Pretty Good Privacy

Murillo Vizcardo Luis Enrique
Lipa Urbina Edson Victor
Salcedo Almiron Melvin David

Universidad Nacional de San Agustin

Tabla de Contenidos

PRETTY GOOD PRIVACY

PRETTY GOOD PRIVACY

- PGP es un paquete de software de código abierto y de libre disponibilidad para la seguridad del correo electrónico. Proporciona autenticación a través del uso de firma digital, confidencialidad mediante el uso de encriptación de bloque simétrico, compresión mediante el algoritmo ZIP y compatibilidad de correo electrónico utilizando el esquema de codificación radix-64.
- PGP brinda un servicio de confidencialidad y autenticación que se puede usar para correo electrónico y aplicaciones de almacenamiento de archivos.
- PGP es un fenómeno notable. En gran parte, el esfuerzo de una sola persona, Phil Zimmermann, PGP brinda un servicio de confidencialidad y autenticación que se puede usar para correo electrónico y aplicaciones de almacenamiento de archivos.

PRETTY GOOD PRIVACY

1. Seleccionó los mejores algoritmos criptográficos disponibles como bloques de construcción.
2. Integra estos algoritmos en una aplicación de propósito general que es independiente del sistema operativo y el procesador y que se basa en un pequeño conjunto de comandos fáciles de usar.
3. Hizo que el paquete y su documentación, incluido el código fuente, estén disponibles gratuitamente a través de Internet, tableros de anuncios y redes comerciales como AOL (America On Line).
4. Se llegó a un acuerdo con una empresa (Viacrypt, ahora Network Associates) para proporcionar una versión comercial de PGP totalmente compatible y de bajo costo.

PRETTY GOOD PRIVACY

1. Está disponible de forma gratuita .
2. Se basa en algoritmos que han sobrevivido a una amplia revisión pública y se consideran extremadamente seguros. Específicamente, el paquete incluye RSA, DSS y Diffie-Hellman para encriptación de clave pública; CAST-128, IDEA y 3DES para encriptación simétrica; y SHA-1 para codificación hash.
3. Tiene una amplia gama de aplicabilidad, desde empresas que desean seleccionar y aplicar un esquema estandarizado para encriptar archivos y mensajes a personas que desean comunicarse de forma segura con otras personas en todo el mundo a través de Internet y otras redes.
4. No fue desarrollado ni está bajo el control de ninguna organización gubernamental o de estándares.

AUTENTICACIÓN

- SHA-1 se utiliza para generar un código hash de 160 bits del mensaje
- El código hash se cifra con RSA utilizando la clave privada del remitente

AUTENTICACIÓN

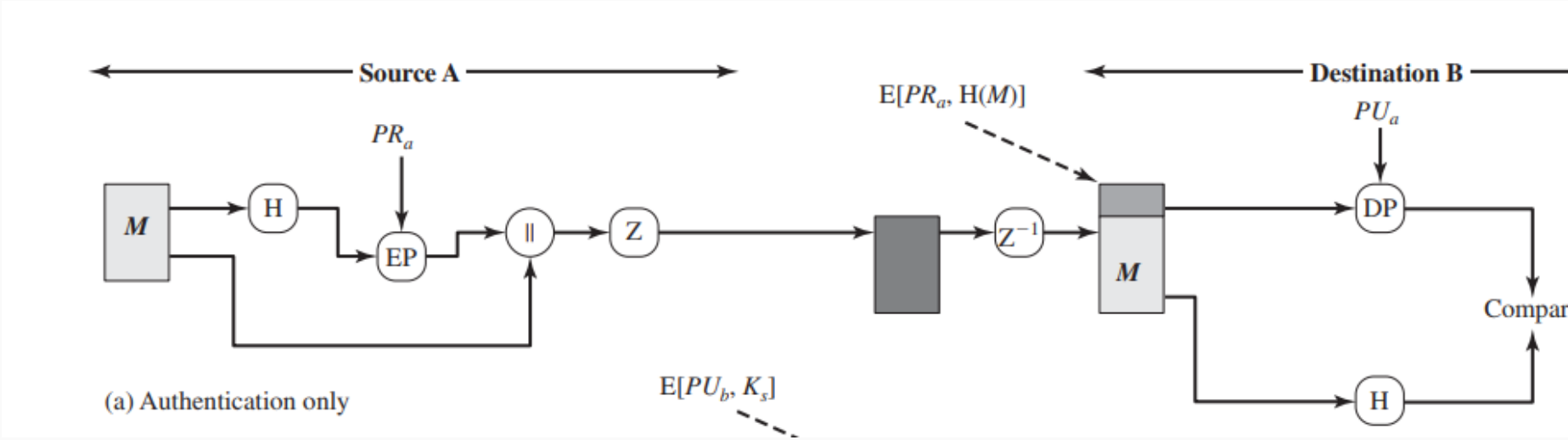


Figure 1: autentificacion

CONFIDENCIALIDAD

- El remitente genera un mensaje y un número aleatorio de 128 bits para ser utilizado como clave de sesión solo para este mensaje.
- El mensaje se cifra con CAST-128 (o IDEA o 3DES) con la clave de sesión.
- La clave de sesión se cifra con RSA usando la clave pública del destinatario y se antepone al mensaje.

