distribución de claves de sesión.
KAS: (Key Agreement Scheme), esquema de acuerdo de claves.
IBC: (Identity Based Cryptography), cifrado basado en la identidad.
$\oplus$: operación o exclusivo (XOR) bit a bit.
$\|$: operación que une de forma secuencial dos cadenas de bits.

DEFINICIÓN 38. Un algoritmo aleatorio se dice *Las Vegas* si como salida puede responder "falla" o responder un resultado correcto. Un algoritmo es (ϵ, Q) si es un algoritmo aleatorio *Las Vegas*, tal que disponiendo de Q intentos, la probabilidad promedio de éxito no supera ϵ.

2.3. Seguridad del cifrado

Usualmente, la seguridad de un cifrado se clasifica según los requerimientos que se indican a continuación.

Ataque con solo texto cifrado: el adversario tiene acceso solo a texto cifrado, es el ataque más difícil para un adversario, y cualquier criptosistema debe ser resistente a ese tipo de ataques para brindar cierto nivel de seguridad.

Ataque con texto original conocido: el adversario tiene acceso al texto original y al texto cifrado correspondiente, no necesariamente para todo el mensaje cifrado. El adversario tiene mucha ventaja y cualquier criptosistema debería proteger contra este tipo de ataque. Muchos mensajes con formato, permiten una fácil realización de este ataque.

Ataque de texto original elegido: el adversario puede elegir un texto original y obtener el cifrado correspondiente. Así podría obtener una tabla que represente la función de cifrado. Una forma de contrarrestarlo es incluir información aleatoria en el texto original a cifrar, de tal forma que un mismo mensaje podrá ser cifrado en diferentes resultados de texto cifrado cada vez.

Ataque de texto original elegido adaptativo: aquí el adversario selecciona el texto original a cifrar en función del resultado cifrado anterior.

Ataque de texto cifrado elegido: el adversario selecciona texto cifrado y puede obtener el texto original correspondiente. Si un algoritmo cifra el mismo texto

original al mismo texto cifrado (el resultado del cifrado no es aleatorio) es susceptible a este tipo de ataque. Cualquier criptosistema de clave pública debería tolerar e ste tipo de ataque.

Ataque de texto cifrado elegido adaptativo: el adversario selecciona texto cifrado según el resultado anterior.

2.4. El esquema RSA de cifrado asimétrico

En RSA (ver sección 5.3 de [Sti06]) se seleccionan dos primos p, q secretos y distintos, donde la factorización de su producto se considere inviable. Entonces se calcula y hace público $n = pq$. Se cumple que $\varphi(n) = (p-1)(q-1)$. Entonces, se elige un entero aleatorio b tal que tenga un inverso módulo $\varphi(n)$. Luego se calcula, aplicando el algoritmo extendido de Euclides (ver [Ste09]), un entero a tal que

$$ab \equiv 1 \pmod{\varphi(n)}.$$

La clave pública es el par (n, b) y la clave privada (p, q, a). Las funciones de cifrado $e_K(x)$ y descifrado $d_K(y)$ se definen como:

$$e_K(x) \equiv x^b \pmod{n},$$
$$d_K(x) \equiv x^a \pmod{n}.$$

El número b se llama exponente de cifrado y el número a exponente de descifrado.

2.4.1. La transformada de Fujisaki–Okamoto. Esta transformada transforma un cifrado de clave pública débil en uno que es seguro contra ataques de texto cifrado elegido.

Sea $E(P, X, R)$ un algoritmo de clave pública aleatorio que cifra el texto plano X usando una entrada aleatoria R y la clave pública P. Sea D la función de descifrado correspondiente a E y sean H_1 y H_2 funciones de *hash* criptográficas. Entonces para cifrar un mensaje M el cifrado E' es resistente a ataques de texto cifrado elegido:

$$E'(P, M, R) = (C_1, C_2) = C$$

Donde:

$$C_1 = E(P, R, H_1(R, M))$$
$$C_2 = H_2(R) \oplus M$$

Para descifrar el mensaje:

$s = D(C_1)$

$M = H_2(s) \oplus C_2$

$r = H_1(s, M)$ verificar que $C_1 = E(P, s, R)$. Si no es cierto, elevar error y terminar.

M es el resultado del descifrado de C.

2.5. Funciones hash

En la práctica un mensaje contiene mucha información redundante y es posible extraer una *huella* (con un largo de bits fijo y relativamente pequeño) del mensaje, de tal forma que cualquier pequeña modificación genere una huella totalmente distinta. Una función inversa de la huella de un mensaje debería ser difícil de deducir a partir de

la observación de sus resultados. La probabilidad de que dos mensajes distintos tengan la misma huella debería ser despreciable.

Una huella puede además requerir el conocimiento de una clave para obtener su resultado. En criptografía (ver sección 4.2 de [Sti06]), estas funciones huella se denominan *hash*.

DEFINICIÓN 39. Una familia (*hash*) es una cuaterna (X, Y, K, H) tal que:

1. X es el conjunto de los mensajes posibles
2. Y es un conjunto finito de huellas posibles
3. K es el conjunto de claves posibles
4. Para cada clave k de K, existe una función *hash* en H, h_k que va de X a Y.

DEFINICIÓN 40. Se elige una función *hash* con entradas x_1 y x_2 y salidas y_1 e y_2. Entonces H es una función *hash criptográfica* si su cálculo es eficiente y tiene las tres propiedades siguientes.

resistencia a colisiones: es difícil hallar x_1, x_2 distintos y que $H(x_1) = H(x_2)$,

resistencia a preimagen: dado cualquier y_1 es difícil encontrar un x_1 con $y_1 = H(x_1)$,

resistencia a segunda preimagen: dado un x_1 con $y_1 = H(x_1)$ es difícil encontrar un x_2 distinto a x_1 e $y_1 = H(x_2)$.

Una función MAC es un hash que depende de una clave (ver sección 4.4 de [Sti06]). A continuación se define la seguridad de una función MAC.

El objetivo de un adversario es obtener un MAC válido de un mensaje sin conocer la clave. Sea x el mensaje particular e y su MAC correspondiente.

El adversario puede observar una secuencia $(x_1, y_1) \dots (x_Q, y_Q)$ de pares válidos de otros mensajes $(x_i \neq x)$. Si el adversario logra obtener (x, y) a partir de Q observaciones (x_i, y_i), habrá logrado una falsificación.

DEFINICIÓN 41. Diremos que una MAC es segura–(ϵ, Q) si a partir de Q MAC, la probabilidad promedio de lograr una falsificación es menor que ϵ. Un adversario que puede tiene probabilidad ϵ o mayor de realizar una falsificación a partir de Q observaciones, será un falsificador–(ϵ, Q).

2.6. Esquemas de firma digital

La firma a mano se adjunta a un documento almacenado en papel para indicar su responsable. Un esquema de firma (digital) es un método de firmar un mensaje almacenado en forma electrónica, es decir almacenado como una sucesión de bits. Sin embargo, una firma digital no queda adjunta al mensaje y su verificación debe realizarse mediante un algoritmo público.

Además todas las copias de una firma digital son exactamente iguales a la original, por lo que el concepto de firma original no es aplicable para habilitar una transacción basada en que una firma es la original.

Un esquema de firma consiste en un algoritmo de firma $sig_K()$ (privado) que depende de la clave privada K y un algoritmo de verificación (público) asociado a la clave privada.

DEFINICIÓN 42. Un esquema de firma es una tupla (P, A, K, S, V) donde se cumple:

1. P es un conjunto finito de mensajes

2. A es un conjunto finito de posibles firmas
3. K es un conjunto finito de posibles claves
4. S es el conjunto de funciones de firma
5. V es el conjunto de funciones de verificación
6. Para cada clave $k \in K$, existe un algoritmo de firma en S y un correspondiente algoritmo de verificación en V. La firma es una función de P sobre A y la verificación es una función de $P \times A \to \{verdadero, falso\}$, que compara la firma con el mensaje de tal forma que si corresponden, el resultado será verdadero o, de lo contrario, falso.

DEFINICIÓN 43. Diremos que un esquema de firma es seguro–(ϵ, Q) si, a partir de la disponibilidad de Q firmas, la probabilidad promedio de falsificarla no supera ϵ.

2.7. Modelo de confianza de certificación

En el conjunto de entidades $\mathcal{E}$ se define una función $\gamma : \mathcal{E} \to \mathbb{N}$, que representa el nivel de autoridad de confianza de la entidad. La propiedad de autoridad de confianza refiere al total de certificados que, directamente o indirectamente a través de otras autoridades de confianza, están firmados por él. El rol de autoridad de confianza, corresponde al TA. La autoridad de certificación (CA) no constituye por sí sola una autoridad de confianza.

Γ_A indica el nivel autoridad de confianza depositada en A.

En el conjunto de los pares ordenados de $\mathcal{E} \times \mathcal{E}$ se toma un subconjunto que define una relación $\mathcal{R}$ entre ellos de tal forma que $(A, B) \in \mathcal{R}$ cuando se cumple que $\Gamma_A \geqslant \Gamma_B$.

Se cumple que $\mathcal{R}$ es una relación de orden entre los niveles de confianza depositados a las entidades certificadoras. En efecto: $\Gamma_A \geqslant \Gamma_A$, ya que en un mismo nivel jerárquico de confianza A puede certificar su propia muestra. Si $\Gamma_A \geqslant \Gamma_B$ y $\Gamma_B \geqslant \Gamma_A$ entonces están en un mismo nivel de confianza es decir: $\Gamma_A = \Gamma_B$. Si $\Gamma A \geqslant \Gamma_B$ y $\Gamma_B \geqslant \Gamma_C$ entonces $\Gamma_A \geqslant \Gamma_C$.

Si el nivel de confianza de A le permite certificar a B indicamos por $\Gamma_A \geqslant \Gamma_B$,

DEFINICIÓN 44. Una relación de confianza es una relación de orden $\geqslant$ entre las entidades certificadoras tal que $A \geqslant B$ cuando A puede emitir un certificado a B.

Esta relación permite establecer niveles de confianza de jerarquía creciente y también un camino de confianza entre varios agentes confiables.

2.8. Criptografía basada en identidad

Sea $G = \langle g \rangle$ de orden p primo, por ejemplo un grupo de puntos en una curva definida en un cuerpo finito y G_t un grupo de orden p, por ejemplo un subgrupo multiplicativo en alguna extensión del cuerpo.

Supongamos que no es viable obtener un homomorfismo de $G_t \to G$.

Sea $e : G \times G \to G_t$ bilineal, es decir que cumple: $\forall u, v \in G$, $\forall a, b \in \mathbb{Z}$,

$$e(u^a, v^b) = e(u, v)^{ab}$$

donde $\langle e(g, g) \rangle = G_t$.

Además, suponemos que las operaciones sobre G, G_t y e son calculables eficientemente.

