به نام خدا

دانشکده مهندسی برق،
دانشگاه صنعتی شریف

مبانی رمزنگاری و امنیت شبکه

امنیت رایانامه

Email Security

مهتاب میرمحسنی

نیم‌سال دوم (بهار) ۹۸-۹۹

امنیت رایانامه

- پراستفاده‌ترین برنامه کاربردی تحت وب
- پروتکل‌های معمول که هیچ امنیتی را فراهم نمی‌کنند:
  - SMTP (Simple Mail Transfer Protocol)
  - MIME (Multipurpose Internet Mail Extensions)

محرمانگی و احراز اصالت (پیام و فرستنده)

- Pretty Good Privacy (PGP)
  - محرمانگی: رمز متقارن قالبی
  - احراز اصالت: امضای دیجیتال
  - فشرده‌سازی: ZIP
  - سازگاری: radix-64
- Secure/Multipurpose Internet Mail Extension (S/MIME)
  - استاندارد امنیتی برای امنیت رایانامه (با استفاده از روشی مشابه PGP)

Pretty Good Privacy (PGP)

- Phil Zimmermann
- انتخاب بهترین الگوریتم‌های رمزنگاری و یکپارچه کردن آن‌ها در یک برنامه کاربردی همه منظوره (ارسال رایانامه یا ذخیره داده - مستقل از نوع سیستم و پردازنده)
- انتشار بسته نرم افزاری (شامل کد) به صورت مجانی در اینترنت (عدم انحصار)
  - نسخه تجاری ارزان نیز تولید شده است
- به طور گسترده مورد استفاده قرار گرفته است
  - سیستم عامل‌های متفاوت (Windows, UNIX, Macintosh)
  - بهترین الگوریتم‌های رمزنگاری (RSA، DSS و DH برای رمز کلید همگانی، CAST-128، IDEA و 3DES برای رمز متقارن و SHA-1 برای چکیده‌ساز)
  - استاندارد اینترنتی (RFC 3156; MIME Security with OpenPGP)

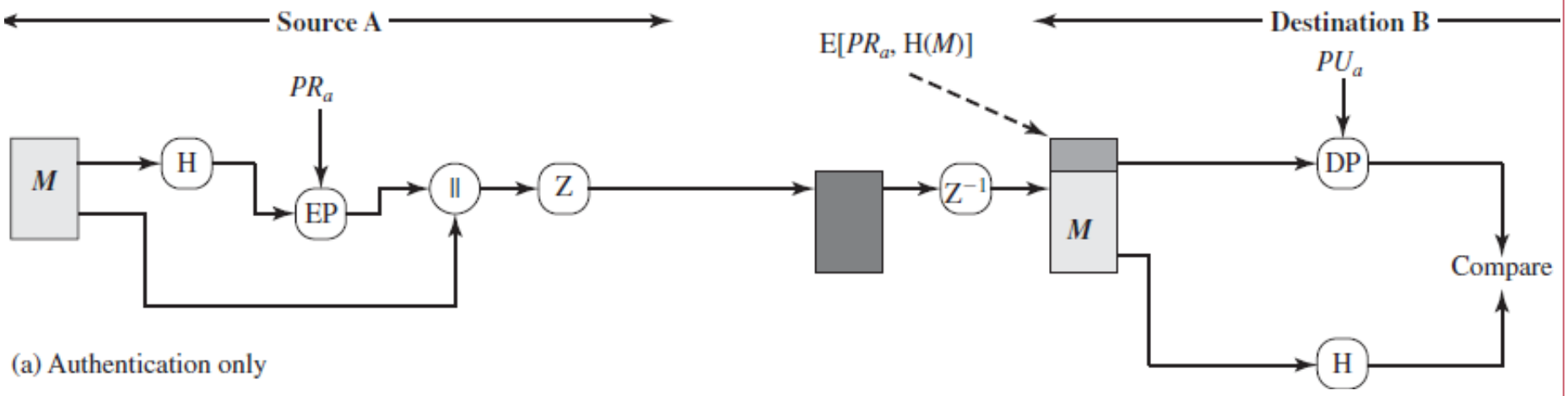
خدمات PGP

- محرمانگی: رمز متقارن قالبی
- احراز اصالت: امضای دیجیتال
- فشرده‌سازی: ZIP
- سازگاری: radix-64