CONFIDENCIALIDAD

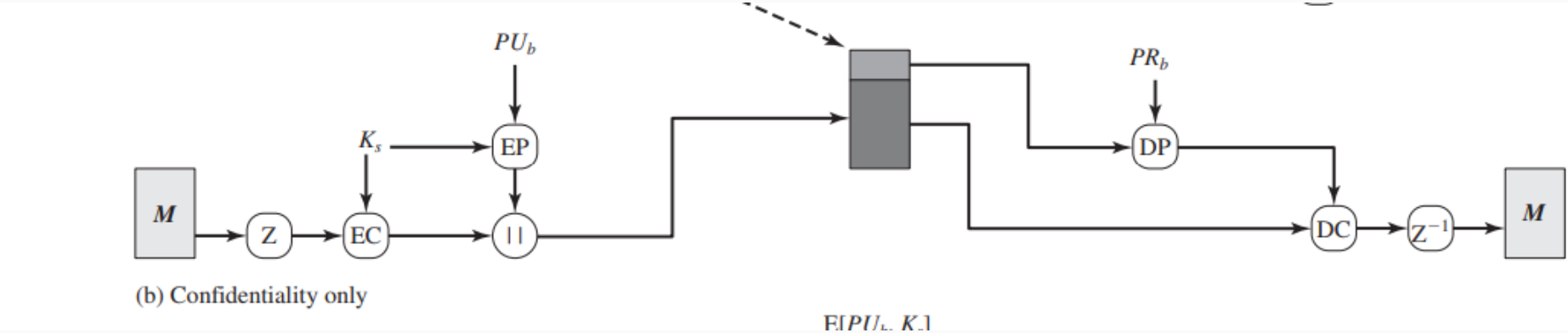


Figure 2: confidencialidad

AUTENTICACIÓN y CONFIDENCIALIDAD

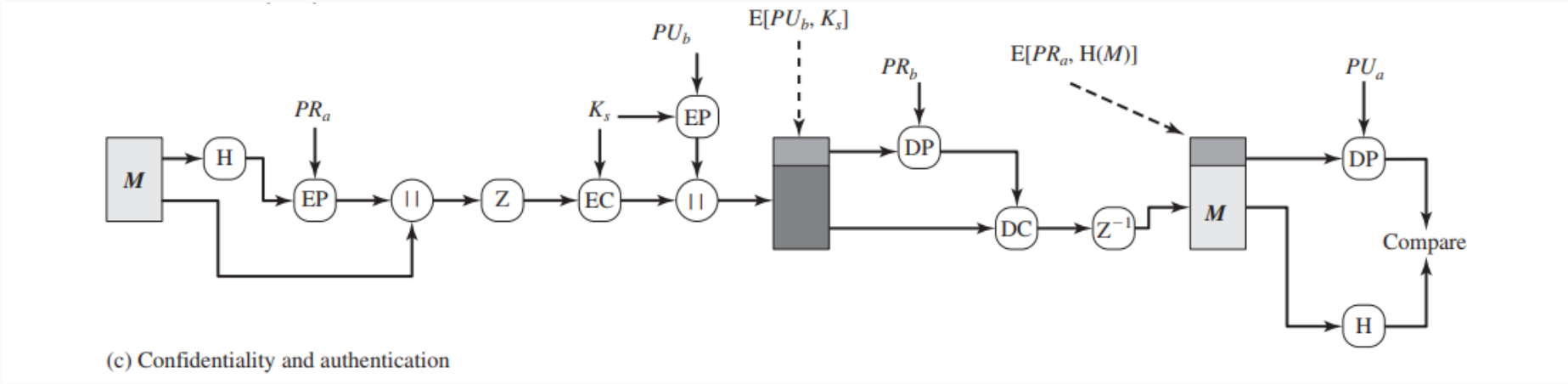
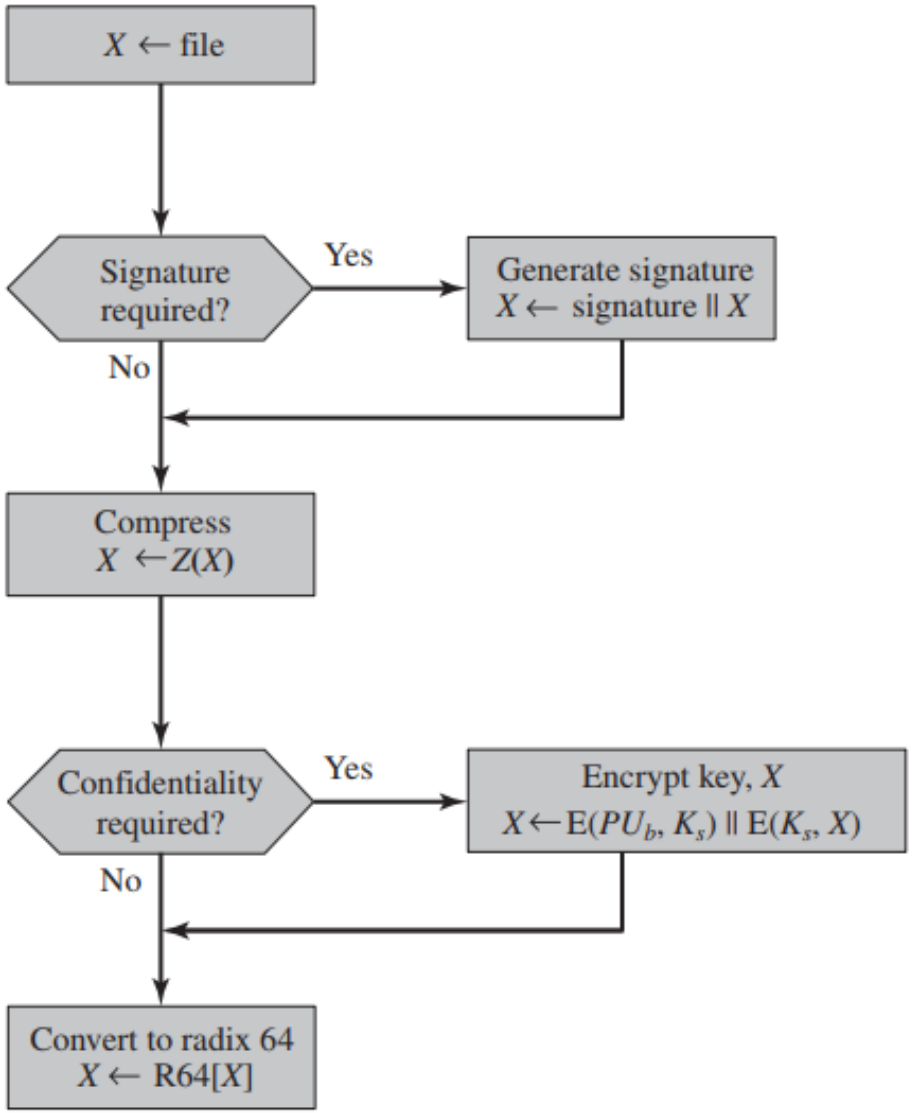


