

# *Criptografía y Seguridad de Datos*

## **Seguridad en el correo electrónico**

Carlos Figueira.

Universidad Simón Bolívar

*Basado en láminas del Profesor*

*Henric Johnson (<http://www.its.bth.se/staff/hjo/>*

*henric.johnson@bth.se)*

# Contenido

- *Pretty Good Privacy*
- *S/MIME*

# ***Pretty Good Privacy*** **(PGP)**

- Creado por Philip R. Zimmerman. Inicio de los 90.
- PGP provee servicios de confidencialidad y autenticación que puede ser usada para correo electrónico y aplicaciones de almacenamiento
- Evolución a partir de versiones 2.x

# PGP (cont.)

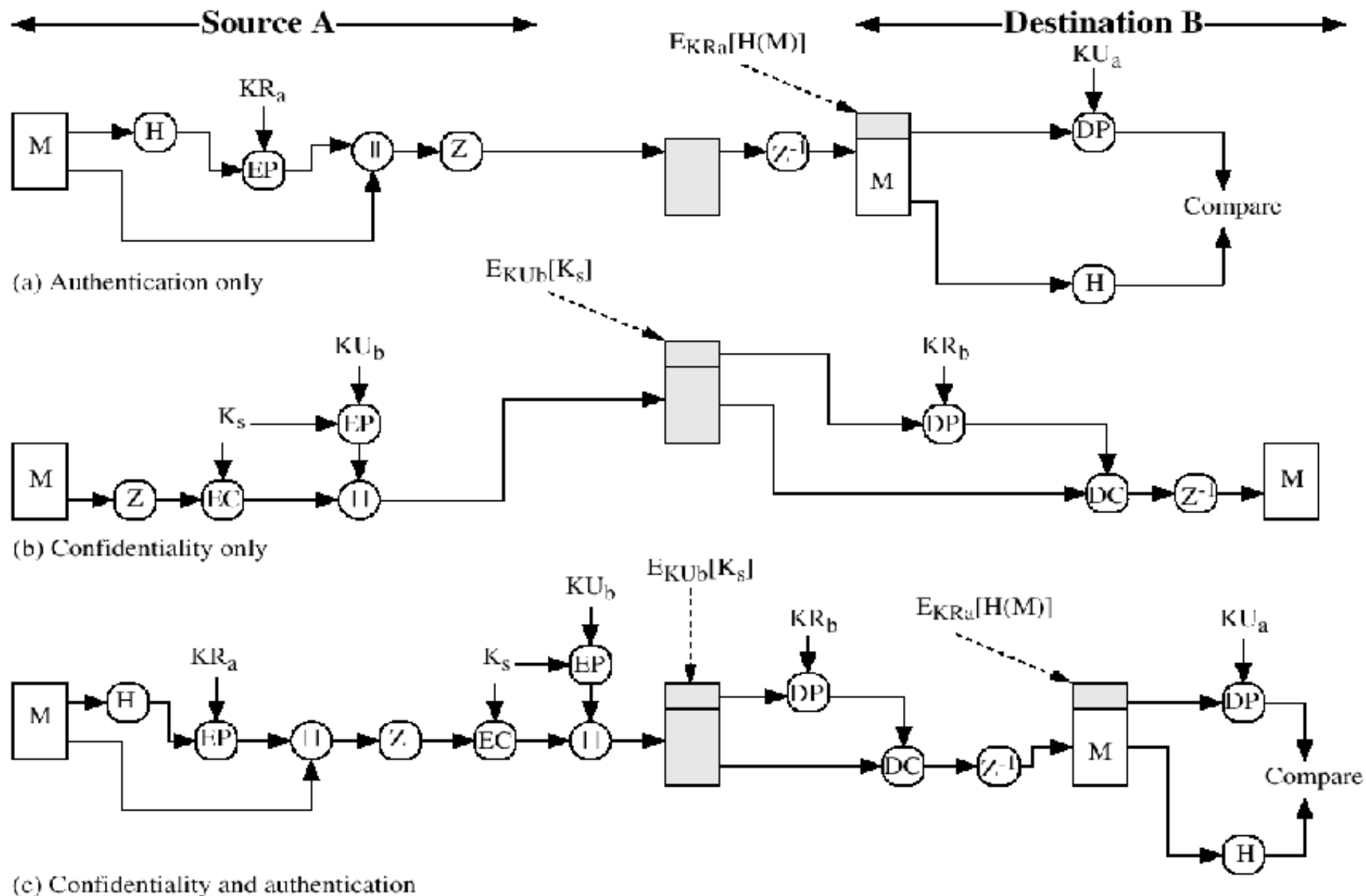
- Zimmerman vendió derechos comerciales a ViaCrypt (hoy parte de Symantec). Versiones pares eran libres (controladas por Zimmerman), las impares eran comerciales.
- RFC 2440. PGP Estándar (OpenPGP). Soportado por OpenPGP Alliance
- Cifrado simétrico (IDEA) y asimétrico (RSA)
- Soportado en clientes como pine, evolution, thunderbird, outlook, outlook express, etc