Function	Algorithms Used	Description
Digital signature	DSS/SHA or RSA/SHA	A hash code of a message is created using SHA-1. This message digest is encrypted using DSS or RSA with the sender's private key and included with the message.
Message encryption	CAST or IDEA or Three-key Triple DES with Diffie-Hellman or RSA	A message is encrypted using CAST-128 or IDEA or 3DES with a one-time session key generated by the sender. The session key is encrypted using Diffie-Hellman or RSA with the recipient's public key and included with the message.
Compression	ZIP	A message may be compressed for storage or transmission using ZIP.
E-mail compatibility	Radix-64 conversion	To provide transparency for e-mail applications, an encrypted message may be converted to an ASCII string using radix-64 conversion.

احراز اصالت در PGP
امضای دیجیتال

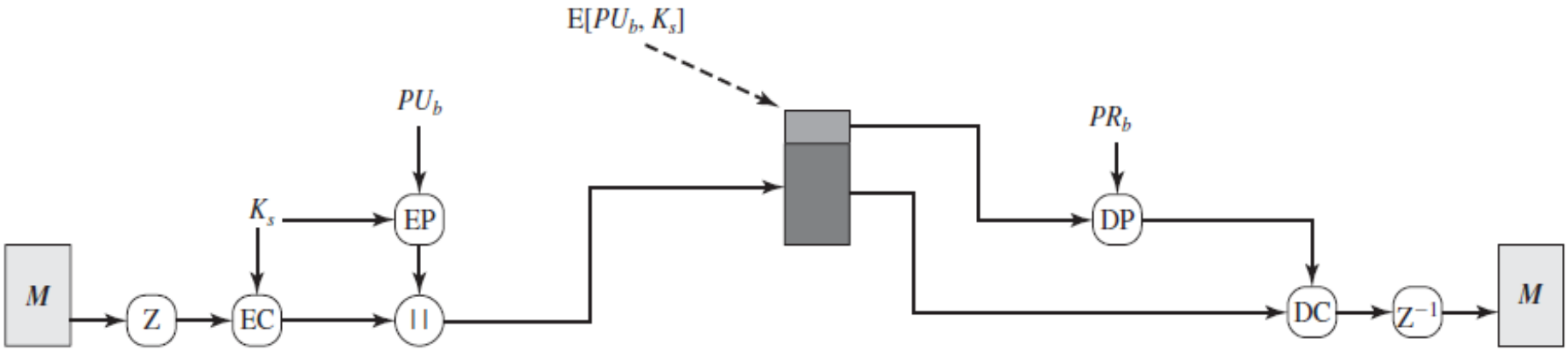
- تولید چکیده ۱۶۰ بیتی از پیام با استفاده از SHA-1
- رمزگذاری چکیده با RSA یا DSS



(a) Authentication only

محرمانگی در PGP

- رمزگذاری پیام با رمز متقارن CAST-128، IDEA و یا 3DES (با کلید نشست)
  - در سبک cipher feedback mode
- کلید مخفی (رمز متقارن) برای هر پیام به صورت یک عدد تصادفی (۱۲۸ یا ۱۶۸ بیتی) تولید می‌شود و کلید نشست نام دارد (در اصل کلید یکبار مصرف)
- کلید نشست با رمز کلید همگانی (RSA یا ElGamal) رمز شده و همراه پیام ارسال می‌شود
- ترکیب رمز متقارن و نامتقارن جهت کاهش زمان رمزنگاری
  - نیاز به توزیع کلید نشست (مشابه پروتکل‌های مدیریت کلید) نداریم