Decimos entonces que G es un grupo bilineal y que el mapa e es simétrico bilineal (o pairing) en el grupo G. La simetría refiere a la invarianza del mapa bilineal al intercambiar sus argumentos.

Consideremos que la identidad del destinatario "ID" consiste en una cadena arbitraria de bits $\{0,1\}^*$, que el mensaje a cifrar M es de longitud fija l y los cuatro hashes criptográficos:

$$H_1 : \{0,1\}^* \to G \text{ (de la identidad en G)},$$
$$H_2 : G_t \to \{0,1\}^l \text{ (para aplicar xor con la clave de sesión)},$$
$$H_3 : \{0,1\}^l \times \{0,1\}^l \to \mathbb{Z}/(p),$$
$$H_4 : \{0,1\}^l \to \{0,1\}^l \text{ (para hacer xor con el texto en claro)}.$$

Entonces el esquema consiste en:

2.8.1. Inicialización.

$$w = \text{rand}(p),$$
$$g_{pub} = g^w,$$
$$(g, g_{pub}) \in G^2 \text{ son los parámetros públicos (params)},$$
$$w \in \mathbb{Z}/(p) \text{ es la clave maestra (masterkey)}.$$

2.8.2. Extracción. El remitente "ID" tramita su clave privada d_{ID} con el TA, que calcula:

$$h_{ID} = H_1(ID),$$
$$d_{ID} = (h_{ID})^w \in G.$$

2.8.3. Cifrado. El remitente desea enviar el mensaje $M \in \{0,1\}^l$ al destinatario identificado por $ID \in \{0,1\}^*$.

$$s = \text{rand}(\{0,1\}^l),$$
$$h_{ID} = H_1(ID),$$
$$y_{ID} = e(h_{ID}, g_{pub}),$$
$$C = (g^r, s \oplus H_2(y_{ID}^r), M \oplus H_4(s)) \in G \times \{0,1\}^l \times \{0,1\}^l.$$

2.8.4. Descifrar.

$$C = (u, v, w),$$
$$s = v \oplus H_2(e(u, d_{ID})),$$
$$M = w \oplus H_4(s),$$
$$r = H_3(s, M).$$

El esquema de cifrado es consistente, en efecto:

$$e(u, d_{ID}) = e(g^r, h_{ID}) = e(g, h_{ID})^r,$$
$$y_{ID}^r = e(h_{ID}, g^w)^r = e(h_{ID}, g)^{wr}.$$

Al descifrar el resultado M se considera válido si $g^r = u$.

Este resumen sigue la línea de [Boy06].

Capítulo 3

Esquemas de realización

3.1. Modelo de ataque y objetivos del adversario

El objetivo de un esquema de establecimiento de claves es intercambiar información que permita a las partes involucradas determinar la clave, sin que un tercero pueda obtener alguna información de esta.

El atacante no debería alterar la información ni los destinatarios en el desarrollo de una sesión protocolo, ni obtener información secreta de este.

La información secreta (por ejemplo una contraseña, una clave o la plantilla en un esquema de identificación) que sea posible obtener de una sesión por parte de un atacante debería ser nula. Un esquema que cumple con este requerimiento se dice *hermético*, (en inglés *zero knowledge scheme*).

Además un esquema debería ser sencillo y eficiente como para ser realizado en una tarjeta inteligente.

3.1.1. Seguridad de las claves. El tiempo de validez de uso de una clave (su largo de vida) es un aspecto importante en la seguridad de un esquema.

Definición 45. Se dice que una clave es de *larga vida* (en inglés *long lifetime*, LL key), cuando su uso en el tiempo es prolongado.

Como se indica en la sección 1.5.1, la clave debe ser lo menos expuesta posible a un posible adversario.

En ese sentido, es preferible utilizar claves de sesión de corta vida (en inglés *short lifetime session keys*). En general las claves deberían ser establecidas de forma aleatoria en cada oportunidad (independientemente de su duración).

Se debe tener en cuenta también el almacenamiento de las claves de larga vida. Naturalmente un esquema donde las claves crecen con los pares de usuarios puede hacerse muy difícil de administrar a medida que el número de usuarios aumenta. Por ejemplo para 10 usuarios habrá 45 pares. Si n es el número de usuarios, los pares crecerán proporcionalmente a n^2. El adversario podría deducir una clave de sesión o una clave de larga vida.

Definición 46. Se dice que se realiza un *ataque con clave de sesión conocida* (en inglés *known session key attack*) cuando un adversario, conociendo una clave de sesión, intenta deducir otras claves de ya sean de sesión o de larga vida.

Definición 47. Se dice que se realiza un *ataque con clave de larga vida conocida* cuando un adversario conoce la clave de larga vida.

Esto obliga a reiniciar totalmente el esquema. De lo contrario, las claves establecidas a partir de ese momento carecerán de garantías.

DEFINICIÓN 48. Se dice que un esquema tiene la propiedad de secreto perfecto a futuro (en inglés *perfect forward secrecy*) cuando aún conociendo la clave de larga vida el atacante no es capaz de deducir las claves de sesión que fueron emitidas previamente.

En este caso, si el atacante no dispone el resto de los parámetros de la sesión con que fue generada, cuando se establece una clave de sesión, la seguridad de la clave permanecerá aún cuando más adelante se obtuviese la clave de larga vida con la que fue generada.

3.1.2. Seguridad de un protocolo. Como se describe en la introducción, si se dispone de un canal digital establecido a través de la línea telefónica, debe distinguirse una cadena de bits que solo puede ser generada por una persona en particular (su plantilla). Si esa cadena de bits viaja por un canal inseguro, puede ser interpretada. *Por lo tanto, debe existir un conocimiento secreto entre las partes que no viaja por el canal inseguro y que permitirá reconocer la identidad.*

DEFINICIÓN 49. Un *protocolo* es una secuencia donde a cada paso del protocolo le corresponde un flujo de información entre las entidades participantes.
Se llama *sesión* a una instancia de un protocolo.

La información de un flujo en un protocolo consiste en una o varias variables que lo componen. El flujo no debería ser predecible ni poder ser reutilizado fuera del paso que corresponde en el protocolo. Para evitarlo, se recurre a agregar componentes aleatorias y a disponer en en los flujos de pasos distintos una estructura particular, por ejemplo, en la cantidad de variables que lo componen.

3.1.3. Esquemas de identificación. Un esquema de identificación brinda un mecanismo que permite, a demanda y en el momento en que se solicita (en "tiempo real"), verificar una identidad ante un verificador a través de un canal inseguro (ver [Sti06] sección 9.1). Enviar la identidad relativa declarándola propia no es suficiente, ya que la identidad relativa permite verificar la *declaración de identidad*, pero no la plantilla que es necesaria para determinar la *identidad virtual*, sin la cual no se puede determinar la identidad de acuerdo al modelo presentado en el primer capítulo.
Es necesario entonces un mecanismo que demuestre al verificador el conocimiento o posesión de la *plantilla* por parte del verificado. Esta prueba de conocimiento deberá ser tal que no revele información de la *plantilla*. La secuencia de pasos para realizar el intercambio de información requerida por el esquema se denomina *protocolo*. Cada paso de dicho protocolo deberá ser inutilizable posteriormente. De lo contrario, su reutilización permitiría, en otro paso de la misma o en otra sesión, usurpar una identidad.

3.1.4. Seguridad de un esquema de identificación. En un protocolo de un esquema de identificación se verificará el cumplimiento de las condiciones previstas en el esquema, para evitar la posibilidad de un ataque exitoso. *Solo si estas condiciones se cumplen, se aceptará la identificación.*

DEFINICIÓN 50. Un participante *honesto* cumple con el esquema, realiza los cálculos correctamente y no revela información al adversario.

DEFINICIÓN 51. Un adversario es pasivo si solo recaba la información que fluye entre los participantes durante el protocolo de establecimiento.

Definición 52. Un adversario es activo si, durante el protocolo de establecimiento, logra introducir un mensaje, cambiar un mensaje o cambiar el destinatario de un mensaje.

Un adversario activo puede tomar el lugar del otro participante legítimo o del TA e interceptar y cambiar mensajes del esquema. El objetivo de un adversario (llamado en adelante Omar) es lograr que un participante *honesto* (que respeta el esquema) acepte la identificación en una sesión donde él es activo. Como modelo de ataque el adversario puede intentar dos fases, una previa de recolección de información (pasiva) y luego intentar (participando activamente) engañar al verificador. La recolección de información realizada por Omar puede lograrse actuando como observador pasivo pero también durante su participación activa.

En una sesión de un protocolo de un esquema de identificación, se pretende probar la posesión de un conocimiento (la plantilla, ver Definición 8) de tal forma que su resultado indique la autenticidad.

Definición 53. Se dirá que una variable es *lógica* o *booleana*, cuando puede tomar dos valores que representan "Falso" o "Verdadero". Una función se dirá *booleana* si toma y devuelve valores booleanos.

Una afirmación cualquiera, por ejemplo un teorema, es una proposición lógica y por lo tanto una variable booleana. En principio esta variable p tiene un valor desconocido y la prueba consiste en determinar su valor.

Definición 54. Un prueba [Pan08] es una función booleana que es:

Completa: cuando a toda entrada verdadera le corresponde un resultado verdadero.

Consistente: cuando a una entrada falsa le corresponde un resultado falso.

Definición 55. Una prueba de identificación es *completa* cuando su resultado final permite verificar la identidad en cuestión.

Definición 56. Una prueba de identificación es consistente (*soundness* [Sti06]) cuando usurpar una identidad implica conocer la *plantilla*.

Definición 57. Un *esquema de identificación* es un esquema que permite a alguien con una información secreta (la plantilla) convencer a otra parte de su conocimiento.

Si un adversario pudiera realizar con éxito la condición impuesta por una prueba interactiva de identificación, sería capaz de *usurpar* la identidad con una probabilidad no despreciable.

Definición 58. Una prueba de identificación es una *prueba de conocimiento* (en inglés *proof of knowledge* [Sti06]) si es una prueba de identificación completa y consistente.

Definición 59. Una prueba de conocimiento es *hermética* (en inglés *zero proof of knowledge* [Sti06]) si no revela información del secreto (la plantilla) durante su ejecución.

Definición 60. Una prueba de conocimiento es *segura* si es una prueba de conocimiento hermética.

DEFINICIÓN 61. Una prueba de identificación es consistente–(p, n) cuando usurpar una identidad luego de observar hasta n sesiones, implica conocer la *plantilla* con mayor probabilidad que p.

DEFINICIÓN 62. Una *prueba de conocimiento*–(p, n) es una prueba de identificación que es completa y consistente–(p, n).

DEFINICIÓN 63. Una prueba de conocimiento será *hermética*–(p, n) si en una cantidad n de sesiones de la prueba, la probabilidad de que la información revelada sea suficiente para obtener el secreto (la plantilla) es menor que p.