# ¿Por qué es tan popular PGP?

- Disponible gratuitamente para varias plataformas
- Basada en algoritmos conocidos
- Amplio rango de aplicabilidad
- No es desarrollado ni controlado por organizaciones gubernamentales o de estándares
- Llaveros

# Descripción Operacional

- Consiste de cinco servicios:
  - Autenticación
  - Confidencialidad
  - Compresión
  - E-mail compatibilidad
  - Segmentación



**Figure 5.1 PGP Cryptographic Functions**

Carlos Figueira

# Compresión

- PGP comprime el mensaje después de aplicar la firma pero antes de cifrar
- La ubicación de algoritmo de compresión es crítico (ZIP)

# Compatibilidad de E-mail

- El esquema usado es conversión radix-64 (3 bytes → 4 caracteres ASCII)
- El uso de radix-64 expande el mensaje en 33%.

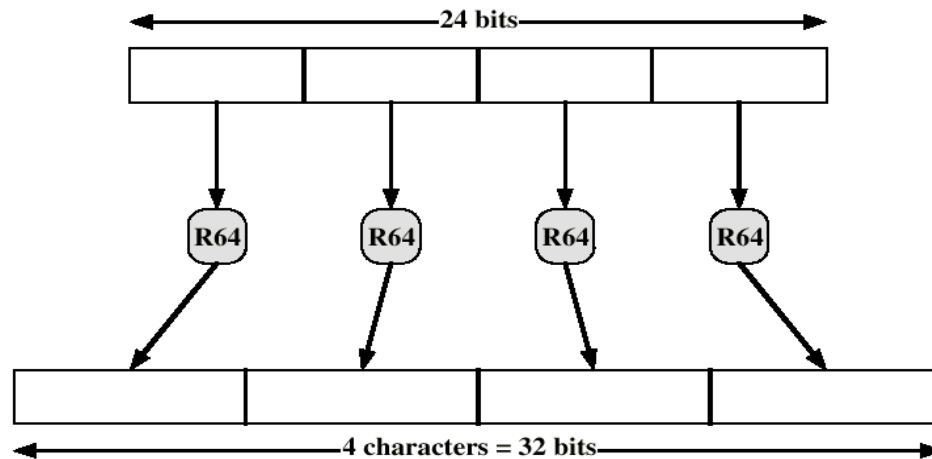


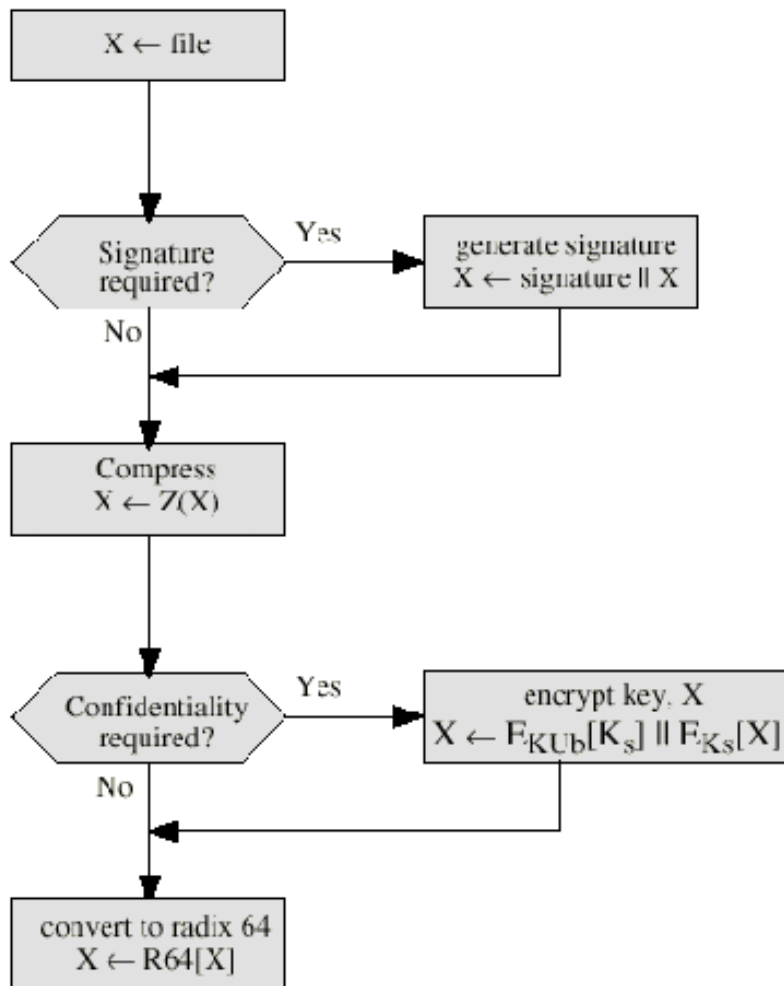
Figure 5.11 Printable Encoding of Binary Data into Radix-64 Format  
Carlos Figuiera

# Segmentación y reensamblaje

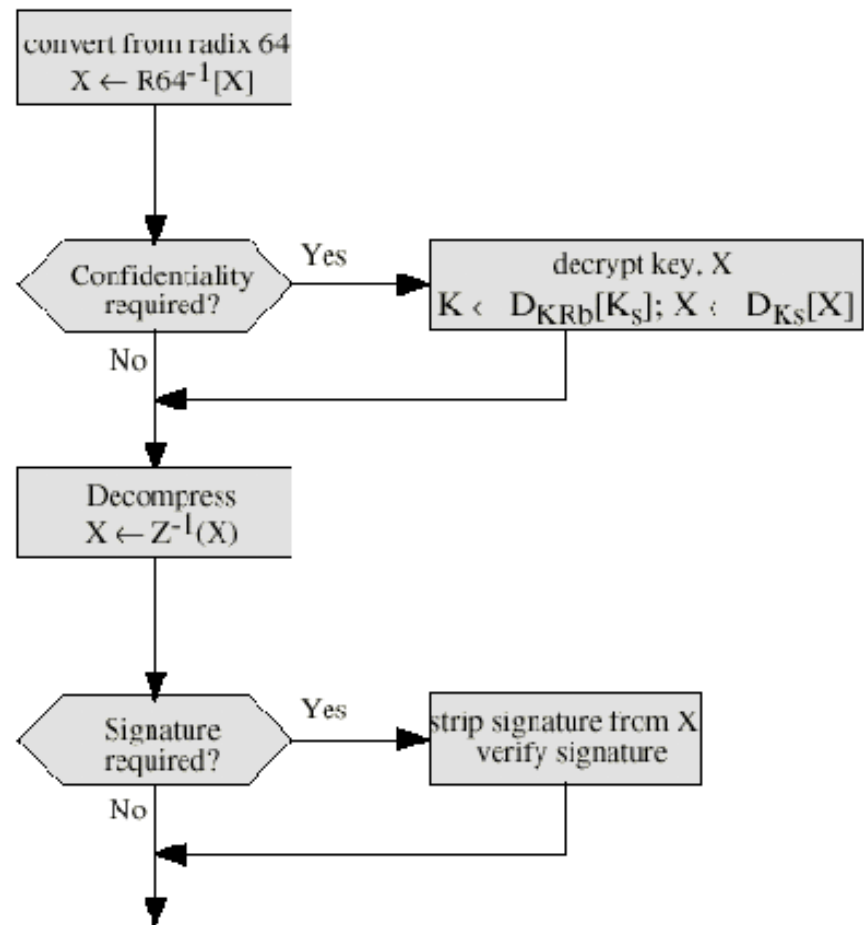
- Correo electrónico a menudo restringido a un tamaño máximo de mensaje de 50,000 octetos.
- Mensajes más largos deben ser divididos en segmentos. PGP automáticamente subdivide mensajes muy largos
- El receptor elimina todos los encabezados y reensambla bloque original.