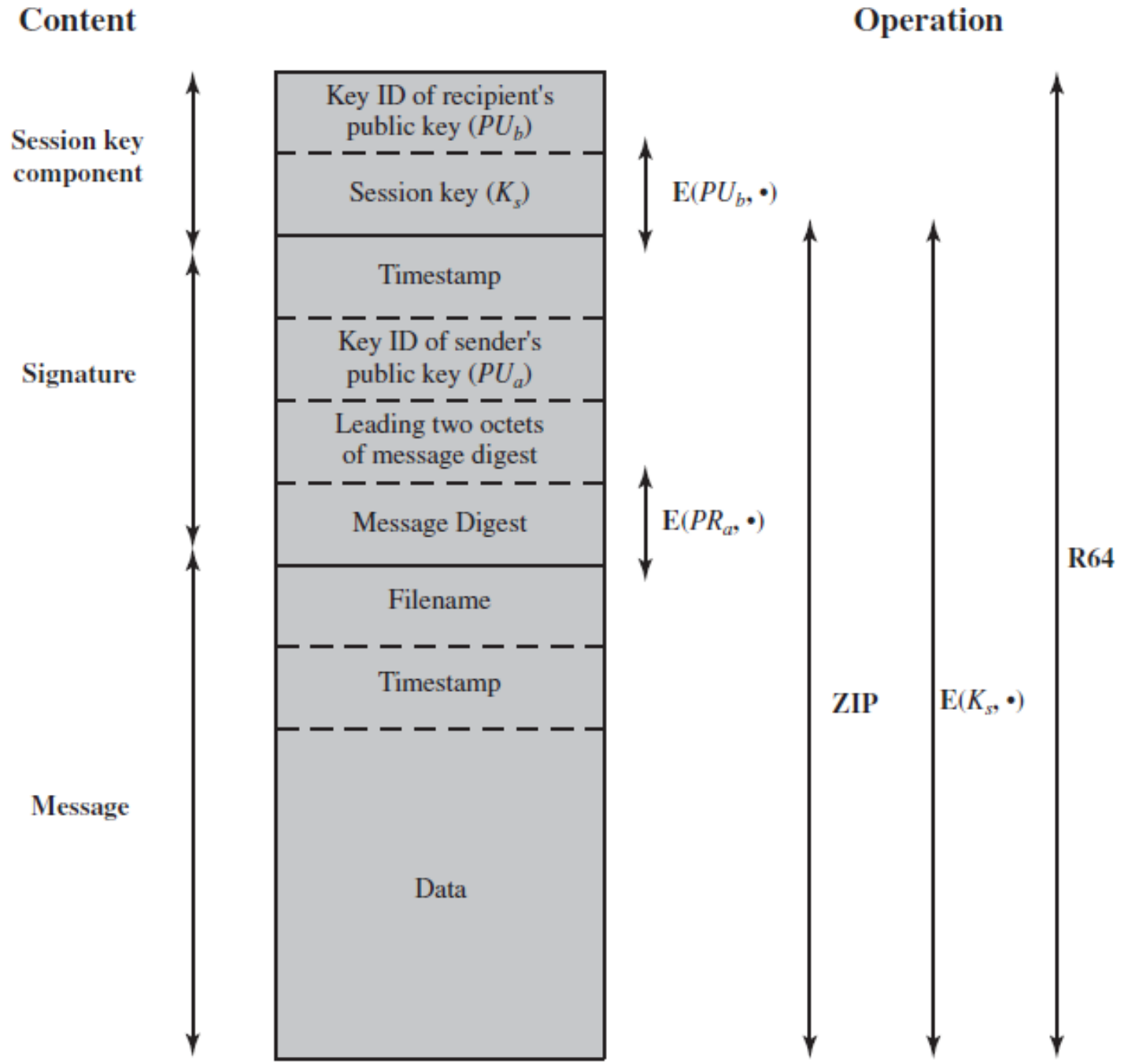
(b) Confidentiality only

کلیدهای PGP

1. کلید مخفی نشست برای رمز متقارن (یکبار مصرف)
   - تولید تصادفی با همان الگوریتم رمز متقارن در سبک CFB (کاربرد رمز متقارن در تولید اعداد تصادفی)
2. کلیدهای همگانی/ خصوصی
   - نیاز به داشتن چند جفت کلید نامتقارن (همگانی-خصوصی) برای هر کاربر
     - استفاده از شناسه کلید (Key Identifier): ارسال شناسه همراه با پیام یا امضا

$$\mathrm{ID} = PU_a \bmod 2^{64}$$

   - هر هستار PGP، باید پرونده‌ای از کلیدهای نامتقارن خود و هستارهای دیگر را ذخیره کند
3. کلید متقارن حاصل از عبارت گذر (passphrase)