DEFINICIÓN 64. Una prueba de conocimiento es *segura*–(p, n) si es una prueba de conocimiento–(p', n') y hermética–(p'', n'') y $p' \leqslant p$, $p'' \leqslant p$, $n' \geqslant n$, $n'' \geqslant n$.

La seguridad de un esquema de identificación estará dada por la seguridad de la prueba que utilice.

EJEMPLO 3.1.1. Sea Omar un participante cualquiera que quiere autentificarse como Ana ante Ben.

1. Si Omar tiene la plantilla de Ana, la prueba de conocimiento *debería* aceptarse por parte de Ben, es la *completitud* de la prueba.
2. Si Omar puede lograr que Ben lo acepte en la prueba de conocimiento interactiva, esto *debería* implicar que Omar tiene la plantilla de Ana, es la *consistencia* de la prueba.
3. Si Omar no puede obtener información de la plantilla de Ana, a partir de sesiones en las que participa Ana, es el *hermetismo* de la prueba. Omar puede recopilar información como observador pasivo o activamente, intentando establecer sesiones con Ana.

3.1.5. Objetivo del adversario. En un esquema de establecimiento de claves, un atacante activo podría:

1. alterar mensajes que observe en el canal,
2. guardar mensajes para reutilizarlos más adelante,
3. intentar usurpar la identidad de usuarios o entidades de la red.

El objetivo del adversario sería:

1. engañar a los participantes en aceptar una clave falsa, por ejemplo una clave del pasado que ha perdido validez o una clave elegida por el adversario,
2. hacer creer al menos a uno de los participantes de haber intercambiado una clave con el otro cuando no ha sido así,
3. determinar cualquier información sobre la clave establecida.

En algunas demostraciones de seguridad de los esquemas de identificación o establecimiento de claves, es posible que se considere obvia la completitud y que la consistencia y el hermetismo se deduzcan probando que un atacante activo o pasivo no puedan alterar ni obtener información de una o varias sesiones.

Resumiendo, el objetivo de una sesión de un esquema de distribución o acuerdo de claves es que, al final de la sesión del esquema, ambas partes involucradas en la sesión obtengan la misma clave y su valor sea totalmente desconocido por cualquier otra parte (excepto cuando así esté previsto que le corresponda al TA). Cuando estos

esquemas requieran el establecimiento autentificado de claves, deberán ser esquemas de identificación seguros.

3.2. Esquemas de identificación *por desafío y respuesta*

Los esquemas de identificación por desafío y respuesta (*Challenge and Response*) que se describen a continuación constituyen una clase de algoritmos que sustentan su seguridad en primitivas criptográficas cuya seguridad ya está establecida previamente en las hipótesis.

3.2.1. Identificación por desafío y respuesta con *clave simétrica*. Este esquema consiste en comprobar la identidad entre dos participantes, donde el nombre del verificador es Ben y Ana es el nombre de quien desea identificarse. A esos efectos (ver Protocolo 3.2.1), Ben elige un desafío aleatorio r de w bits y lo envía a quien debe reconocer. Cuando Ana recibe el desafío de Ben responde con la MAC del valor ("Ana" $\|$ r), obteniendo $\text{mac}_K(\text{"Ana"} \| r)$. (Utilizando la clave simétrica K compartida previamente entre Ana y Ben).

Suponemos que la MAC es segura–(ϵ, Q) (ver la Definición 41). Por lo tanto el atacante (Omar), puede recopilar Q MACs e intentar un ataque a la MAC con una probabilidad no mayor que ϵ. Pero independientemente a las características de seguridad de la MAC, Omar podría tener la suerte de que entre los Q MACs recuperados de sesiones anteriores para valores ("Ana" $\|$ r_i), elija uno que coincida con el desafío actual r. Pero como los r son aleatorios, la probabilidad en este caso es $Q/2^w$.

1. Ben : $r = \text{rand}(2^w)$, $\quad r \longrightarrow$ Ana.
2. Ana : $u = \text{mac}_K(\text{"Ana"} \| r)$, $\quad u \longrightarrow$ Ben.
3. Ben : $u^* = \text{mac}_K(\text{"Ana"} \| r)$, acepta si $u = u^*$.

PROTOCOLO 3.2.1. Desafío y respuesta con clave simétrica.

El tamaño w en bits de r permite mantener baja la probabilidad de reutilización de la respuesta (2^{-w}). La respuesta debe contener el nombre de Ana para que solo pueda reutilizarse respuestas emitidas por ella.

$$\begin{aligned} \text{Ana} &\xleftarrow{\quad r \quad} \text{Ben}, \\ \text{Ana} &\xrightarrow{\quad u \quad} \text{Ben}. \end{aligned}$$

DIAGRAMA 3.2.1. Desafío y respuesta con clave simétrica.

La seguridad del protocolo se mide como la probabilidad máxima de que, luego de cierto número Q de sesiones en que Omar es pasivo y observa Q MACs, al pasar Omar a ser activo en una sesión, engañe a Ben logrando que la acepte cuando debería rechazarla. Se asumen MACs seguras–(ϵ, Q), es decir que la probabilidad de falsificarlas a partir de observar Q no es mayor a ϵ. Se dice que un esquema es seguro–(p, n) si en n sesiones la probabilidad de un ataque exitoso no es mayor a p (ver sección 2.5 y [Sti06] sección 4.2.2).

3.2.1.1. Estimación de una cota de probabilidad en la unión de sucesos. Cuando dos sucesos son muy poco probables [PM08] (como se establece al definir los parámetros de seguridad de los esquemas en criptografía), la probabilidad de que ocurra uno u otro (su unión) es la suma de cada uno menos la probabilidad de su ocurrencia simultánea (su intersección). Ya sea que los procesos sean independientes o que difícilmente ocurran simultáneamente, se considerará que la suma de las probabilidades es una buena cota del peor caso. También cuando tengo varios intentos que pueden resultar en éxito o fracaso (intentos de Bernoulli), e interesa calcular la probabilidad de tener éxito en Q intentos y la probabilidad p de éxito es muy baja se cumple:

$$\Pr\left[\text{algún éxito en Q intentos}\right] = 1 - \Pr\left[\text{no tener ningún éxito}\right] = 1 - (1-p)^{Q} \approx Qp.$$

TEOREMA 3.2.1. *Utilizando un MAC seguro–(ϵ, Q), si los desafíos son aleatorios y de w bits, el esquema de identificación «Desafío y respuesta con clave simétrica» es seguro–$(Q/2^w + \epsilon,\ Q)$.*

DEMOSTRACIÓN. La prueba de conocimiento es completa, ya que si Omar conoce la clave K, podrá usurpar la identidad de Ana con probabilidad 1.

Para probar que la prueba de conocimiento es consistente–$(Q/2^w + \epsilon, Q)$, supongamos que Omar logra usurpar la identidad de Anaen Q intentos con probabilidad mayor a $Q/2^w + \epsilon$, haciendo que Ben haya aceptado en alguna de esas Q sesiones y por tanto observando Q MACs. Si Omar obtuvo el valor de u, solo pudo haberlo hecho reutilizando o falsificando u. La probabilidad de reutilización no puede ser mayor que $Q/2^w$ por ser el desafío aleatorio y de w bits.

Entonces la probabilidad de reutilización de Omar es mayor que ϵ, pero esto no es posible por hipótesis.

Para probar que la prueba de conocimiento es hermética–$(\epsilon,\ Q)$, observar que si Omar logra obtener K en Q sesiones, estará en condiciones de obtener una MAC, por lo que la probabilidad de Omar de hacerlo debe ser menor que ϵ.

Por lo tanto el esquema es seguro–$(Q/2^w + \epsilon,\ Q)$. □

3.2.2. Identificación por *desafío y respuesta mutua con clave simétrica*. En este caso ambos participantes realizan la prueba de conocimiento entre sí. Como en el esquema anterior debe evitarse la reutilización de cualquier respuesta, ya sea en la misma sesión o en una siguiente. Se describen los pasos necesarios de una sesión del esquema en el protocolo (3.2.2).

1. Ben : $r_1 = \text{rand}(2^w)$, $\quad r_1 \longrightarrow$ Ana.
2. Ana : $r_2 = \text{rand}(2^w)$, $\quad u_1 = \text{mac}_K(\text{“Ana”} \parallel r_1 \parallel r_2)$, $\quad (r_2, u_1) \longrightarrow$ Ben.
3. Ben : $u_1^* = \text{mac}_K(\text{“Ana”} \parallel r_1 \parallel r_2)$, $\quad$ Si $u_1 = u_1^*$ acepta,
   $u_2 = \text{mac}_K(\text{“Ben”} \parallel r_2)$, $\quad u_2 \longrightarrow$ Ana.
4. Ana : $u_2^* = \text{mac}_K(\text{“Ben”} \parallel r_2)$, $\quad$ Si $u_2 = u_2^*$ acepta.

PROTOCOLO 3.2.2. Desafío y respuesta mutua con clave simétrica.

Notar que se requiere imponer una asimetría en las MAC de forma que una enviada en un sentido no pueda luego ser reutilizada en el sentido contrario. En el diagrama 3.2.2 se ilustra los flujos de información del protocolo.

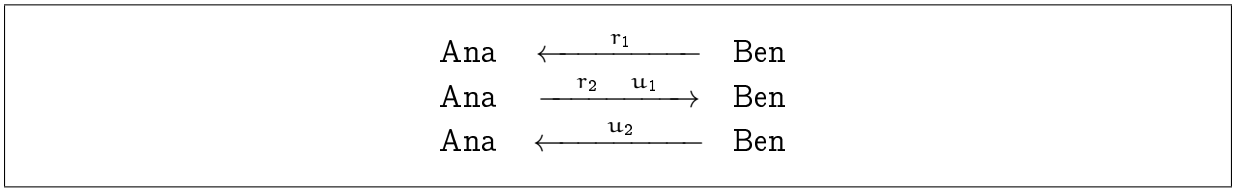

DIAGRAMA 3.2.2. Desafío y respuesta mutua con clave simétrica.

La seguridad del Protocolo 3.2.2 se demuestra en el Teorema 3.2.2.

TEOREMA 3.2.2. *Utilizando un MAC seguro–*(ϵ, Q)*, si los desafíos son aleatorios y de* w *bits, el esquema de identificación mutua «Desafío y respuesta con clave simétrica» es seguro–*$(Q/2^w + 2\epsilon, Q/2)$.

DEMOSTRACIÓN. La prueba es completa, ya que si Omar conoce la clave, podrá autentificarse ante Ben. Para el hermetismo, se aplica un argumento similar al caso del Teorema 3.2.1.

En cuanto a la consistencia, que Ben acepte a Omar implique que Omar conoce la clave, es equivalente a que si Omar no conoce la clave, Ben no acepte. En primer lugar, en el caso de identificación mutua, el límite de sesiones que puede observar Omar es $Q/2$. Así podrá disponer de Q MACs. Como los mensajes u_1 son creados por Ana con una estructura distinta al de los mensajes u_2 creados por Ben, los mensajes u_1 no pueden reutilizarse como creados por Ben o los mensajes u_2 como creados por Ana. Para usurpar la identidad de Ana alcanza determinar u_1 y para usurpar la identidad de Ben alcanza con determinar u_2. La mitad de los MAC disponibles son generados por Ana y la otra mitad son generados por Ben con la misma clave (ya que esta es simétrica).