# Resumen de servicios de PGP

- Firma: DSS/SHA, RSA/SHA
- Cifrado:
  - Simétrico: CAST o IDEA o 3DES
  - Asimétrico (para cifrar clave simétrica): Diffie-Hellman o RSA
- Compatibilidad email: Radix-64



(a) Generic Transmission Diagram (from A)



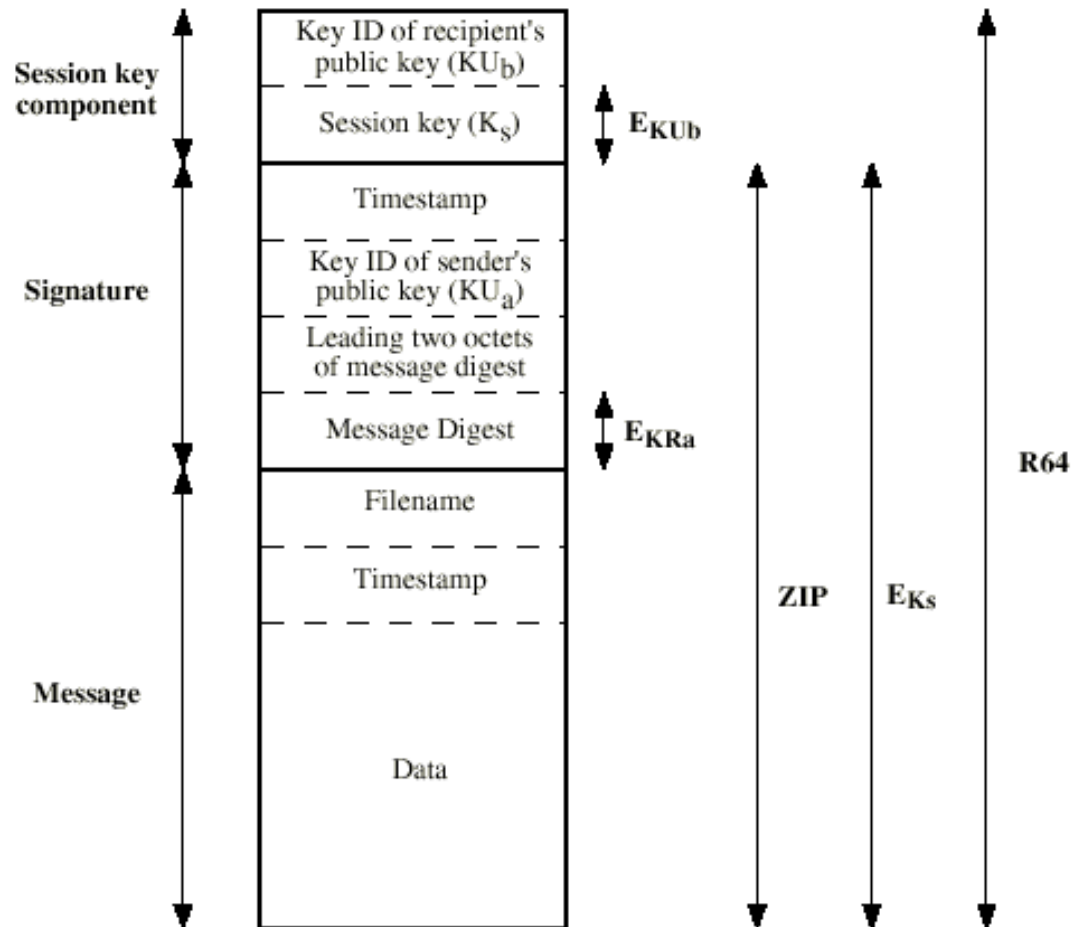
(b) Generic Reception Diagram (to B)