ساختار پیام در PGP

دسته کلیدها (Key Rings)

- کلید خصوصی (در دسته کلید خصوصی): به صورت رمز شده با **کلید متقارن حاصل از عبارت گذر** (با اعمال تابع چکیده‌ساز SHA-1 به عبارت گذر کاربر)
- زمان و تاریخ تولید کلیدها (Timestamp)
- شناسه کلید (Key ID)
- شناسه کاربر مالک کلید (User ID)

- دسته کلید خصوصی

Private-Key Ring

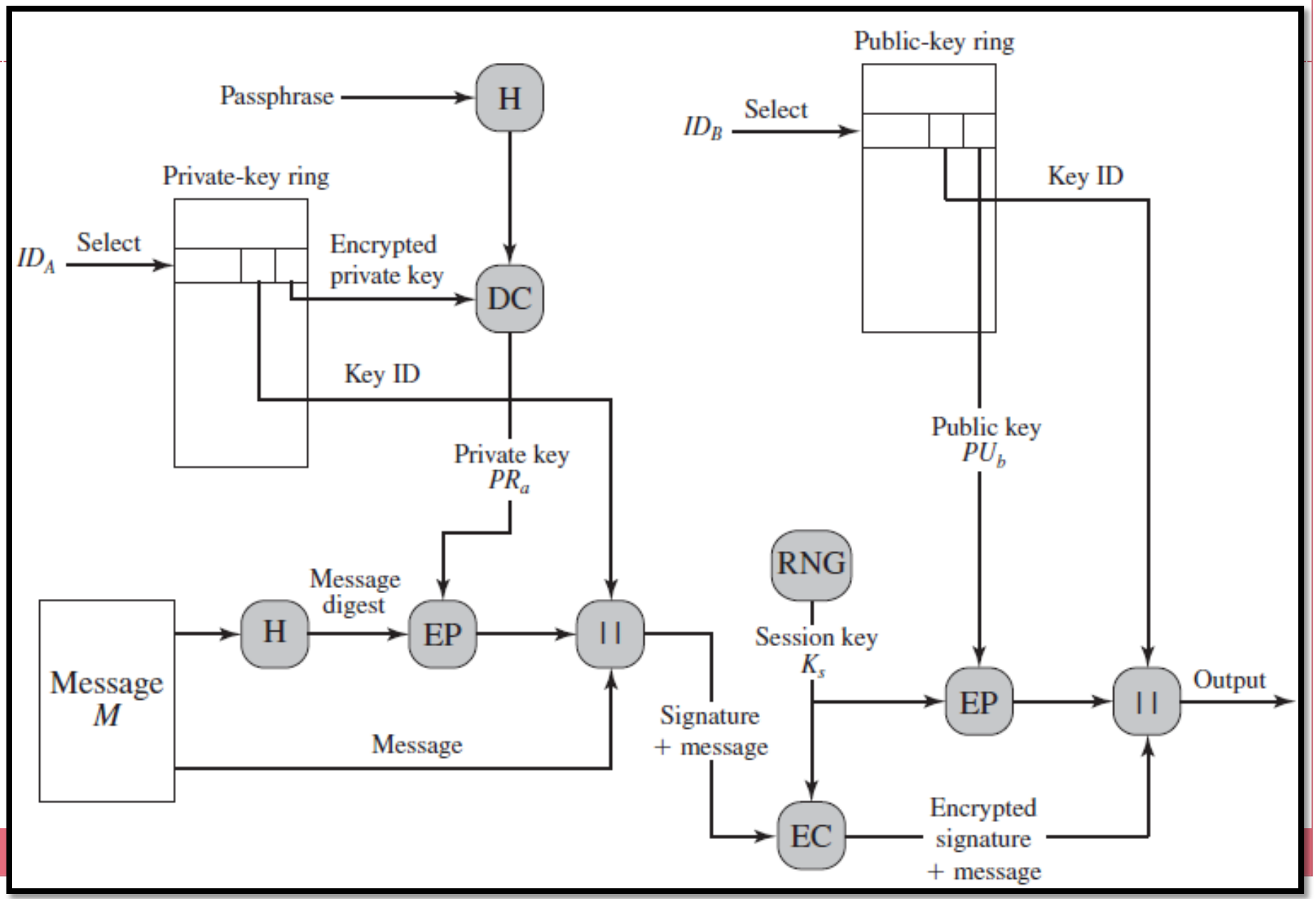
Timestamp	Key ID*	Public Key	Encrypted Private Key	User ID*
• • •	• • •	• • •	• • •	• • •
T_i	$PU_i \bmod 2^{64}$	PU_i	$E(H(P_i), PR_i)$	User i
• • •	• • •	• • •	• • •	• • •