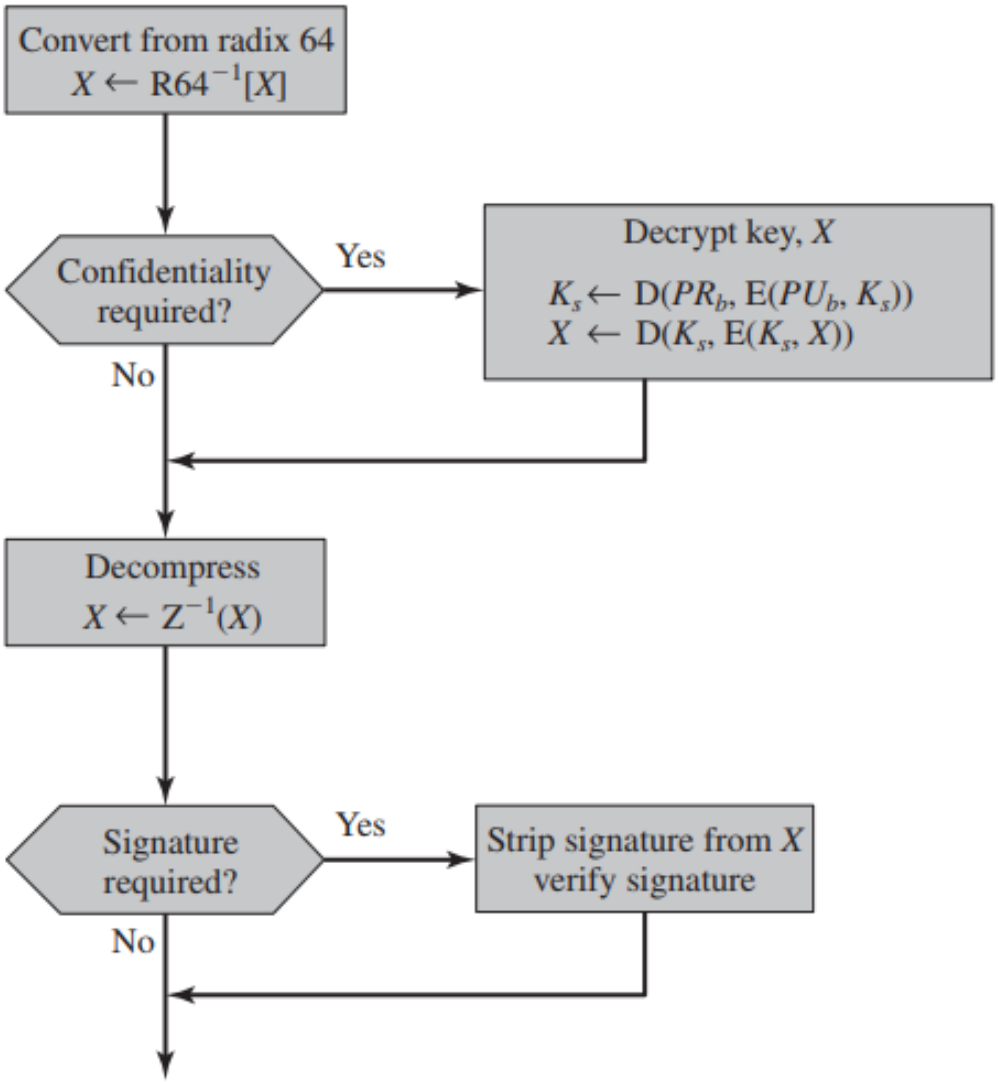
Figure 3: AUTENTICACIÓN y CONFIDENCIALIDAD

COMPATIBILIDAD DE CORREO ELECTRÓNICO



(a) Generic transmission diagram (from A)

COMPATIBILIDAD DE CORREO ELECTRÓNICO



(b) Generic reception diagram (to B)

Cryptographic Keys and Key Rings

Cryptographic Keys and Key Rings

- claves simétricas de sesión únicas.
- claves públicas.
- claves privadas
- claves simétricas basadas en frase de contraseña

Cryptographic Keys and Key Rings

requisitos respecto a estas claves.

- Se necesita un medio para generar claves de sesión impredecibles.
- Un usuario puede tener múltiples pares de claves pública / claves privada (El usuario puede desear cambiar su par de claves de vez en cuando).
- Cada entidad de PGP debe mantener un archivo de sus pares de claves públicas / privadas, así como un archivo de claves públicas de corresponsales.

Cryptographic Keys and Key Rings (SESSION KEY GENERATION)

GENERACIÓN DE LAS CLAVES DE SESIÓN

- Cada clave de sesión está asociada a un solo mensaje y se usa solo con el fin de cifrar y descifrar ese mensaje (algoritmo de cifrado simétrico)(CAST-128).
- El resultado es producir una secuencia de claves de sesión que sea efectivamente impredecible.

Cryptographic Keys and Key Rings (KEY IDENTIFIERS)

IDENTIFICADORES CLAVE

- .Un mensaje cifrado va acompañado de una clave cifrada de la clave de sesión.
- La clave de sesión está encriptada con la clave pública del destinatario. Por lo tanto, solo el destinatario podrá recuperar la clave de sesión y, por lo tanto, recuperar el mensaje.
- Si cada usuario empleara un solo par de claves pública / privada, el destinatario sabría automáticamente qué clave usar para descifrar la clave de sesión. Sin embargo, hemos establecido un requisito de que cualquier usuario dado puede tener múltiples pares de claves públicas / privadas.