**Figure 5.2** Transmission and Reception of PGP Messages

# Format of PGP Message

Content

Operation



### Private Key Ring

Timestamp	Key ID*	Public Key	Encrypted Private Key	User ID*
•	•	•	•	•
•	•	•	•	•
•	•	•	•	•
$T_i$	$KU_j \bmod 2^{64}$	$KU_i$	$EH(P_i)[KR_i]$	User i
•	•	•	•	•
•	•	•	•	•
•	•	•	•	•

### Public Key Ring

Timestamp	Key ID*	Public Key	Owner Trust	User ID*	Key Legitimacy	Signature(s)	Signature Trust(s)
•	•	•	•	•	•	•	•
•	•	•	•	•	•	•	•
•	•	•	•	•	•	•	•
$T_i$	$KU_j \bmod 2^{64}$	$KU_i$	trust_flag <sub>i</sub>	User i	trust_flag <sub>i</sub>		
•	•	•	•	•	•	•	•
•	•	•	•	•	•	•	•
•	•	•	•	•	•	•	•

\* = field used to index table

**Figure 5.4 General Structure of Private and Public Key Rings**

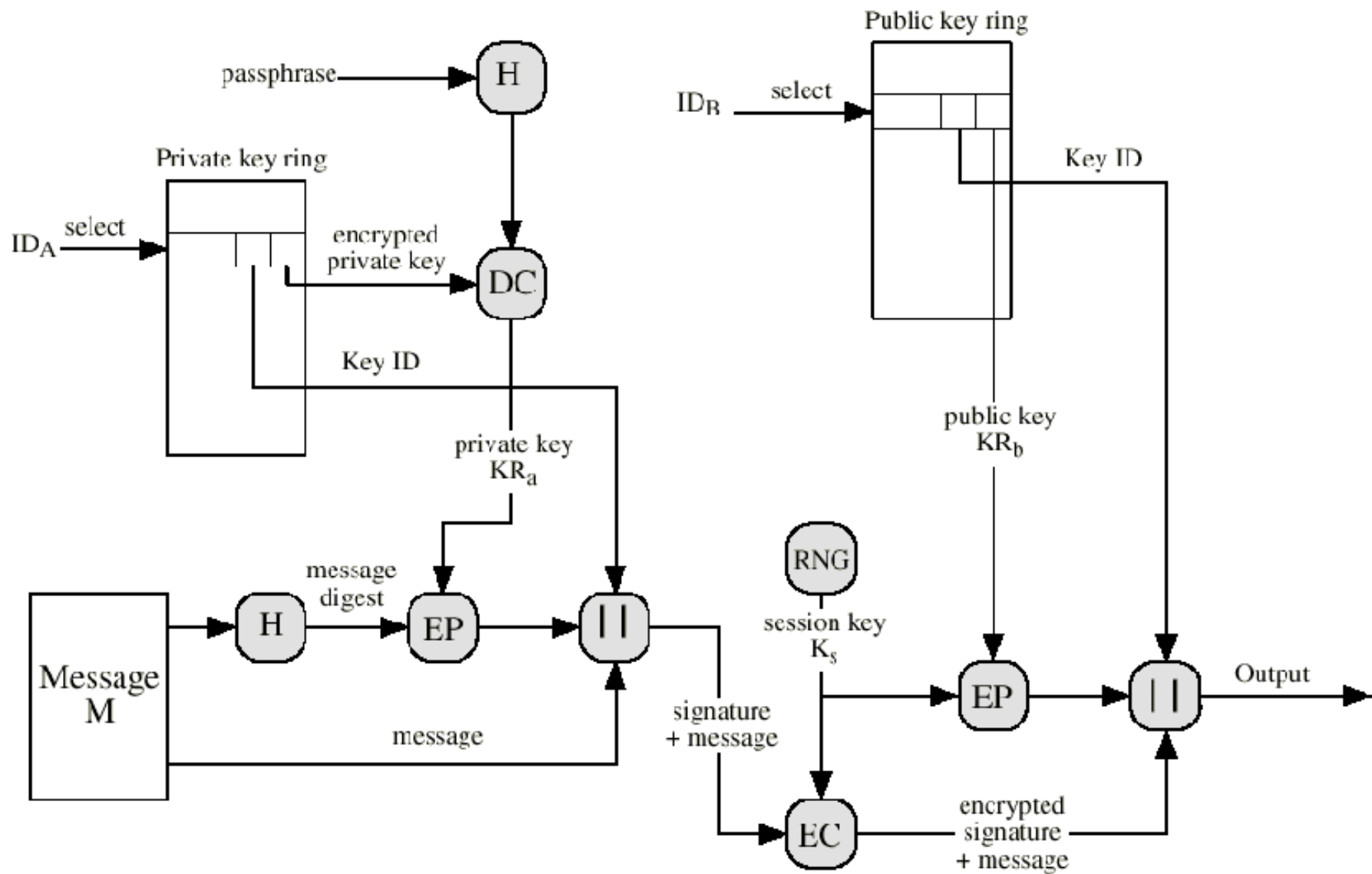


Figure 5.5 PGP Message Generation (from User A to User B; no compression or radix 64 conversion)