Diremos que el atacante Omar logra una sustitución si acierta al seleccionar entre sus Q MAC recolectados el auténtico valor. Como la información de MAC observada por Omar está protegida por la misma clave, puede recolectar información de la MAC en ambos sentidos para intentar una sustitución.

Para usurpar la identidad de Ana, Omar podría intentar reutilizar un u_1 de los $Q/2$ que dispone, si se le permitiese recopilar Q MACs donde él mismo elige el desafío r_2 y lo mantiene fijo. En ese caso los ("Ana" $\|$ r_1 $\|$ r_2) posibles son 2^w y $p_{A1} = Q/2^{w+1}$ o falsificarlo con probabilidad $p_{A2} = \epsilon$, por lo que

$$p_A = p_{A1} + p_{A2} = Q/2^{w+1} + \epsilon.$$

Para usurpar la identidad de Ben, Omar podría intentar también reutilizar un u_2 de los $Q/2$ que dispone entre los 2^w con probabilidad $p_{B1} = Q/2^{w+1}$ o falsificarlo con probabilidad $p_{B2} = \epsilon$, por lo que

$$p_B = p_{B1} + p_{B2} = Q/2^{w+1} + \epsilon$$

Entonces la probabilidad de éxito de Omar no es mayor a $Q/2^w + 2\epsilon$. □

3.2.3. Identificación mutua por *desafío y respuesta con clave asimétrica*. En este caso se asumen que las firmas digitales son seguras–(ϵ, Q), es decir que no pueden ser falsificadas a partir de la observación previa de Q de ellas con una probabilidad mayor a ϵ. En el Protocolo 3.2.3, se describen los pasos necesarios.

Notar que para un usuario U cualquiera, ver_U representa su clave pública, que está directamente asociada a $\text{ver}_U(m, s)$, la función de verdad (*booleana*) que permite verificar si la firma s del mensaje m corresponde o no a su clave pública.

1. Ben: $r_1 = \text{rand}(2^w)$, $\quad (\text{Cert}_{\text{Ben}}, r_1) \longrightarrow$ Ana.
2. Ana : $r_2 = \text{rand}(2^w)$, $\quad s_1 = \text{sig}_{\text{Ana}}(\text{“Ben”} \parallel r_1 \parallel r_2)$, $\quad (\text{Cert}_{\text{Ana}}, r_2, s_1) \longrightarrow$ Ben.
3. Ben verifica ver_{Ana} en Cert_{Ana}. Si $\text{ver}_{\text{Ana}}(\text{“Ben”} \parallel r_1 \parallel r_2, s_1)$ acepta,
   $s_2 = \text{sig}_{\text{Ben}}(\text{“Ana”} \parallel r_2)$, $\quad s_2 \longrightarrow$ Ana.
4. Ana verifica ver_{Ben} en Cert_{Ben}. Si $\text{ver}_{\text{Ben}}(\text{“Ana”} \parallel r_2, s_2)$ acepta.

PROTOCOLO 3.2.3. Desafío y respuesta mutuo con clave asimétrica.

En el Teorema 3.2.3 se prueba la seguridad del esquema.

TEOREMA 3.2.3. *Si el esquema de firma* $\text{sig}()$ *es seguro–*(ϵ, Q) *y los desafíos son aleatorios de longitud* w*, el protocolo del esquema de identificación mutua «Desafío y respuesta con clave asimétrica» es seguro–*$(Q/2^{w-1} + 2\epsilon, Q)$.

DEMOSTRACIÓN. La demostración es análoga a la correspondiente simétrica, teniendo en cuenta que las firmas tienen una clave distinta en cada sentido, por lo que se toman Q sesiones y que ahora la probabilidad de usurpar una firma es

$$p_{A1} = p_{B1} = \frac{Q}{2^w},$$

a partir de lo cual de la misma forma que en el teorema anterior, se obtiene el valor enunciado en la tesis. □

3.3. Esquemas de identificación *basados en una conjetura*

Los esquemas de identificación basados en una conjetura, parten de la confianza en que un problema que se conjetura como sin solución y que por lo tanto se puede considerar de muy difícil solución en tiempo polinomial y con probabilidad no despreciable. El problema permite a partir de un secreto (clave privada) generar una clave pública.

La seguridad de estos esquemas requiere que sean completos, consistentes y herméticos. No es necesario partir de la seguridad de otras primitivas, pero si la conjetura fuera falsa, el esquema perdería utilidad.

3.3.1. El esquema de identificación *Schnorr*. El *esquema de identificación Schnorr* es un tipo de esquema basado en el problema del logaritmo discreto, que no usa herramientas criptográficas cuya medida de seguridad está definida. Una ventaja de este tipo de esquemas es que podrían ser más eficientes y consumir menos recursos de comunicación. Se tomará λ como un elemento de orden primo y muy grande q,

Se elige un parámetro de seguridad w tal que $2^w < q$ sea cota del desafío aleatorio (exponente) $r = \text{rand}(2^w)$. Ana define un secreto, su clave privada a y los parámetros

públicos son: λ, q, w y la clave pública correspondiente $\alpha = \lambda^{-a}$. En el Protocolo 3.3.1 se describen los pasos de una sesión del esquema. Cuando Ana intenta identificarse y Ben desea verificarlo, Ana elige como clave privada un exponente a y será:

$$\alpha \equiv \lambda^{-a} \equiv \lambda^{q-a} \pmod{p}.$$

El uso de los certificados se omite para simplificar la descripción en el Protocolo 3.3.1.

(1)	Ana: $k = \text{rand}(q)$, $\gamma = \lambda^k$	$\gamma \longrightarrow$ Ben.
(2)	Ben: $r = \text{rand}(2^w)$	$r \longrightarrow$ Ana.
(3)	Ana: $y \equiv k + ar \pmod{q}$	$y \longrightarrow$ Ben.
(4)	Ben: $\lambda^y \alpha^r \equiv \gamma$.	

PROTOCOLO 3.3.1. Schnorr

El esquema Schnorr está diseñado para ser eficiente y rápido, requiriendo mínimo esfuerzo de cálculo para identificarse. En efecto el mayor esfuerzo de cálculo para Ana se da en el paso (1), pero es posible realizar el cálculo previamente. En el paso (3) se requiere una multiplicación y una suma en los exponentes naturales menores que q. En el caso de implementarse el grupo cíclico a trabajando en el cuerpo finito F_p, es decir eligiendo un primo muy grande y un elemento λ en $[1, p-1]$ que genere el grupo cíclico de orden q, la información en bits intercambiada son $p + w + q$ bits. En general p es el tamaño en bits necesario para representar γ. Puede disminuirse esta información a costa de utilizar una función de *hash* adecuada (por ejemplo SHA–1, ver sección 2.5) y enviando $\gamma' = \text{SHA–1}(\gamma)$; Ben podrá comparar el *hash* recibido contra el *hash* del γ calculado. A los efectos de demostrar la seguridad del esquema, el primer paso es verificar que es completo.

3.3.1.1. Completitud.

PROPOSICIÓN 3.3.1. El esquema Schnorr es completo.

DEMOSTRACIÓN.

$$\lambda^y \alpha^r \equiv \lambda^{k+ar} \alpha^r \equiv \lambda^k \equiv \gamma \pmod{p}.$$

□

3.3.1.2. Consistencia. A continuación se verificará que el esquema son consistentes (ver la Definición 56), es decir que usurpar la identidad de Ana implica que se puede obtener la clave privada con mayor probabilidad que la dada por el parámetro de seguridad. Para esto se supone primero que se logra usurpar la identidad de Ana y se intenta probar que esto equivale a tener la capacidad de obtener la clave privada en tiempo polinomial y con probabilidad no despreciable. El siguiente lema será de utilidad.

LEMA 3.3.1. *Sustituir a Ana implica que es posible adivinar en tiempo polinomial, para un valor dado γ, dos pares (r', y'), y (r'', y'') válidos con probabilidad no despreciable, es decir tales que:*

$$\gamma = \lambda^{y'} \alpha^{r'} = \lambda^{y''} \alpha^{r''} \pmod{p}.$$

Se presentan dos demostraciones de este lema, cuyo resultado se presume en la Demostración 9.4.1 de [Sti06] (página 375). La primera se propone como solución al Ejercicio 9.6 [Sti06]. La demostración está basada en un ataque mediante un algoritmo explícito, por lo que se considera ilustrativo.

DEMOSTRACIÓN. Observando el Protocolo 3.3.1, si Omar está en condiciones de usurpar la identidad de Ana, puede deducir en tiempo polinomial un y a partir de un par (γ, r) con mejor probabilidad que adivinar r (que es 2^{-w}). Podemos suponer entonces que Omar dispone de un oráculo $\mathcal{O}(\gamma, r)$ del tipo *Las Vegas* (ver la Definición 38), cuya respuesta sería y a partir un par cualquiera (γ, r) con probabilidad ϵ.

Para obtener los dos pares Omar ejecuta el Algoritmo 3.3.1

(3.3.1)	$N = \lceil 1/\epsilon \rceil$
(3.3.2)	Se generan N pares: $(\gamma_i, r_i) = (\text{rand}(q), \text{rand}(2^w))$.
(3.3.3)	Se prueba N veces $\mathcal{O}(\gamma_i, r_i)$.
(3.3.4)	Si el par (γ_i, r_i) es exitoso: $(\gamma', r') = (\gamma_i, r_i)$.
(3.3.5)	Se generan N valores: $s_i = \text{rand}(2^w)$.
(3.3.6)	Se prueba N veces $\mathcal{O}(\gamma', s_i)$.
(3.3.7)	Si el par (γ', s_i) es exitoso y si $s_i \neq r' \Rightarrow r'' = s_i$.

ALGORITMO 3.3.1. Hallar respuestas Schnorr válidas.

Para que este algoritmo pueda realizarse en tiempo polinomial en el parámetro de seguridad w, el valor de N debe ser polinomial en t. En ese caso veremos que es posible obtener el par de valores buscados con una probabilidad no despreciable.