دسته کلید همگانی

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 $_i$		
• • •	• • •	• • •	• • •	• • •	• • •	• • •	• • •

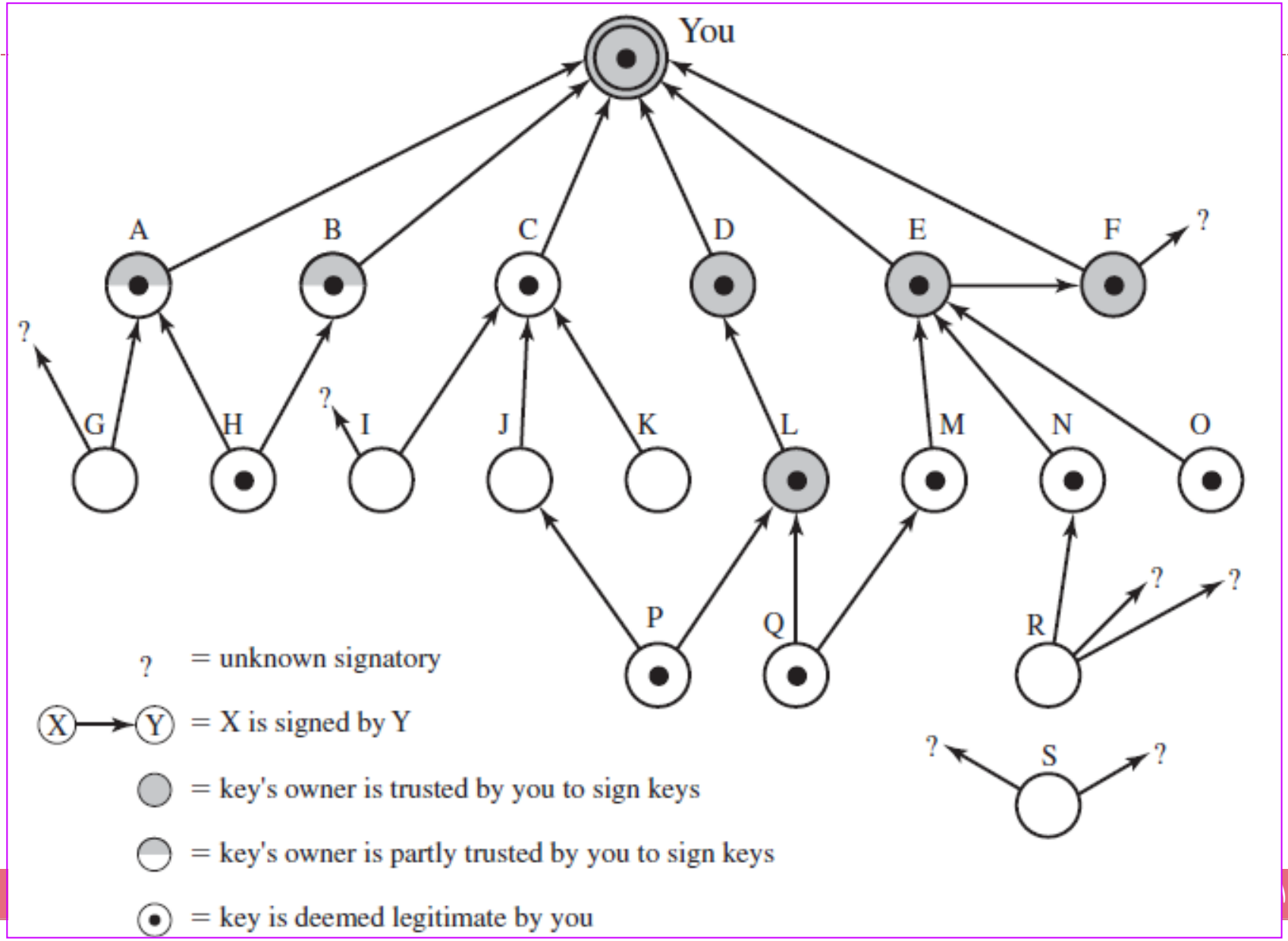
تولید پیام در PGP (بدون فشرده‌سازی و سازگاری)



مدیریت کلیدهای همگانی در PGP

- نیاز به اطمینان به مالک کلیدهای همگانی
- ارسال کلید همگانی همراه با احراز اصالت فرستنده
  - ارسال فیزیکی
  - دریافت کلید توسط شخصی که مورد اعتماد دو طرف است (امضای گواهی)
  - گواهی امضا شده توسط مرجع مجازشناس (مرجع صدور گواهی): CA
- PGP، روشی را برای اخذ گواهی تحمیل نمی‌کند و بر اساس توزیع اعتماد عمل می‌کند
  - به جای تکیه بر CAها، هر کاربری CA است و می‌تواند گواهی کاربرهایی که مستقیماً می‌شناسد، را امضا کند
  - همگی کاربرها تشکیل مدلی از اعتماد توزیع شده (Web of Trust) را می‌دهند
  - کلیدی قانونی (legal) است که توسط شخص مورد اعتماد امضا شود
  - میزان اعتماد ممکن است متفاوت باشد

مثالی از مدل اعتماد (Trust) در PGP



S/MIME
(Secure/Multipurpose Internet Mail Extension)

- پروتکل مبادله ایمیل MIME
  - MIME جهت رفع مشکلات نسخه اولیه پروتکل مبادله ایمیل (RFC822) ارائه شده
  - RFC822 تنها از داده‌های متنی پشتیبانی می‌کرد (عدم ارسال داده‌های باینری)
  - MIME از انواع متفاوت محتوا و پیام‌های چند بخشی (همراه با کدگذاری‌های متفاوت) پشتیبانی می‌کند
- S/MIME نسخه امن شده پروتکل مبادله رایانامه MIME است
- بسیاری از سرورهای ایمیل از S/MIME (نسخه امن شده) پشتیبانی می‌کنند
  - MS Outlook، Mozilla، Mac Mail و ...