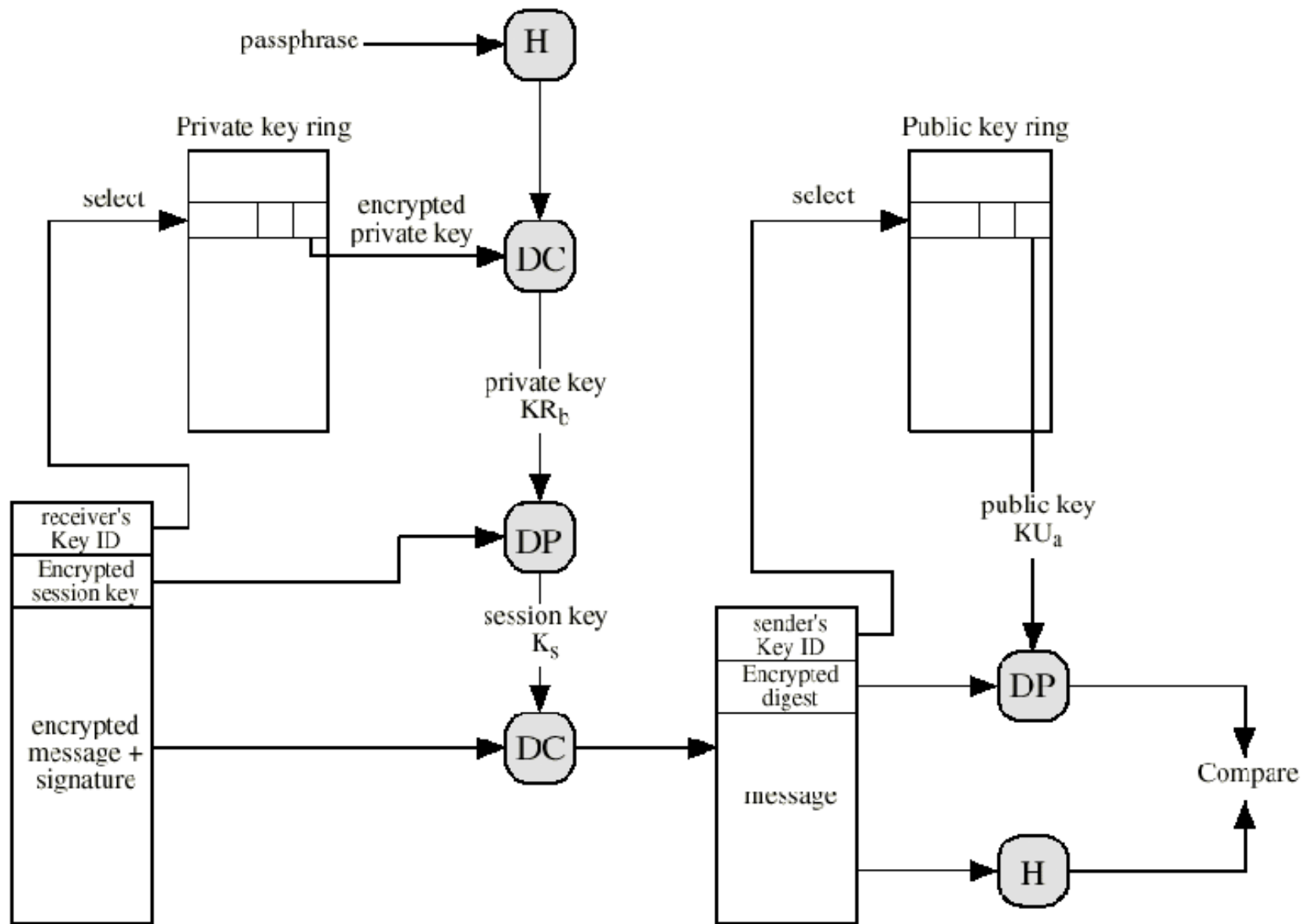