En la Figura 3.3.1 se muestra el espacio de probabilidad de generación de los pares (γ, r), siendo Γ el conjunto de los γ y R el conjunto de los r y $X \subset \Gamma \times R$. X es el conjunto de los casos en que la respuesta es válida. Su probabilidad es por hipótesis ϵ.

$$P(X) = \frac{|X|}{|R||\Gamma|} = \epsilon.$$

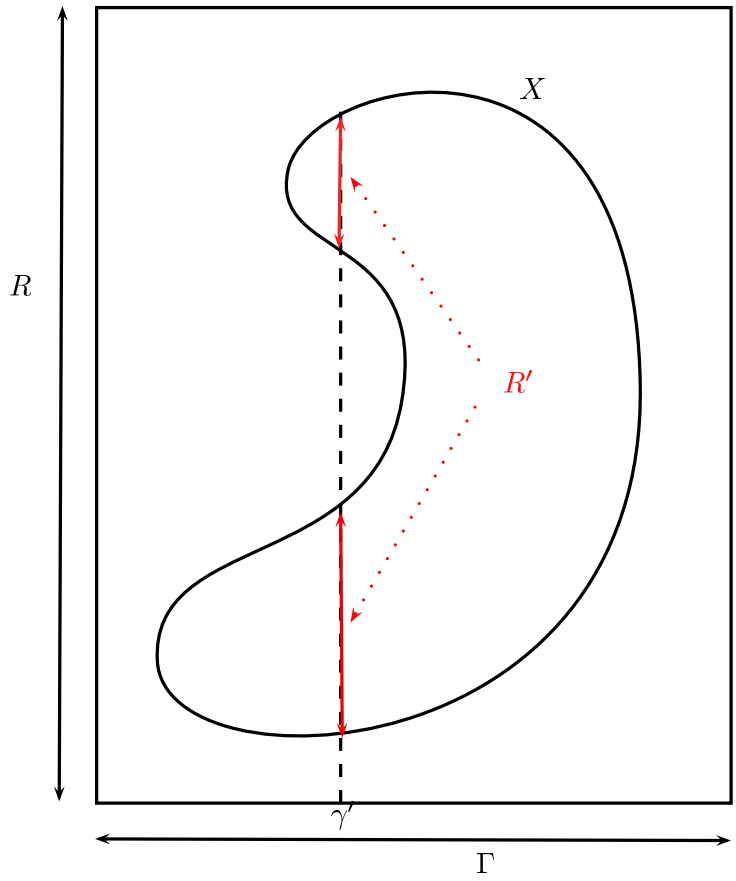

FIGURA 3.3.1. Espacio de probabilidad.

Es fácil observar que el Algoritmo 3.3.1 es $O(N)$. Además, la probabilidad de fallar en N intentos es

$$\binom{N}{0}(1-1/N)^N = e^{-1},$$

por lo que la probabilidad de éxito es $1-e^{-1}$. Una vez obtenido el par (γ', r'), se debería evaluar la probabilidad de obtener un nuevo r'' pero distinto a r' para el γ' del par anterior. Observando la Figura 3.3.1, el conjunto de los pares exitosos de abscisa γ' consisten en $R' = X \cap \{(\gamma, r) : \gamma = \gamma'\}$.

Veremos que la probabilidad de obtener un γ' para el cual la probabilidad de éxito sea mayor o igual a $\epsilon/2$, es mayor o igual a $1/2$. Se definen:

$$\begin{aligned} p =& \Pr\left[(\gamma', r) \in X\right] \Rightarrow p = \frac{|R'|}{|R|}, \\ \Gamma_0 =& \left\{\gamma' : \quad p \geqslant \frac{\epsilon}{2}\right\}, \\ \Gamma_1 =& \Gamma \backslash \Gamma_0. \end{aligned}$$

Entonces (ver Figura 3.3.2):

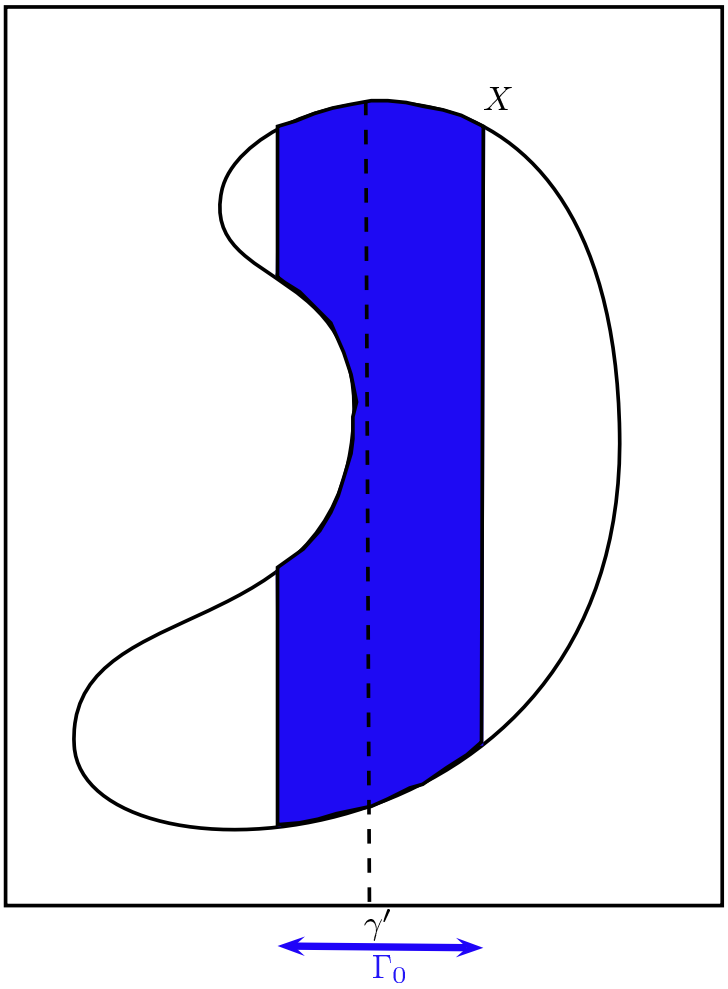

FIGURA 3.3.2. Probabilidad de Γ_0.

$$P(\gamma' \in \Gamma_1) = \frac{\sum_{\gamma' \in \Gamma_1} |R'|}{|X|} = \frac{|R| \sum_{\gamma' \in \Gamma_1} p}{|X|}$$
$$= \frac{|\Gamma_1| p}{\frac{|X|}{|R|}} \leqslant \frac{|\Gamma_1| p}{\epsilon |\Gamma|} \leqslant \frac{|\Gamma_1| \epsilon/2}{\epsilon |\Gamma|} = \frac{1}{2} \frac{|\Gamma_1|}{|\Gamma|} \leqslant \frac{1}{2}.$$

Por lo tanto la probabilidad de obtener un "buen" γ' es mayor o igual a

$$\frac{1}{2}(1 - e^{-1}).$$

En el segundo intento la probabilidad de obtener un par (γ', r'') es

$$1 - (1 - \frac{\epsilon}{2})^N - \frac{1}{(2^w)^2} \approx 1 - (1 - \frac{\epsilon}{2})^{\frac{\frac{1}{2}}{\frac{\epsilon}{2}}} \approx 1 - e^{-\frac{1}{2}}.$$

La probabilidad de tener éxito sería mayor o igual a

$$\frac{1}{2}(1 - e^{-1})(1 - e^{-\frac{1}{2}}),$$

que es una probabilidad no despreciable (ver sección 3.3.1.2). □

La segunda demostración, corresponde a la nota publicada en [Sti07].

Demostración. La consistencia del esquema significa que cualquiera que pueda usurpar la identidad de Ana con una probabilidad no despreciable en tiempo polinomial, podrá calcular la clave privada de Ana en tiempo polinomial. Se supone entonces que es posible obtener dos algoritmos: G e Y. El algoritmo G obtiene un γ válido en tiempo polinomial. $Y(\gamma, r)$ es un algoritmo *Las Vegas* que obtiene un y válido con probabilidad ϵ o indica «Falla» en caso contrario. La idea es ejecutar G para obtener un γ y luego ejecutar Y varias veces hasta que se encuentre un par (r', r'') con respuestas válidas para el mismo valor de γ, donde $\epsilon = \frac{1}{w^c}$ con c constante. Es decir que habrá una respuesta por cada $\frac{2^w}{w^c}$ desafíos r posibles (ya que $|r| = w$). Esto corresponde a la hipótesis de que ϵ represente una probabilidad no despreciable. Ahora si se ejecuta Y w^c veces, es decir un número polinomial en el parámetro w, la probabilidad de no obtener ninguna respuesta será (por la distribución binomial)

$$p_0 = (1 - \frac{1}{w^c})^{w^c}.$$

Y la probabilidad de obtener exactamente una respuesta será

$$p_1 = w^c \times \frac{1}{w^c} \times (1 - \frac{1}{w^c})^{(w^c - 1} = (1 - \frac{1}{w^c})^{w^c - 1}.$$

Como $p_0 \approx p_1 \approx e^{-1} \approx 0{,}37$, la probabilidad de obtener por lo menos dos respuestas correctas es

$$1 - p_0 - p_1 \approx 0{,}26.$$

Por lo tanto, se ha logrado en tiempo polinomial y con probabilidad constante y positiva, un par de valores (r, y) para un γ dado. Como veremos en la proposición siguiente, esto implica haber obtenido una forma eficiente de calcular la clave privada de Ana. □

Proposición 3.3.2. El esquema Schnorr es consistente.

Demostración. A partir del Lema 3.3.1, si Omar puede usurpar la identidad de Ana, puede obtener en tiempo polinomial r', r'' y también y', y'' tales que

$$\gamma \quad = \lambda^{y'} \alpha^{r'} = \lambda^{y''} \alpha^{r''},$$
$$\lambda^{y' - y''} = \alpha^{r'' - r'} \equiv \lambda^{a(r' - r'')}.$$

Y como λ es de orden q

$$y' - y'' \equiv a(r' - r'') \pmod{q}.$$

Siendo así posible obtener la clave privada a. Por lo tanto poder usurpar la identidad de Ana implica poder obtener la clave privada. El esquema es consistente. □

3.3.1.3. Hermetismo. A continuación se prueba que el esquema es hermético.

Proposición 3.3.3. El esquema Schnorr es hermético (cero).

Demostración. La información que viaja en una sesión puede resumirse en un estado $t = (\gamma, r, y)$ donde se cumple que

$$\gamma \equiv \lambda^y \alpha^r \pmod{p}.$$

Supongamos que con un algoritmo E, se obtiene la clave privada con probabilidad ϵ a partir de una sucesión real de estados $t_1, \ldots, t_l$. Si a su vez $t'_1, \ldots, t'_l$ son sesiones

simuladas con la misma distribución de probabilidad, E podría extraer con probabilidad ϵ la clave privada.