Cryptographic Keys and Key Rings

- ¿Cómo sabe el destinatario cuál de sus claves públicas se utilizó para encriptar la clave de sesión?
- Una solución simple sería transmitir la clave pública con el mensaje. El destinatario podría verificar que es una de sus claves públicas, y proceder.
- Este esquema funcionaría, pero desperdiciaría espacio. Una clave pública RSA puede tener cientos de dígitos decimales de longitud.

Cryptographic Keys and Key Rings

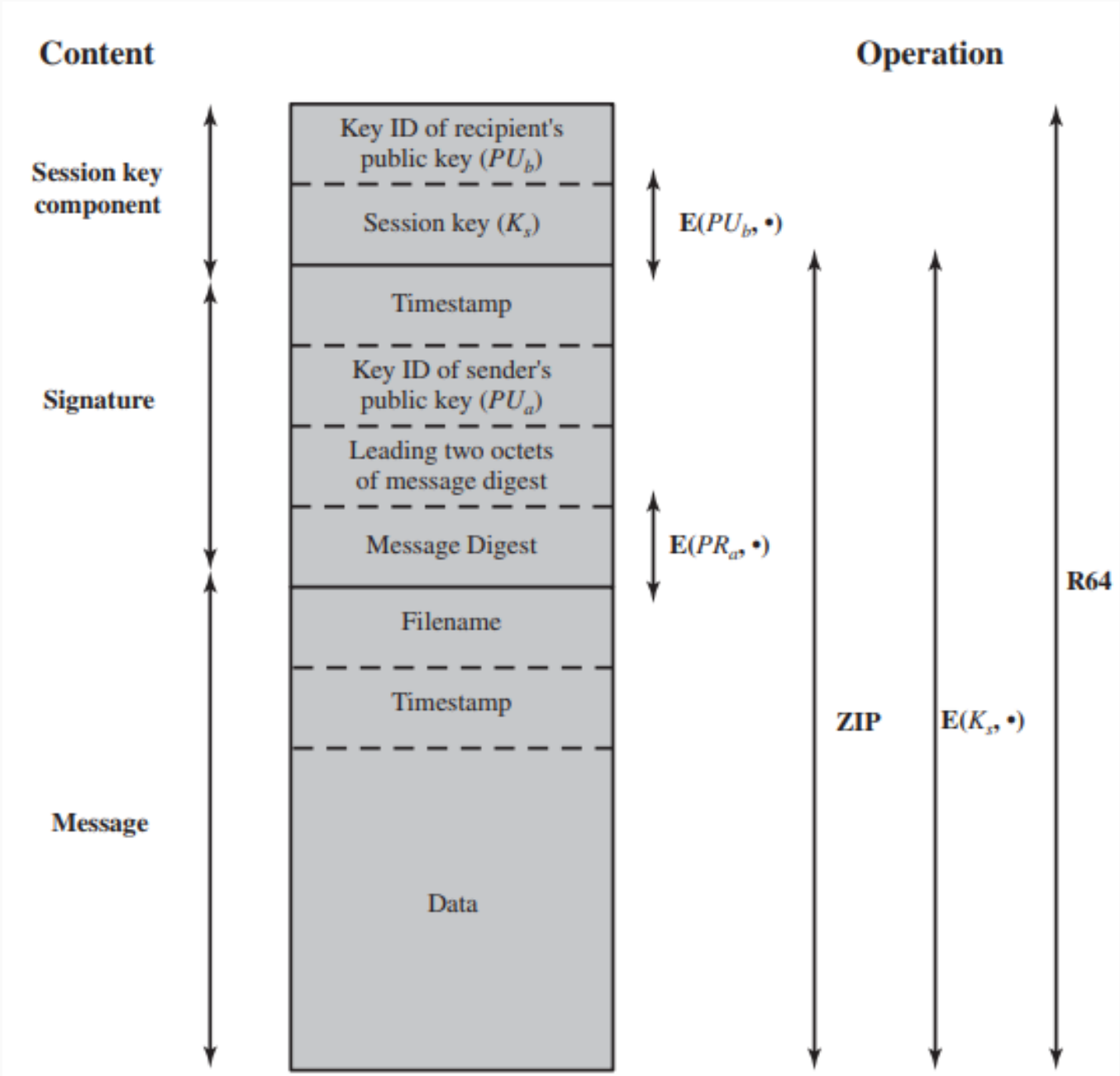
- La solución adoptada por PGP es asignar una ID de clave a cada clave pública (única dentro de una ID de usuario)
- La ID de clave asociada con cada clave pública consiste en sus 64 bits menos significativos.
- Es decir, la ID de clave pública(PU_a) es ($PU_a \bmod 2^{64}$). Esta es una longitud suficiente para que la probabilidad de identificadores de claves duplicadas sea muy pequeña.
- También se requiere una identificación de clave para la firma digital de PGP. Debido a que un remitente puede usar una de una serie de claves privadas para encriptar el resumen del mensaje.

Cryptographic Keys and Key Rings

Formato de un mensaje transmitido

- Componente de mensaje
  - datos reales que se almacenarán o transmitirán, así como un nombre de archivo y una marca de tiempo .
- componente firma (opcional)
  - Marca de tiempo: hora a la que se realizó la firma.
  - Resumen del mensaje:
    - El resumen SHA-1 de 160 bits cifrado con la clave de firma privada del remitente.
    - El resumen se calcula sobre la marca de tiempo de la firma concatenada con la porción de datos del componente del mensaje.
    - La inclusión de la marca de tiempo de la firma en el resumen nos asegura contra los tipos de ataques repetidos.