قابلیت‌های S/MIME

- مشابه PGP: محرمانگی + امضا
  - enveloped data
    - محتوای رمز شده + کلیدهای همراه
  - signed data
    - پیام + امضا (چکیده رمزشده) ← هر دو کدگذاری می‌شوند (مثلا با base64)
    - تنها کاربر با قابلیت S/MIME قادر به مشاهده پیام است
  - clear-signed data
    - پیام + امضا (چکیده رمزشده) کدگذاری شده
    - تنها بدون قابلیت S/MIME قادر به مشاهده پیام است ولی نمی‌تواند امضا را تایید کند
  - signed and enveloped data
    - ترکیبی از داده رمز شده (محرمانگی) و امضا

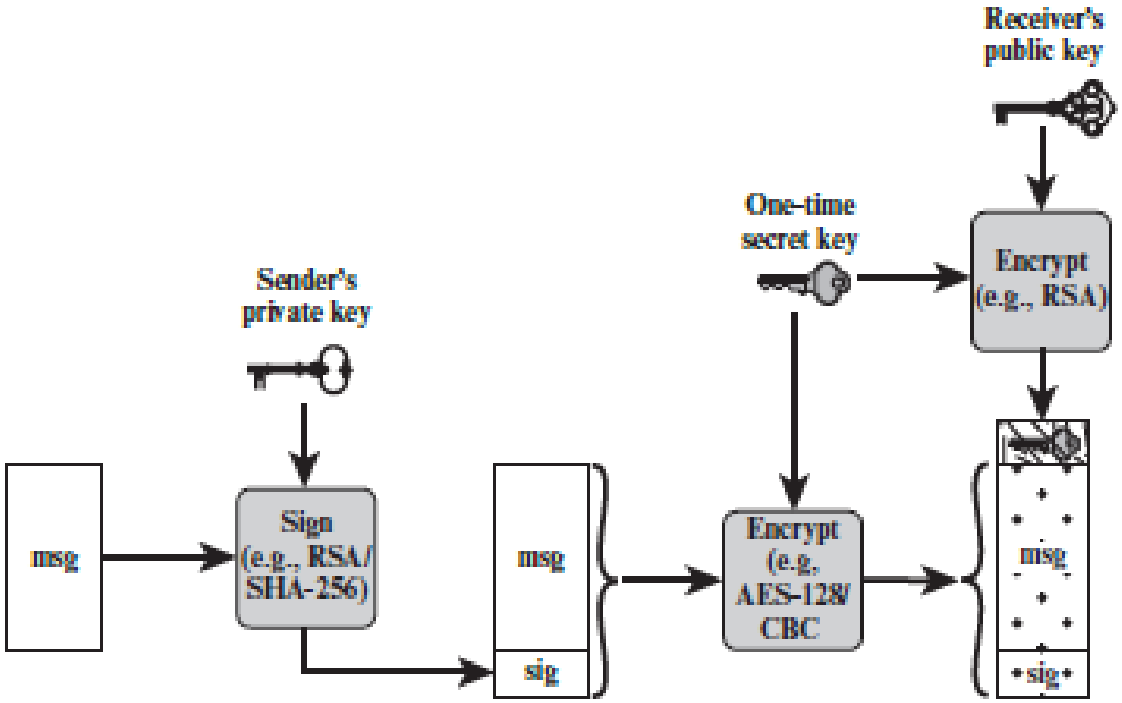
الگوریتم‌های رمزنگاری در S/MIME

- امضای دیجیتال: DSS و RSA
- رمزنگاری کلید نشست: ElGamal (گاهی با نام دیفی-هلمن) و RSA
- تابع چکیده ساز: SHA-1 و MD5 (برای حفظ سازگاری با نسخه قبلی)
- رمزنگاری متقارن پیام: 3-DES، AES و RC2/40 (برای حفظ سازگاری)
- کد احراز اصالت (MAC): HMAC با بکارگیری SHA-1