Todos los estados posibles son:

$$\mathcal{T} = \{(\gamma, r, y) : \quad \gamma \equiv \lambda^y \alpha^r \pmod{p}\},$$

donde $r \in [1, 2^w]$ e $y \in [0, q-1]$. Entonces $|\mathcal{T}| = q2^w$.

$$P(T = t) = P(Y = y, R = r) = P(Y = y \mid R = r)P(R = r)$$
$$P(Y = y|R = r) = P(K + aR = y|R = r) = P(K = y - ar) = q^{-1}.$$

Entonces

$$P(T = t) = q^{-1}2^{-w}.$$

Omar podría entonces realizar una simulación de la sucesión de estados donde

$$r = \text{rand}(2^w),$$
$$y = \text{rand}(q)$$
$$\gamma = \lambda^y \alpha^r,$$

tienen la misma distribución de probabilidad que el caso real. Por lo tanto la sucesión de estados real no aporta información a Omar. □

3.3.2. El esquema de identificación *Guillou–Quisquater*. El esquema está basado en esquema RSA (ver sección 2.4). El TA elige dos primos p y q y forma el producto $n = pq$. Los valores de p y q son secretos, mientras que n es público. Los valores de los primos p y q deben ser elegidos de forma tal que sea difícil factorizar n. También el TA elige $a \gg 1$ como exponente RSA y parámetro de seguridad, cota del desafío aleatorio $r = \text{rand}(a)$. Los parámetros públicos son n, a.

Ana elige la clave privada u tal que (ver sección 2.1) el máximo común divisor de u y n sea igual a 1 y luego calcula la clave pública

$$\beta \equiv (u^{-1})^a \pmod{n}.$$

En el Protocolo 3.3.2 se describen los pasos de una sesión del esquema.

(1)	Ana: $k = \text{rand}(n), \quad \gamma = k^a$	$\gamma \longrightarrow$ Ben.
(2)	Ben: $r = \text{rand}(a)$	$r \longrightarrow$ Ana.
(3)	Ana: $y = ku^r$	$y \longrightarrow$ Ben.
(4)	Ben: $y^a \beta^r \equiv \gamma \pmod{n}$.	

PROTOCOLO 3.3.2. Guillou–Quisquater.

3.3.2.1. Completitud.

PROPOSICIÓN 3.3.4. El esquema Guillou–Quisquater es completo.

DEMOSTRACIÓN.

$$y^a \beta^r \equiv (ku^r)^a u^{-ar} \equiv k^a \equiv \gamma \pmod{n}.$$

□

3.3.2.2. Consistencia. A continuación se verificará que el esquema son consistentes (ver la Definición 56), es decir que usurpar la identidad de Ana implica que se puede obtener la clave privada con mayor probabilidad que la dada por el parámetro de seguridad. Para esto se supone primero que se logra usurpar la identidad de Ana y se intenta probar que esto equivale a tener la capacidad de obtener la clave privada en tiempo polinomial y con probabilidad no despreciable.

PROPOSICIÓN 3.3.5. El esquema Guillou–Quisquater es consistente.

DEMOSTRACIÓN. El Lema 3.3.1 sobre las ternas (y, γ, r), es aplicable también en este esquema, ya que cumplen exactamente el mismo rol. Si Omar puede usurpar la identidad de Ana, puede obtener en tiempo polinomial r', r'' y también y', y'' tales que $\gamma \equiv y_1^a \beta^{r_1} \equiv y_2^a \beta^{r_2} \pmod{n}$. Por simetría sin pérdida de generalidad podemos asumir que $r_1 > r_2$, entonces

$$\beta^{r_1 - r_2} \equiv (y_2 y_1^{-1})^b \pmod{n} \text{ y si } t \equiv (r_1 - r_2)^{-1} \pmod{a} \text{ entonces}$$
$$\beta^{(r_1 - r_2)t} \equiv (y_2 y_1^{-1})^{at} \pmod{n}.$$

Dado que existe $l \in \mathbb{N} : \ (r_1 - r_2)t = la + 1$

$$\beta^{lb+1} \equiv (y_2 y_1^{-1})^{at} \pmod{n} \implies \beta \equiv (y_2 y_1^{-1})^{at} (\beta^{-1})^{la}.$$

Elevando al exponente $a^{-1} \pmod{n}$ y tomando inversas:

$$u^{-1} \equiv (y_2 y_1^{-1})^t (\beta^{-1})^l \pmod{n}$$
$$u \equiv (y_1 y_2^{-1})^t \beta^l \pmod{n}.$$

□

3.3.2.3. Hermetismo. A continuación se prueba que el esquema es hermético.

PROPOSICIÓN 3.3.6. El esquema Guillou–Quisquater es hermético (cero).

DEMOSTRACIÓN.

$$\mathcal{T} = \{(\gamma, r, y) : \quad \gamma \equiv y^a \beta^r \pmod{n}\},$$

donde $r \in [1, a]$ e $y \in [0, n-1]$.

Entonces $|\mathcal{T}| = an$.

$$P(T = t) = P(Y = y, R = r) = P(Y = y | R = r) P(R = r)$$

$$P(Y = y | R = r) = P(K = u^{-r} | R = r) = n^{-1}.$$

Entonces

$$P(T = t) = n^{-1} a^{-1}.$$

Omar podría entonces realizar una simulación de la sucesión de estados donde

$$r = \text{rand}(a), y = \text{rand}(n).$$

$$\gamma = y^a \beta^r \pmod{n}.$$

tendrá la misma distribución de probabilidad que la real. Por lo tanto la sucesión de estados real no aporta ninguna información a Omar y el esquema es hermético. □

3.4. Esquemas de distribución previa de claves (KPS)

En la distribución previa de claves (KPS [Sti06]), se distribuye una clave de larga vida y se usa para cada sesión de comunicación. Es el esquema mas sencillo, pero al ser usada la clave en cada sesión, su exposición puede implicar un riesgo mayor ([Sha49]).

3.4.1. Distribución previa de claves trivial. El TA distribuye las claves entre los n participantes. Es incondicionalmente seguro. La cantidad de claves que debe administrar y distribuir el TA crece de forma cuadrática con los participantes. En efecto el TA deberá establecer una clave para cada uno de los $\frac{n(n-1)}{2}$ pares de participantes.

3.4.2. Distribución previa *(KPS) por acotación de complot*. Una técnica posible para acotar las claves que el TA debe distribuir en KPS es determinar un número reducido de participantes a partir del cual el riesgo de complot se considere insignificante. Esto se puede lograr considerando a las claves de larga vida distribuidas por el TA como información parcial a partir de la cual, cualquier par de usuarios puede deducir una clave que sea inaccesible para el resto de los usuarios, a menos que se reúnan n o más participantes. Esta técnica se basa en la interpolación de Lagrange (por ejemplo Blom KPS [Sti06]) o en métodos combinatorios (distribución de patrones: Fiat-Naor, Mitchell-Piper KPS [Sti06]).

3.4.3. Distribución previa *(KPS) Diffie–Hellman*. Sea un grupo cíclico multiplicativo $\langle\lambda\rangle$ de orden q tal que el problema de Decisión Diffie–Hellman sea inviable. Se conviene por notación, que las claves privadas se indican por letras minúsculas y las claves públicas por letras griegas. Cada usuario U elije un exponente aleatorio $u = rand(q)$ como clave privada de larga vida y determina su clave pública como la potencia correspondiente,

$$\upsilon = \lambda^u.$$

A continuación, el usuario U entrega la clave pública al TA para que cree el certificado con su firma correspondiente que garantice un sistema de identificación seguro. Así, cualquier par de usuarios Ana y Ben puede intercambiar certificados, verificar las claves públicas con la firma del TA y obtener la claves simétricas de comunicación aplicando la fórmula:

$$K_{Ana,Ben} = \beta^a = \alpha^b.$$

3.4.3.1. Propiedades.

- Las claves de los usuarios son de larga vida.
- Si los usuarios no revelan su clave privada al TA, la clave determinada queda disponible solo para el par de usuarios involucrados.
- La seguridad está basada en el problema DDHP [Sti06]. Se espera que sea inviable en tiempo polinomial distinguir claves Diffie–Hellman de elementos aleatorios del subgrupo $\langle\lambda\rangle$.
- Las claves públicas a distribuir por el TA crecen de forma lineal con el número de participantes.

TEOREMA 3.4.1. *El esquema KPS Diffie–Hellman es seguro si utiliza un sistema de certificación seguro y si el problema de cálculo Diffie–Hellman en el subgrupo $\langle\alpha\rangle$ es inviable.*

Demostración. Para demostrar la seguridad del esquema hay que verificar que un adversario no podrá realizar un ataque activo o pasivo exitoso y que el protocolo de identificación es seguro. El protocolo de identificación es seguro por hipótesis.

Al no haber interacción en el esquema entre los participantes (que pueden intercambiar información pública como sus nombres de identificación o sus certificados pero no información privada) y, asumiendo que las claves privadas satisfacen las hipótesis de la inviabilidad del problema DDHP, no hay oportunidad de éxito para un ataque activo.

En ataque pasivo el adversario solo puede observar las claves públicas y determinar alguna información de la clave no es resolver el problema $\mathrm{DDHP}(\lambda, \alpha, \beta)$ que no es viable por hipótesis. □

3.5. El esquema SKDS *Bellare–Rogaway*

Los esquemas de distribución de claves de sesión (SKDS) fueron presentados en la sección 1.4.4. Aquí se tratará el esquema Bellare–Rogaway y la demostración de su seguridad.

3.5.1. Descripción. En el Protocolo 3.5.1 tanto Ana como Ben eligen desafíos aleatorios que envían al TA: en primer lugar, Ana envía la solicitud de sesión a Ben, que consiste en una terna formada por los nombres Ana, Ben y el desafío aleatorio de Ana. Luego Ben envía la solicitud completa al TA con los nombres de Ana, Ben y los desafíos aleatorios de Ana y Ben. Entonces el TA genera una clave de sesión aleatoria K y genera, para cada usuario, una MAC de la cadena de caracteres formada por los nombres de los dos usuarios, el desafío aleatorio del destinatario y el cifrado (con la clave correspondiente entre el TA y cada usuario) de la clave de sesión. Los parámetros w_1 y w_2 se eligen para hacer despreciable la probabilidad del adversario de adivinar los desafíos aleatorios o la clave de sesión respectivamente..

1. $\mathrm{Ana} : r_{\mathrm{Ana}} = \mathrm{rand}(2^{w_1}), \quad (\text{“Ana”}, \text{“Ben”}, r_{\mathrm{Ana}}) \longrightarrow \mathrm{Ben}.$
2. $\mathrm{Ben} : r_{\mathrm{Ben}} = \mathrm{rand}(2^{w_1}), \quad (\text{“Ana”}, \text{“Ben”}, r_{\mathrm{Ana}}, r_{\mathrm{Ben}}) \longrightarrow \mathrm{TA}.$
3. $\mathrm{TA} : K = \mathrm{rand}(2^{w_2}) :$

$$y_B = (e_{K_{\mathrm{Ben}}}(K), \mathrm{mac}_{K_{\mathrm{Ben}}}(\text{“Ana”} \parallel \text{“Ben”} \parallel r_{\mathrm{Ben}} \parallel e_{K_{\mathrm{Ben}}}(K))), \quad y_B \longrightarrow \mathrm{Ben}.$$

$$y_A = (e_{K_{\mathrm{Ana}}}(K), \mathrm{mac}_{K_{\mathrm{Ana}}}(\text{“Ben”} \parallel \text{“Ana”} \parallel r_{\mathrm{Ana}} \parallel e_{K_{\mathrm{Ana}}}(K))), \quad y_A \longrightarrow \mathrm{Ana}.$$

Protocolo 3.5.1. SKDS Bellare–Rogaway.