Cryptographic Keys and Key Rings



Cryptographic Keys and Key Rings

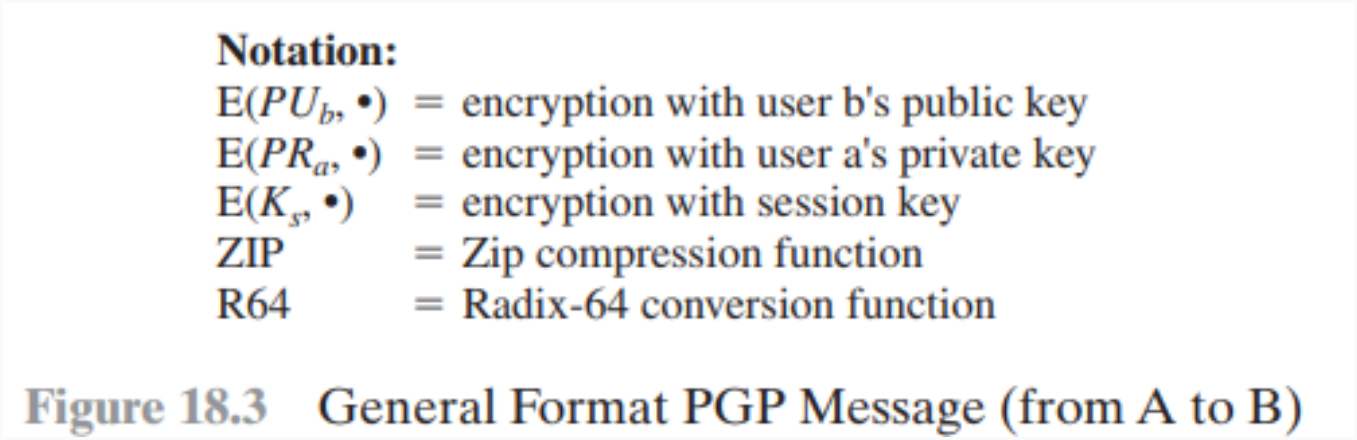


Figure 5: Mi Figura

Cryptographic Keys and Key Rings

Dos octetos de resumen de mensaje:

- Permite al destinatario determinar si se utilizó la clave pública correcta para descifrar el resumen del mensaje para la autenticación.

ID de clave de la clave pública del remitente

- identifica la clave pública que se debe usar para descifrar el resumen del mensaje.

Cryptographic Keys and Key Rings

- El componente de mensaje y el componente de firma opcional se pueden comprimir usando ZIP y se pueden encriptar usando una clave de sesión.

El componente clave de la sesión

- incluye la clave de sesión y el identificador de la clave pública del destinatario que el remitente utilizó para cifrar la clave de sesión. Todo el bloque generalmente está codificado con codificación radix-64

Cryptographic Keys and Key Rings (KEY RINGS)

KEY RINGS

- .Se incluyen dos ID de clave en cualquier mensaje de PGP que proporcione confidencialidad y autenticación. Estas claves deben almacenarse y organizarse de manera sistemática para que todas las partes las utilicen de manera eficiente y efectiva.
- El esquema utilizado en PGP es proporcionar un par de estructuras de datos en cada nodo, una para almacenar los pares de claves públicas / privadas propiedad de ese nodo y otra para almacenar las claves públicas de otros usuarios conocidos en este nodo. Estas estructuras de datos se denominan, respectivamente, como el anillo de clave privada y el anillo de clave pública

Cryptographic Keys and Key Rings (KEY RINGS)

Private-Key Ring

Timestamp	Key ID*	Public Key	Encrypted Private Key	User ID*
• • •	• • •	• • •	• • •	• • •
T_i	$PU_i \bmod 2^{64}$	PU_i	$E(H(P_i), PR_i)$	User i
• • •	• • •	• • •	• • •	• • •

Figure 6: Mi Figura

Cryptographic Keys and Key Rings (KEY RINGS)

- Marca de tiempo: la fecha / hora en que se generó este par de claves.
- ID de clave: los 64 bits menos significativos de la clave pública para esta entrada.
- Clave pública: la porción de clave pública del par.
- Clave privada: la parte de clave privada del par; este campo está encriptado.
- ID de usuario: por lo general, esta será la dirección de correo electrónico del usuario (por ejemplo, stallings@acm.org). Sin embargo, el usuario puede elegir asociar un nombre diferente con cada par (por ejemplo, Stallings, WStallings, WilliamStallings, etc.) o reutilizar el mismo ID de usuario más de una vez.

Cryptographic Keys and Key Rings (KEY RINGS)

Public-Key Ring

Timestamp	Key ID*	Public Key	Owner Trust	User ID*	Key Legitimacy	Signature(s)	Signature Trust(s)
• • •	• • •	• • •	• • •	• • •	• • •	• • •	• • •
T_i	$PU_i \bmod 2^{64}$	PU_i	trust_flag_i	User i	trust_flag_i		
• • •	• • •	• • •	• • •	• • •	• • •	• • •	• • •

Figure 7: Mi Figura

Cryptographic Keys and Key Rings (KEY RINGS)

- Marca de tiempo: la fecha / hora en que se generó esta entrada.
- ID de clave: los 64 bits menos significativos de la clave pública para esta entrada.
- Clave pública: la clave pública para esta entrada.
- ID de usuario: identifica al propietario de esta clave. Se pueden asociar múltiples ID de usuario con una sola clave pública

Cryptographic Keys and Key Rings (KEY RINGS)

- La clave privada está encriptada usando CAST-128 (o IDEA o DES). El procedimiento es el siguiente:

Cryptographic Keys and Key Rings (KEY RINGS)

- El usuario selecciona una frase de contraseña que se utilizará para cifrar claves privadas.
- Cuando el sistema genera un nuevo par de claves pública / privada utilizando RSA, le pide al usuario la frase de contraseña. Con SHA-1, se genera un código hash de 160 bits a partir de la frase de contraseña, y la frase de contraseña se descarta.
- El sistema encripta la clave privada usando CAST-128 con los 128 bits del código hash como clave. El código hash se descarta y la clave privada encriptada se almacena en el anillo de clave privada.