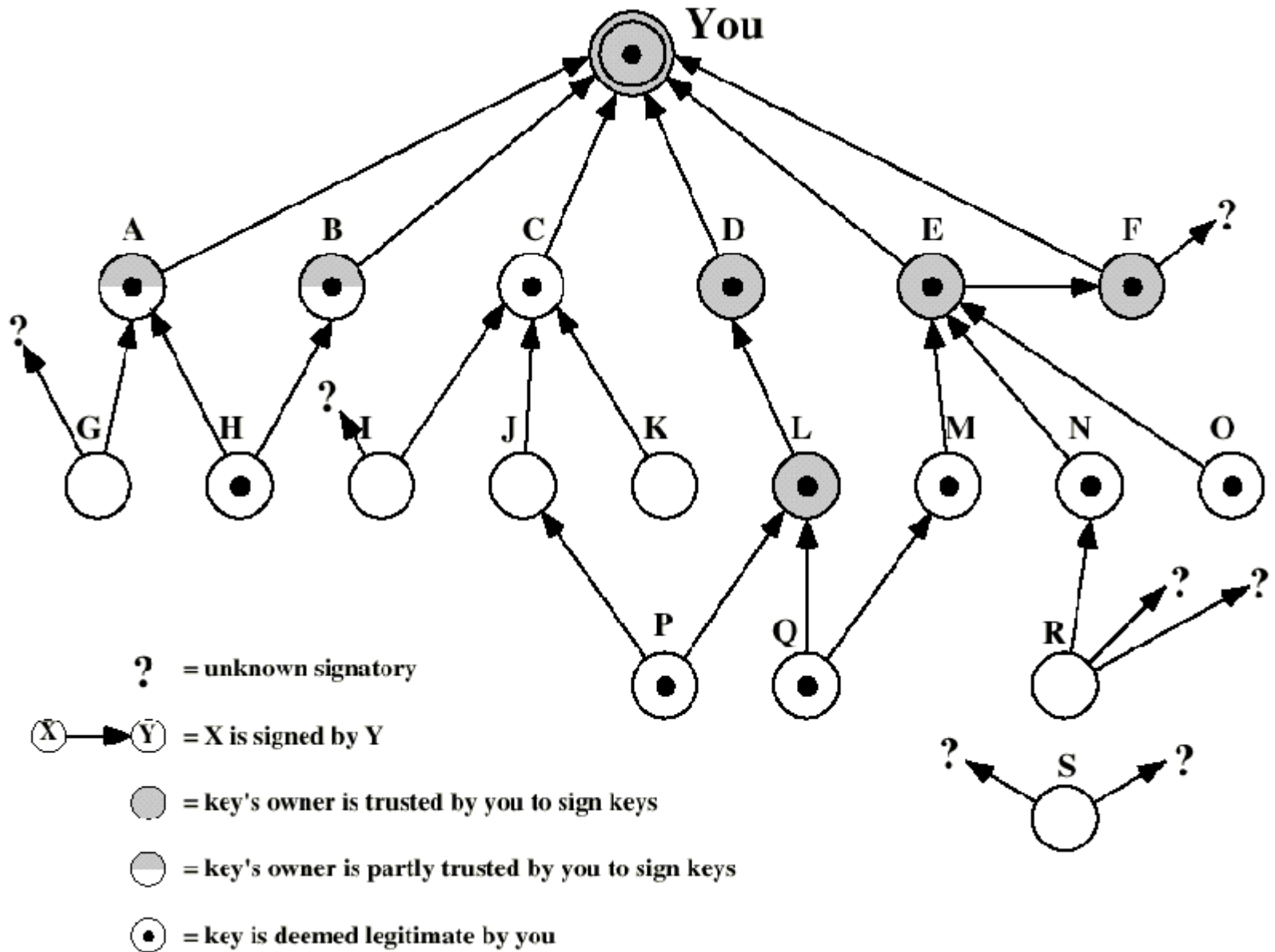