En el protocolo Bellare–Rogaway, al recibir y_A, Ana puede estar seguro que B recibió r_A y que por lo tanto fue notificado de la intención de Ana de establecer una clave de sesión y de que Ben también solicitó la clave. Solo queda entonces esperar la recepción de un mensaje cifrado con la clave de sesión por parte de Ben, para confirmar la clave.

Teorema 3.5.1. *El esquema SKDS Bellare–Rogaway (3.5.1) es seguro. Se supone que los participantes en el esquema lo hacen honestamente y que los esquemas de cifrado y de MAC utilizados son seguros. También que las claves secretas lo son entre los participantes y que los desafíos se obtienen por generadores aleatorios perfectos.*

DEMOSTRACIÓN. Se debe demostrar que el esquema es seguro ante un ataque activo y pasivo y que el esquema de identificación es seguro. El esquema de identificación se basa en la seguridad de las primitivas criptográficas utilizadas. Se analizan los ataques posibles.

Omar es pasivo. En este, caso en cualquier sesión del esquema, los participantes del conjunto de control aceptan y podrán descifrar la clave de sesión. Nadie más podrá lograrlo debido a la seguridad del esquema de cifrado.

Omar es activo frente a A. El objetivo de Ana es obtener una clave de sesión que no pueda determinarse fuera del conjunto de control. Observar que Ana no puede distinguir durante la sesión si alguien fuera del conjunto de control está sustituyendo a Ben. Cuando Ana recibe y_A, verifica la validez de la MAC, que incorpora su propio desafío aleatorio r_A, las identidades de Ana y Ben, y la de la clave de sesión cifrada $e_{K_{Ana}}(K)$. Esto limita la posibilidad por parte de Omar de reutilizar la MAC debido al desafío aleatorio y a que $mac_{K_{Ana}}()$ es solo disponible para TA en los márgenes de seguridad de las hipótesis. También se evita que $e_{K_{Ana}}(K)$ sea alterada fuera del conjunto de control de participantes indicados en el esquema. *Omar es activo frente a Ben.* Ben no sabe si Omar está sustituyendo a Ana. Cuando Ben recibe el mensaje y_B, verifica la validez de $mac_{K_{Ben}}()$ que incorpora el propio desafío aleatorio r_B, las identidades de ambos y la clave se sesión cifrada $e_{K_{Ben}}(K)$. Así Ben verifica que la MAC ha sido calculada por el TA, al ser el TA el único que conoce la clave de la MAC. Además el desafío aleatorio evita la reutilización de un MAC de una sesión previa. El cifrado de la clave evita que Omar usurpe la clave establecida por el TA.

Por lo tanto, tanto Ana como Ben pueden confiar que su par es el único que es capaz de descifrar la clave K, aún si Omar intenta usurpar la identidad en una sesión del esquema. □

3.6. Esquemas de acuerdo de claves (KAS)

Un esquema de acuerdo de claves (ver 1.4.5) es seguro si es un esquema de identificación mutua seguro: ningún participante honesto aceptará ante un ataque activo y, ante un ataque pasivo ambos participantes calcularán la misma clave de sesión sin brindar información alguna de su valor.

DEFINICIÓN 65. Un esquema de acuerdo de claves brinda *autentificación implícita* si nadie más que su par supuesto puede calcular la clave (en particular, el adversario no debería poder calcular la clave).

DEFINICIÓN 66. Un esquema de acuerdo de claves brinda *confirmación implícita* (implicit key confirmation) si cualquiera de las partes pueden suponer que su par supuesto *podría calcular* la clave, pero nadie más.

DEFINICIÓN 67. Un esquema de acuerdo de claves brinda *confirmación explícita* si cualquiera de las partes pueden suponer que su par *calculó* la clave, pero nadie más.

En la práctica, la información previa que debe almacenar cada participante son los los certificados de los n participantes. Por lo tanto:

1. cada participante almacena los certificados de los demás,
2. el TA no participa en la determinación de la clave de sesión,

3. el acuerdo de claves requiere criptografía asimétrica para mantener el crecimiento lineal de la cantidad de claves almacenadas.

Todo protocolo de acuerdo de claves debería cumplir los requerimientos que se enumeran a continuación. Estas condiciones son satisfechas en los esquemas SKDS B–R y KAS STS.

1. Identificar la sesión para evitar su reutilización mediante un parámetro aleatorio totalmente independiente (no predecible ni que permita predecir) respecto la información de sesión.
2. Identificar los usuarios participantes (requerimiento para lograr la confidencialidad).
3. Tener distinto número de variables en cada flujo del protocolo para evitar su posible reutilización.
4. Producir una clave aleatoria (no predecible).

3.6.1. El esquema de acuerdo de claves *Diffie–Hellman*. En este esquema, los parámetros de dominio público consisten en el grupo cíclico $\langle\lambda\rangle$ y su orden q. La obtención de la clave corresponde al problema de cálculo Diffie–Hellman, $\mathrm{CDH}(\lambda, \alpha, \beta)$. Asumiendo que dicho cálculo es inviable, un adversario pasivo no podría calcular la clave ni obtener información de ella (problema de decisión Diffie–Hellman DDH).

1. $\mathrm{Ana} : a = \mathrm{rand}(q), \quad \alpha = \lambda^a, \quad \alpha \longrightarrow \mathrm{Ben}.$
2. $\mathrm{Ben} : b = \mathrm{rand}(q), \quad \beta = \lambda^b, \quad \beta \longrightarrow \mathrm{Ana}.$
3. $\mathrm{Ana} : K = \beta^a,$
   $\mathrm{Ben} : K = \alpha^b.$

PROTOCOLO 3.6.1. KAS Diffie–Hellman

Este esquema no es seguro ante un ataque activo MIM (ver definición 14).

3.6.2. El esquema de acuerdo de claves (KAS) *estación a estación* (STS). El esquema de acuerdo de claves autentificado *estación a estación* (STS) es una modificación del *KAS Diffie–Hellman*, para adaptarlo a los esquemas ISO 9798–3, (ver [Sti06]). Fue presentado en 1987 y desarrollado por W. Diffie, P. C. van Oorschot y M. J. Wiener. Se utilizan certificados firmados por un agente con el rol de TA. Todos los usuarios disponen de un esquema de firmas y su par de claves $\mathrm{ver}, \mathrm{sig}$, así como el TA que entrega de manera segura su algoritmo de verificación $\mathrm{ver}_{\mathrm{TA}}()$. Cada usuario U posee un certificado (ver la Definición 13)

$$\mathrm{Cert}_U = (\mathrm{Decl}_{\mathrm{ID}}(U), \mathrm{sig}_{\mathrm{TA}}(\mathrm{Decl}_{\mathrm{ID}}(U))),$$

donde

$$\mathrm{Decl}_{\mathrm{ID}}(U) = \text{“U”} \parallel \mathrm{ver}_U.$$

La idea básica del Protocolo 3.6.2 es combinar el *KAS Diffie–Hellman* con un esquema de identificación mutua segura, donde los exponentes cumplen la función de desafíos aleatorios. Se puede decir, que al firmar los desafíos aleatorios, se logra la autentificación mutua. Finalmente, estos desafíos calculados como en el KAS Diffie–Hellman, permiten que ambas partes calculen la misma clave $K = \mathrm{CDH}(\lambda, \alpha, \beta)$.

1. $\text{Ana} : a = \text{rand}(q);\ \alpha = \lambda^a; \quad (\text{Cert}_{\text{Ana}}, \alpha) \longrightarrow \text{Ben}.$
2. $\text{Ben} : b = \text{rand}(q);\ \beta = \lambda^b;\ K = \alpha^b$
   $y_2 = \text{sig}_{\text{Ben}}(\text{“Ana”} \parallel \alpha \parallel \beta); \quad (\text{Cert}_{\text{Ben}}, \beta, y_2) \longrightarrow \text{Ana}.$
3. Ana : Verificar certificado y extraer verificación, si $\text{ver}_{\text{Ben}}(y_2)$ aceptar,
   $K = \beta^a$
   $y_1 = \text{sig}_{\text{Ana}}(\text{“Ben”} \parallel \alpha \parallel \beta), \quad y_1 \longrightarrow \text{Ben}.$
4. Ben : Verificar certificado y extraer verificación, si $\text{ver}_{\text{Ana}}(y_1)$ aceptar,
   $K = \alpha^b$.

PROTOCOLO 3.6.2. KAS STS.

EJEMPLO 3.6.1. Antes de demostrar la seguridad de este esquema, se verificará cómo las firmas brindan protección ante un ataque *MIM*. Al reemplazar Omar en el ataque λ^a con $\lambda^{a'}$, recibirá de Ben:

$$\lambda^b,\ \text{sig}_{\text{Ben}}(\text{“Ana”} \parallel \lambda^b \parallel \lambda^{a'}). \tag{3.6.1}$$

Además debería reemplazar λ^b por $\lambda^{b'}$, para lo cual debería reemplazar la firma por

$$\text{sig}_{\text{Ben}}(\text{“Ana”} \parallel \lambda^{b'} \parallel \lambda^a).$$

Sin embargo, para Omar no es posible calcular la firma de Ben sobre

$$\text{“Ana”} \parallel \lambda^{b'} \parallel \lambda^a,$$

porque no posee la clave privada de Ben que le permitiría hacerlo. Tampoco podrá reemplazar

$$\text{sig}_{\text{Ana}}(\text{“Ben”} \parallel \lambda^a \parallel \lambda^{b'}) \text{ por}$$
$$\text{sig}_{\text{Ana}}(\text{“Ben”} \parallel \lambda^{a'} \parallel \lambda^b)$$

porque no posee la clave privada de Ana.

TEOREMA 3.6.1. *Asumiendo que el problema de decisión de Diffie–Hellman es inviable, STS es un esquema de acuerdo de claves autentificado y brinda* confirmación implícita *de clave. Además es seguro contra un ataque con claves de sesión conocidas (ver la Definición 66).*

La demostración se divide en tres partes:

1. es un esquema de identificación mutua seguro,
2. es un esquema con confirmación implícita de clave,
3. es un esquema seguro contra un ataque con claves de sesión conocidas.

LEMA 3.6.1. *Asumiendo que el problema de decisión de Diffie–Hellman es inviable, STS es un esquema de identificación mutua seguro.*

DEMOSTRACIÓN. El protocolo STS es una combinación del esquema KAS Diffie–Hellman y de un esquema de identificación mutua por desafío y respuesta con clave pública. La demostración se deduce inmediatamente a partir de la correspondiente realizada para el Protocolo 3.2.3. □

LEMA 3.6.2. *Asumiendo que el problema de decisión de Diffie–Hellman es inviable, el acuerdo de claves STS brinda* confirmación de clave implícita.