Cryptographic Keys and Key Rings (KEY RINGS)

- Posteriormente, cuando un usuario accede al anillo de clave privada para recuperar una clave privada, él o ella debe proporcionar la frase de contraseña. PGP recuperará la clave privada encriptada, generará el código hash de la frase de contraseña y descifrará la clave privada encriptada utilizando CAST-128 con el código hash.la seguridad de este sistema depende de la seguridad de la contraseña, el usuario debe usar una frase de contraseña que no se adivina fácilmente pero que se recuerda fácilmente.
- La estructura clave pública se usa para almacenar claves públicas de otros usuarios que son conocidas por este usuario.

transmisión de mensajes

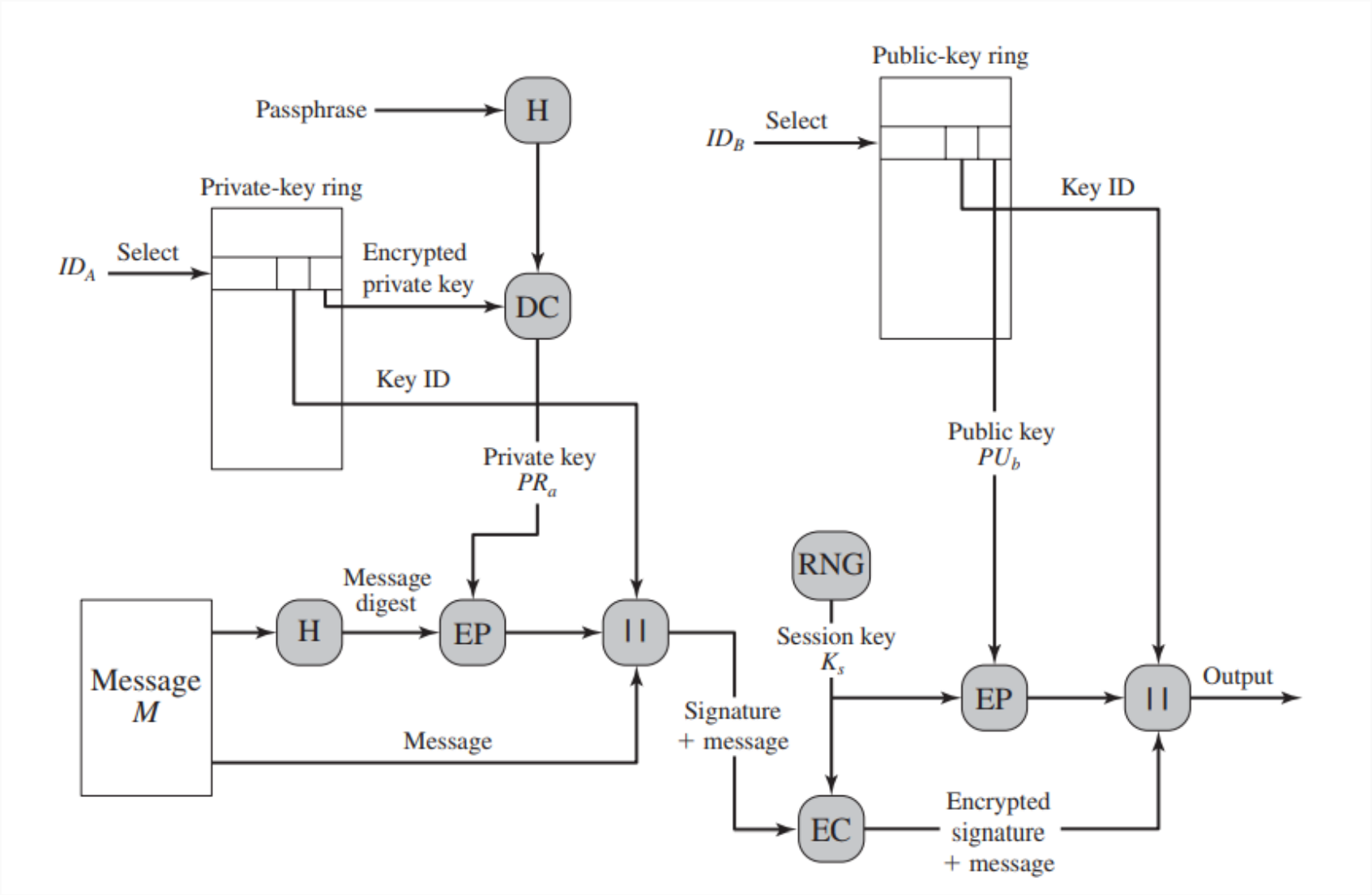


Figure 8: Mi Figura

Cryptographic Keys and Key Rings (KEY RINGS)

Firmando el mensaje:

- PGP recupera la clave privada del remitente del anillo de clave privada usando your_userid como índice. Si your_userid no se proporcionó en el comando, se recupera la primera clave privada del anillo.
- PGP solicita al usuario la frase de contraseña para recuperar la clave privada no encriptada.
- El componente de firma del mensaje está construido.

Cifrando el mensaje:

- PGP genera una clave de sesión y encripta el mensaje.
- PGP recupera la clave pública del destinatario del anillo de clave pública utilizando her_userid como índice.
- El componente clave de sesión del mensaje está construido.

La entidad PGP receptora realiza los siguientes pasos
Descifrar el mensaje:

- PGP recupera la clave privada del receptor del anillo de clave privada usando el campo ID de clave en el componente clave de sesión del mensaje como índice.
- PGP solicita al usuario la frase de contraseña para recuperar la clave privada no encriptada.
- PGP recupera la clave de sesión y descifra el mensaje

Autenticando el mensaje:

- PGP recupera la clave pública del remitente del anillo de clave pública utilizando el campo ID de clave en el componente clave de firma del mensaje como índice.
- PGP recupera el resumen del mensaje transmitido
- PGP calcula el resumen del mensaje para el mensaje recibido y lo compara con el resumen del mensaje transmitido para autenticarse.