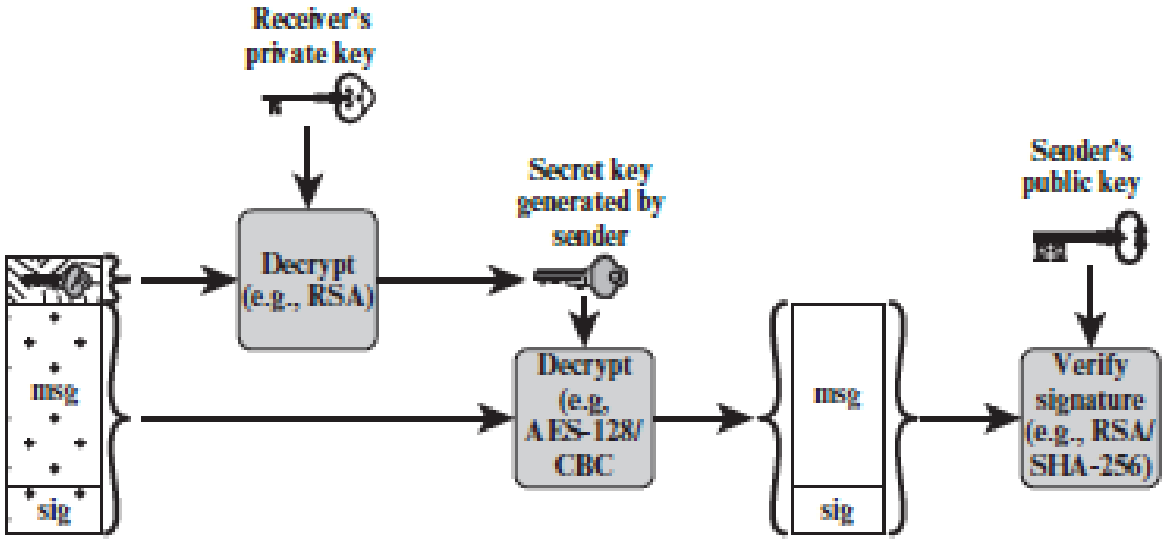
- MUST: پیاده‌سازی الزامی است
- SHOULD: پیاده‌سازی توصیه شده است
- قوانینی جهت انتخاب الگوریتم‌ها وجود دارد

الگوریتم‌های رمزنگاری در S/MIME

Function	Requirement
Create a message digest to be used in forming a digital signature.	MUST support SHA-1. Receiver SHOULD support MD5 for backward compatibility.
Encrypt message digest to form a digital signature.	Sending and receiving agents MUST support DSS. Sending agents SHOULD support RSA encryption. Receiving agents SHOULD support verification of RSA signatures with key sizes 512 bits to 1024 bits.
Encrypt session key for transmission with a message.	Sending and receiving agents SHOULD support Diffie-Hellman. Sending and receiving agents MUST support RSA encryption with key sizes 512 bits to 1024 bits.
Encrypt message for transmission with a one-time session key.	Sending and receiving agents MUST support encryption with tripleDES. Sending agents SHOULD support encryption with AES. Sending agents SHOULD support encryption with RC2/40.
Create a message authentication code.	Receiving agents MUST support HMAC with SHA-1. Sending agents SHOULD support HMAC with SHA-1.



(a) Sender signs, then encrypts message



(b) Receiver decrypts message, then verifies sender's signature

گواهی‌های کلید همگانی در S/MIME

- از گواهی X.509 v3 استفاده می‌کند
- ترکیبی از PKIX (برای روابط CAها و ...) و مفهوم web of trust در PGP

- گواهی‌ها توسط CAها امضا می‌شوند
- ولی مدیریت گواهی‌ها در هر کاربر صورت می‌گیرد
  - تولید کلید
  - ثبت گواهی
  - ذخیره و بازیابی گواهی