DEMOSTRACIÓN. Se analiza primero el caso en que Ana acepta y luego el caso en que Ben acepta.

1. - Si Ana acepta, por el Lema 3.6.1, Ana puede asumir que se comunicó con Ben y que Omar ha sido pasivo antes del último flujo del protocolo.
   - Si Ben es honesto y además ejecutó bien el esquema, Ana puede asumir que Ben puede calcular K y nadie más que él.
   - Ana puede asumir que Ben está en condiciones de calcular K. En efecto, Ana ha recibido la firma de Ben de λ^a y de λ^b, así como conoce su clave privada b.
   - Para Ana no hay garantía de que Ben *haya* calculado K.
2. Si Ben acepta, puede confiar en que se ha comunicado con Ana y que K puede ser calculado por Ana y nadie más. Sin embargo existe una diferencia:
   - cuando Ben acepta, si se supone que A es honesto, puede confiar en que Ana aceptó,
   - cuando Ana acepta no puede adelantar si Ben aceptará, ya que Omar podría afectar el último flujo provocando el rechazo de Ben.

No obstante, esto no afecta la seguridad del esquema. □

En un escenario real, una red permite a muchos usuarios establecer múltiples sesiones STS simultáneamente. Esto brinda al atacante nuevas oportunidades para atacar el esquema. Si Omar lograse obtener las claves de una serie de sesiones $[\mathcal{S}] = s_1, s_2, \ldots, s_t$ podría intentar, a partir de esa información, obtener la clave de otra sesión s_r. El ataque no requiere que todas las sesiones $s_1, s_2, \ldots, s_t$ hayan culminado para realizarse, sino que puede consistir en un ataque realizado sobre varias sesiones en paralelo.

Para probar la seguridad contra un ataque con claves conocidas, alcanza con verificar que dicho conocimiento no aporta a los efectos de determinar otras claves.

La demostración utiliza la misma estrategia que en las demostraciones de hermetismo en las demostraciones de seguridad de los esquemas de identificación, (ver Lema 3.3.3). Se escribe dicha información en la forma de listas, cuya distribución de probabilidad es la misma que una serie de listas simuladas que es posible construir sin conocimiento de claves.

LEMA 3.6.3. *El acuerdo de claves STS es seguro contra un ataque con claves de sesión conocidas, asumiendo que el problema de decisión de Diffie–Hellman es inviable.*

DEMOSTRACIÓN. En una sesión cualquiera del esquema, la información relevante consiste en la que es posible observar, las potencias, y la que un rival desea obtener, que es la clave correspondiente. Por lo tanto, la información completa de una sesión cualquiera s_i puede resumirse por una terna $T_i = (\alpha_i, \beta_i, K_i)$. Estas sesiones pueden corresponder a sesiones KAS STS entre dos usuarios cualesquiera. En la hipótesis se supone que Omar ha podido obtener una secuencia finita $\mathcal{T}$ consistente en r ternas T_i. El atacante Omar podría obtener $\mathcal{T}$, participando él mismo en sesiones con otros participantes si es un socio no honesto con un certificado válido o robando las claves de otras sesiones, ya que, como KAS STS es un esquema de identificación segura, no

tiene otra opción. Obtener el valor de K_i implica resolver CDHP$(\lambda, \alpha_i, \beta_i)$ (ver sección 2.2.1) y obtener alguna información sobre K_i implica poder resolver DDHP$(\lambda, \alpha_i, \beta_i)$ (ver sección 2.2.2).

Supongamos que, a partir de $\mathcal{T}$, Omar quiere obtener la clave K de una sesión dada entre dos usuarios Ana y Ben.

Supongamos que existiese un algoritmo $\mathcal{A}$ de la forma

$$\mathcal{A}(\mathcal{T}, \alpha, \beta),$$

que en tiempo polinomial permitiese a Omar obtener alguna información sobre la clave de sesión K.

A continuación demostraremos que si DDHP (ver sección 2.2.2) es inviable, un algoritmo de tales características no podría existir.

La idea de la demostración es que si Omar conociese un algoritmo $\mathcal{A}$ como el descripto anteriormente, también podría resolver DDHP(λ, α, β), contradiciendo la hipótesis.

En efecto, sin tomar parte en sesiones extra ni obtener claves de sesión conocidas, Omar puede obtener una lista $\mathcal{T}'$ de ternas simuladas de la forma:

$$T' = (\alpha'_i, \beta'_i, K'_i),$$

donde Omar realiza:

$$a'_i = \text{rand}(q), \alpha'_i = \lambda^{a'_i}. \tag{3.6.2}$$

$$b'_i = \text{rand}(q), \beta'_i = \lambda^{b'_i}. \tag{3.6.3}$$

$$K'_i = (\beta'_i)^{a'_i} \text{ y define } T' = (\alpha'_i, \beta'_i, K'_i). \tag{3.6.4}$$

La diferencia sustancial de la simulación $\mathcal{T}'$ consiste en que se sustituye la elección aleatoria de un socio honesto por una elección aleatoria de Omar.

Como Omar determina a'_i y b'_i con la misma distribución de probabilidad uniforme, resulta que una lista $\mathcal{T}'$ es indistinguible de otra preparada a partir de sesiones reales como $\mathcal{T}$. Por lo tanto las salidas de $\mathcal{A}(\mathcal{T}, \alpha, \beta)$, tienen la misma distribución de probabilidad que las de $\mathcal{A}(\mathcal{T}', \alpha'_i, \alpha'_i)$. Por lo tanto, la posibilidad de conocer un algoritmo (de tiempo polinomial) $\mathcal{A}$, sería equivalente a resolver DDHP en tiempo polinomial.

Sin embargo, esta posibilidad no es factible sin contradecir la hipótesis del lema. □

3.7. El esquema de acuerdo de claves por intercambio cifrado con contraseña

Este esquema consiste en el acuerdo de claves Diffie–Hellman pero la información viaja cifrada por una contraseña acordada previamente. Esto puede simplificar la administración de claves cuando son contraseñas fáciles de recordar por los usuarios. Requiere KPS con las contraseñas. Se considera un grupo cíclico $\langle\lambda\rangle$ de orden q. TA distribuye previamente las contraseñas y las funciones de cifrado $e_p()$ y descifrado $d_p()$. Los pasos necesarios para una sesión se describen en el Protocolo 3.7.1.

1. $\text{Ben} : a = \text{rand}(q), \quad \alpha = \lambda^a, \quad y_{\text{Ana}} = e_p(\alpha), \quad (\text{“Ana”}, y_{\text{Ana}}) \longrightarrow \text{Ben}$
2. $\text{Ben} : b = \text{rand}(q), \quad \beta = \lambda^b, \quad y_{\text{Ben}} = e_p(\beta), \quad (\text{“Ben”}, y_{\text{Ben}}) \longrightarrow \text{Ana}$
3. $\text{Ana} : \beta = d_p(y_{\text{Ben}}), \quad K = \beta^a$
4. $\text{Ben} : \alpha = d_p(y_{\text{Ana}}), \quad K = \alpha^b$

PROTOCOLO 3.7.1. KAS por contraseña.

Bibliografía

[Ass00] Network Associates, *Introduction to Cryptography*, ftp://ftp.pgpi.org/pub/pgp/7.0/docs/english/IntroToCrypto.pdf, 2000.

[BB10] Riccardo Bresciani and Andrew Butterfield, *ProVerif Analysis of the ZRTP Protocol*, Tech. report, Foundations and Methods Group, Trinity College Dublin Lero – the Irish Software Engineering Research Centre, bresciar@scss.tcd.ie, Andrew.Butterfield@scss.tcd.ie, September 2010, Ver http://infonomics-society.org/IJ/ProVerif Analysis of the ZRTP Protocol.pdf.

[Boy06] Xavier Boyen, *The BF Identity-Based Encryption System*, http://grouper.ieee.org/groups/1363/IBC/submissions/Boyen-bf_ieee.pdf, August 2006.

[Bre07] Riccardo Bresciani, *The ZRTP Protocol Security Considerations*, Research Report LSV-07-20, Laboratoire Spécification et Vérification, Ecole Normale Supérieure de Cachan, CNRS, 61, avenue du Président Wilson 94235 Cachan Cedex France, May 2007, Ver http://www.lsv.ens-cachan.fr/Publis/RAPPORTS_LSV/PDF/rr-lsv-2007-20.pdf.

[ETS11] ETSI, *Mobile technologies gsm*, 2011, Ver http://www.etsi.org/index.php/technologies-clusters/technologies/mobile/gsm.

[Jud94] T.W. Judson, *Abstract algebra: Theory and applications*, The Prindle, Weber & Schmidt Series in Advanced Mathematics, PWS Publishing Company, 1994.

[KHPC01] Richard Kuhn, Vincent Hu, Timothy Polk, and Shu-Jen Chang, *NIST SP 800-32, Introduction to Public Key Technology*, "http://csrc.nist.gov/publications/nistpubs/800-32/sp800-32.pdf", February 2001, p. 5.

[LN97] Rudolf Lidl and Harald Niederreiter, *Finite fields*, second ed., Encyclopedia of Mathematics and its Applications, vol. 20, Cambridge University Press, Cambridge, 1997, With a foreword by P. M. Cohn. MR 1429394 (97i:11115)

[Lut08] Martin Luther, *Introduction to Identity Based-Encryption*, first ed., Discrete Mathematics and its Applications (Boca Raton), Artech House Publishers, 2008, Theory and practice.

[NIS11] NIST, *Glossary of Key Information Security Terms*, "http://cacr.uwaterloo.ca/~dstinson/CS_758/2007/Schnorr-soundness.pdf", February 2011, pp. 86–87.

[Pan08] A.M. Panait, *Security aspects of zero knowledge identification schemes*, McGill University, 2008.

[PM08] Valentín.V Petrov and Ernesto Mordecki, *Teoría de la probabilidad*, 2 ed., Dirac (Facultad de Ciencias UDELAR), 2008.

[Sha49] C. E. Shannon, *Communication theory of secrecy systems*, Bell System Tech. J. **28** (1949), 656–715. MR 0032133 (11,258d)

[Ste09] W.A. Stein, *Elementary number theory: Primes, congruences, and secrets*, Undergraduate texts in mathematics, Springer London, Limited, 2009.

[Sti06] Douglas R. Stinson, *Cryptography*, third ed., Discrete Mathematics and its Applications (Boca Raton), Chapman & Hall/CRC, Boca Raton, FL, 2006, Theory and practice. MR 2182472 (2007f:94060)

[Sti07] ———, *On the soundness of the Schnorr Scheme*, Preprint, http://cacr.uwaterloo.ca/~dstinson/CS_758/2007/Schnorr-soundness.pdf, January 2007.

Índice alfabético