Cryptographic Keys and Key Rings (KEY RINGS)

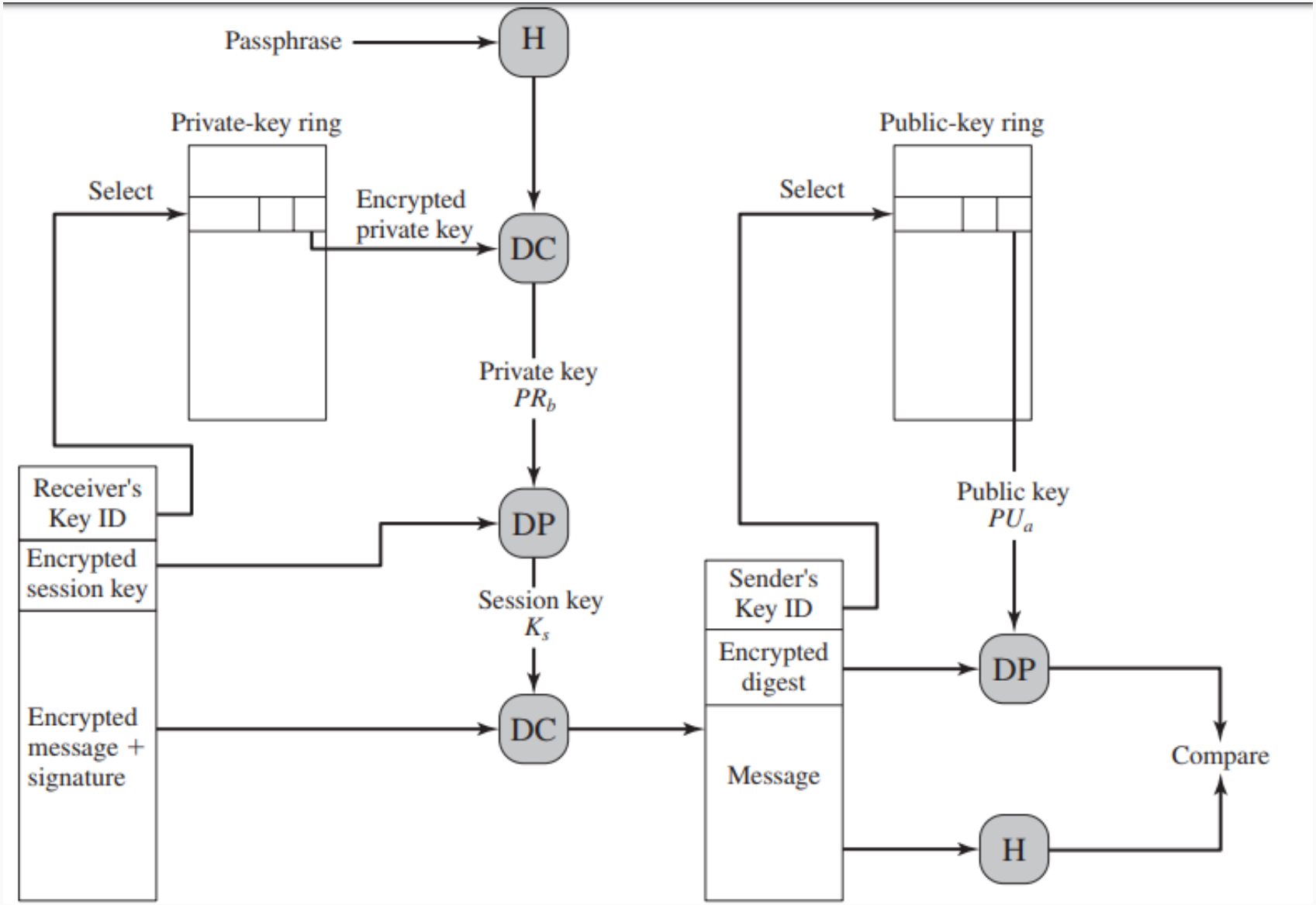


Figure 9: Mi Figura

Gestión de clave pública

Gestión de clave pública

Todo este asunto de proteger las claves públicas de la manipulación indebida es el problema más difícil en las aplicaciones prácticas de clave pública. Es el ”talón de Aquiles” de la criptografía de clave pública, y una gran cantidad de complejidad de software está ligada a la solución de este problema.

Enfoque para la gestión de la clave pública

Una serie de enfoques son posibles para minimizar el riesgo de que el anillo de clave pública de un usuario contenga claves públicas falsas. Supongamos que A desea obtener una clave pública confiable para B. Los siguientes son algunos enfoques que podrían usarse.

Enfoque para la gestión de la clave pública

- Obtenga físicamente la clave de B. B podría almacenar su clave pública (PU b) en un disquete y entrégalo en A. A podría cargar la clave en su sistema desde el disquete. Este es un método muy seguro pero tiene limitaciones prácticas obvias.
- Verifique una llave por teléfono. Si A puede reconocer B en el teléfono, A podría llamar a B y pedirle que dicte la clave, en formato radix-64, por teléfono. Como una alternativa más práctica, B podría transmitir su clave en un mensaje de correo electrónico a A. A podría hacer que PGP genere un resumen SHA-1 de 160 bits de la clave y lo muestre en formato hexadecimal; esto se conoce como la ”huella dactilar” de la clave. A podría llamar a B y pedirle que dicte la huella digital por teléfono. Si las dos huellas dactilares coinciden, la clave se verifica.

Enfoque para la gestión de la clave pública

- Obtenga la clave pública de B de un individuo de confianza mutua D. Para este propósito, el introductor, D, crea un certificado firmado. El certificado incluye la clave pública de B, la hora de creación de la clave y un período de validez para la clave. D genera un resumen SHA-1 de este certificado, lo encripta con su clave privada y adjunta la firma al certificado. Debido a que solo D podría haber creado la firma, nadie más puede crear una clave pública falsa y pretender que está firmada por D. El certificado firmado podría enviarse directamente a A por B o D, o podría publicarse en un tablero de anuncios.
- Obtenga la clave pública de B de una autoridad de certificación confiable. Nuevamente, la autoridad crea y firma un certificado de clave pública. A podría acceder a la autoridad, proporcionando un nombre de usuario y recibiendo un certificado firmado.