Figure 5.6 PGP Message Reception (from User A to User B; no compression or radix 64 conversion)

# Uso de “Confianza” (*Trust*)

- En lugar de usar certificados y CA, cada usuario actúa como autoridad certificadora.
- Campo de legitimidad de la clave
- Campo de confianza de la firma
- Campo de confianza de Propietario



# Revocando Claves Públicas

- El propietario genera un certificado de revocación de clave
- Certificado de firma normal, con un indicador de revocación
- La clave privada correspondiente es usada para firmar el certificado

# **S/MIME**

## ***(Secure/Multipurpose Internet Mail Extension)***

- Mejoras de seguridad para MIME
  - MIME provee soporte para correos con diferentes tipos de contenido y multi-parte
  - MIME codifica datos binarios en ASCII
- S/MIME disponible en clientes como Mozilla, Mac Mail, etc.
- Debería ser el estándar en el mundo profesional

# Simple Mail Transfer Protocol (SMTP, RFC 822)

- **Limitaciones de SMTP - No puede transmitir o tiene problemas con:**
  - Archivos ejecut. o binarios (p.e. imagen jpeg)
  - Idiomas diferentes al inglés (caract. no-ASCII)
  - Mensajes mayores a cierto tope
  - Problemas de traducción ASCII to EBCDIC
  - Líneas largas (72 to 254 characters)

# Rol del *User Agent*

- S/MIME usa Certificados X.509 version 3, firmados por la Autoridad Certificadora
- Funciones:
  - **Gener. claves** - Diffie-Hellman, DSS, RSA.
  - **Registro** - Claves púb. registradas con X.509 CA.
  - **Almacenamiento del Certificado** - Local (como en un navegador) para diferentes servicios
  - **Firma y empaquetado de datos** - Diferentes órdenes para cifrar y firmar

# **S/MIME: Algoritmos criptográficos**

- Firma digital: DSS & RSA
- Resumen: SHA-1 & MD5
- Cifrado de clave de sesión:  
ElGamal & RSA
- Cifrado de mensaje: AES, Triple-DES, RC2/40 y otros
- MAC: HMAC on SHA-1

# Clases de Certificados

- **Ejemplo:** *Verisign* ([www.verisign.com](http://www.verisign.com))
  - **Class-1:** email del comprador confirmado por email (*vital info*)
  - **Class-2:** Se verifica además dirección postal, los datos chequeados contra directorios
  - **Class-3:** Comprador debe presentarse, o enviar documento notariado

# GNU Privacy Guard (gpg)

- Implementación GNU de OpenPGP
- Integrado en Evolution, Kmail, etc
- EnigMail – extensión para Thunderbird
- ¡Funciona hasta en Windows!
- Soporta algoritmos no patentados. Por defecto DSA (firma) y ElGamal (asimétrico). Además CAST5, Triple DES, AES, Blowfish

# GPG

- Generar clave
  - `gpg --gen-key`
- Exportar (para pasarla a alguien)
  - `gpg --export -armor`
- Importar (para incluir en llavero)
  - `gpg --import file`
- Servidores de claves públicas:
  - `pgp.mit.edu`, `keyserver.net`