El uso de la Confianza

La estructura básica es la siguiente:

- Un **campo clave de legitimidad** que indica en qué medida PGP confiará en que esta es una clave pública válida para este usuario; cuanto mayor sea el nivel de confianza, más fuerte será el enlace de esta identificación de usuario a esta clave.
- Un **campo de confianza de firma** que indica el grado en que este usuario PGP confía en el firmante para certificar claves públicas.
- Un **campo de confianza del propietario** que indica el grado en que se confía en esta clave pública para firmar otros certificados de clave pública; este nivel de confianza es asignado por el usuario.

El uso de la Confianza

(a) Trust Assigned to Public-Key Owner (appears after key packet; user defined)	(b) Trust Assigned to Public Key/User ID Pair (appears after User ID packet; computed by PGP)	(c) Trust Assigned to Signature (appears after signature packet; cached copy of OWNERTRUST for this signator)
OWNERTRUST Field —undefined trust —unknown user —usually not trusted to sign other keys —usually trusted to sign other keys —always trusted to sign other keys —this key is present in secret key ring (ultimate trust)	KEYLEGIT Field —unknown or undefined trust —key ownership not trusted —marginal trust in key ownership —complete trust in key ownership	SIGTRUST Field —undefined trust —unknown user —usually not trusted to sign other keys —usually trusted to sign other keys —always trusted to sign other keys —this key is present in secret key ring (ultimate trust)
BUCKSTOP bit —set if this key appears in secret key ring	WARNONLY bit —set if user wants only to be warned when key that is not fully validated is used for encryption	CONTIG bit —set if signature leads up a contiguous trusted certification path back to the ultimately trusted key ring owner

Figure 10: Contenido de la bandera de confianza

El uso de la Confianza

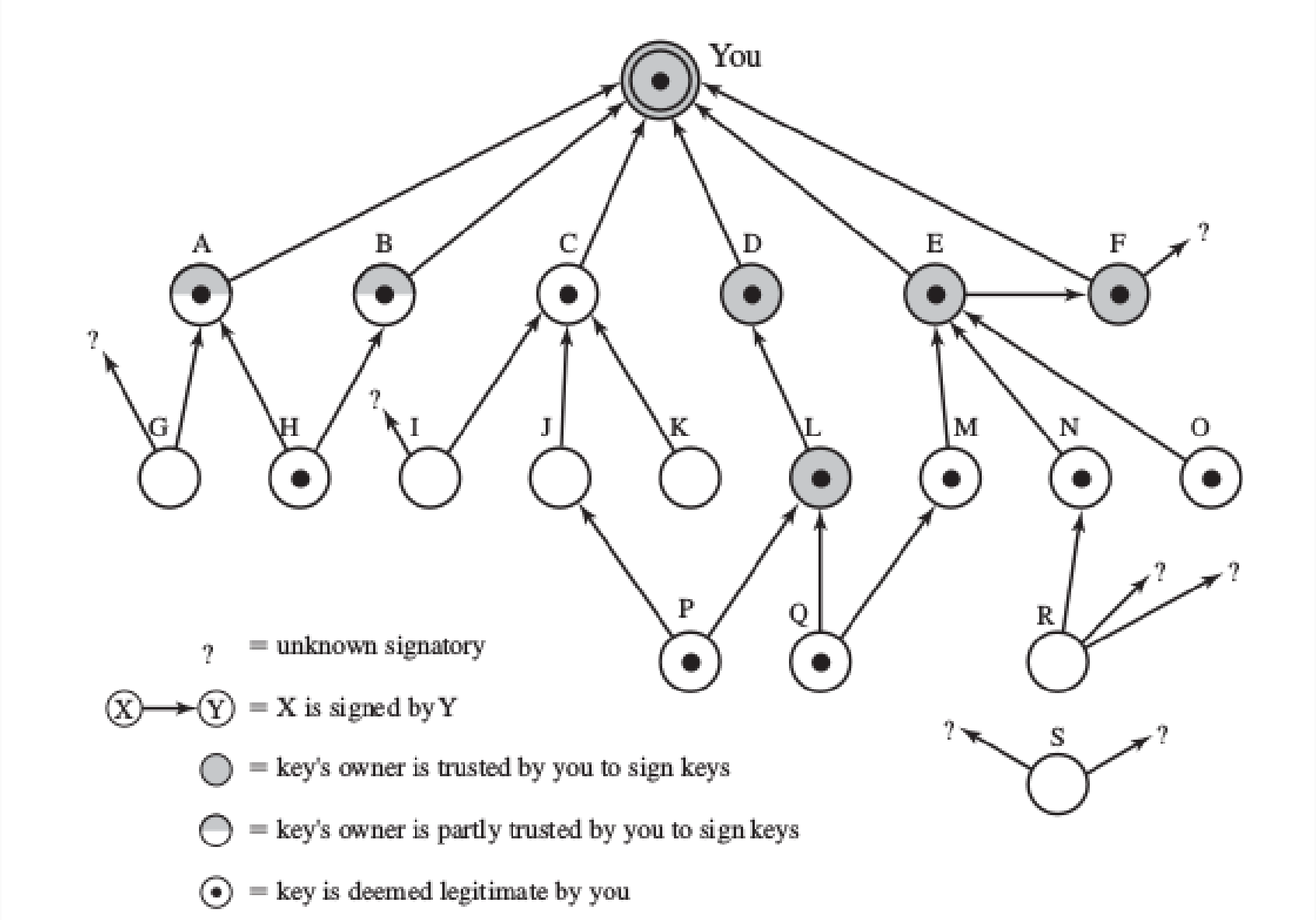


Figure 11: Modelo de Confanza de PGP

Bibliografía

- Cryptanalysis of 48-step RIPEMD-160
  https://tosc.iacr.org/index.php/ToSC/article/view/643
- On the Collision Resistance of RIPEMD-160 *
  https://pdfs.semanticscholar.org/0cda/303a042fbe199821ffedac1fb05cf
- RIPEMD-160:A Strengthened Version of RIPEMD
  https://homes.esat.kuleuven.be/ bosselae/ripemd160/pdf/AB-9601/AB-9601.pdf