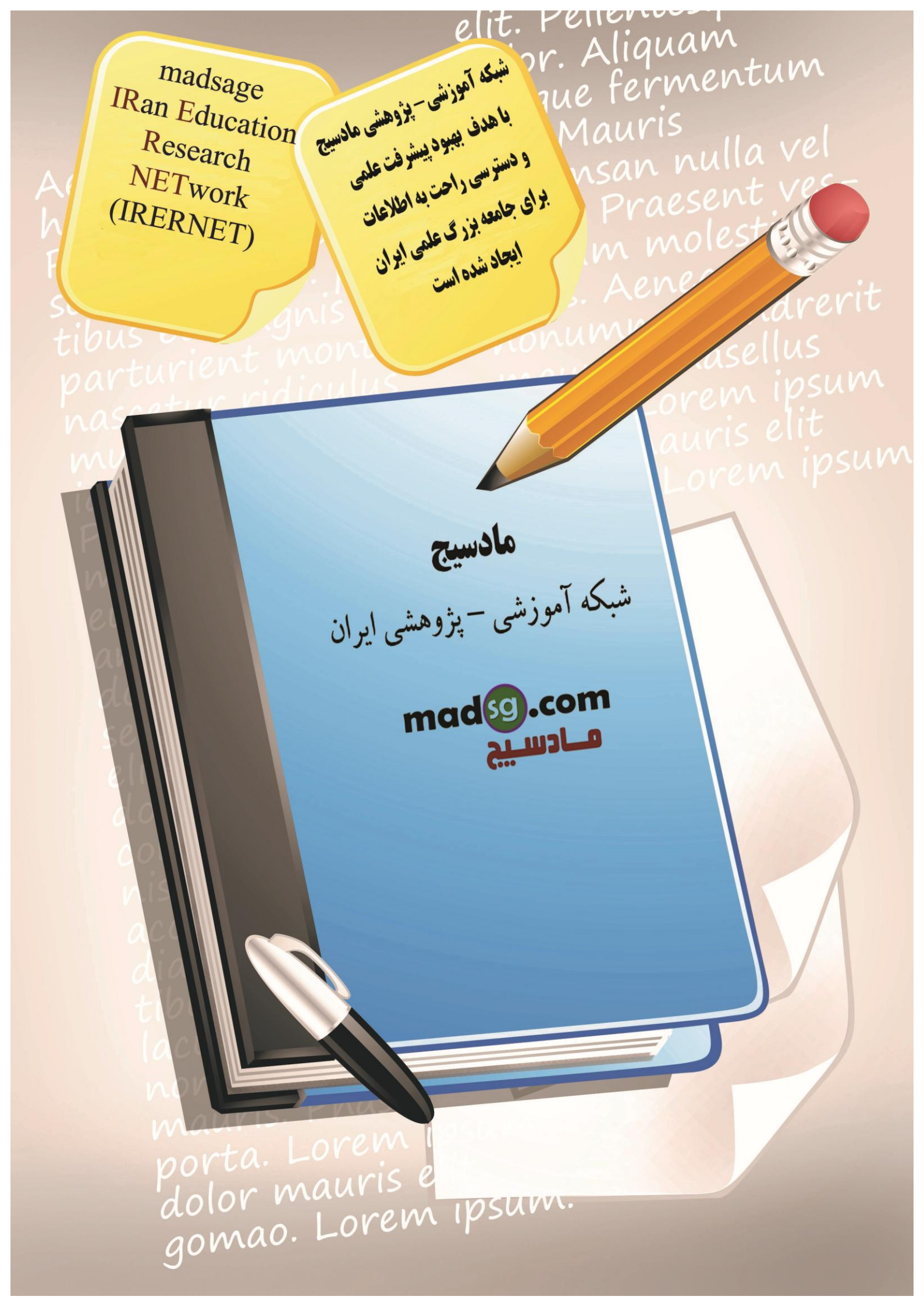

madsage
IRan Education
Research
NETwork
(IRERNET)
شبکه آموزشی-پژوهشی مادسیج
با هدف بهبود پیشرفت علمی
و دسترسی راحت به اطلاعات
برای جامعه بزرگ علمی ایران
ایجاد شده است
مادسیج
شبکه آموزشی - پژوهشی ایران
madsg.com
مادسیج

یا ذاالامن والامان

امنیت داده و شبکه

امنیت پست الکترونیکی

مرتضی امینی - نیمسال اول ۹۱-۹۰

مرکز امنیت داده و شبکه شریف
http://dnsl.ce.sharif.edu

فهرست مطالب

- امنیت پست الکترونیکی
- پروتکل PGP
  - ویژگی‌های PGP
  - سرویس‌های PGP
  - انواع کلیدهای مورد استفاده
  - مدیریت کلید
- پروتکل S/MIME

نیاز به امنیت در ایمیل

- استفاده گسترده از سرویس پست الکترونیکی برای تبادل پیام‌ها
- نیاز به استفاده از این سرویس برای کاربردهای دیگر
  - به شرط تضمین محرمانگی و احراز اصالت
- دو روش برای احراز اصالت و حفظ محرمانگی در ایمیل
  - PGP (Pretty Good Privacy)
  - S/MIME (Secure/Multipurpose Internet Mail Extensions)

نیاز به امنیت در پست الکترونیکی

- محرمانگی
  - محافظت در مقابل افشای اطلاعات
- احراز اصالت
  - احراز اصالت فرستنده پیام
- صحت پیام
  - محافظت در مقابل تغییر پیام
- عدم انکار منبع (فرستنده)
  - جلوگیری از امکان انکار ارسال پیام توسط فرستنده آن

قراردادهای پست الکترونیکی

SMTP (Simple Mail Transfer Protocol)

- قرارداد SMTP اصلی‌ترین و عمومی‌ترین قرارداد پست الکترونیکی است.
- یک پیام را بصورت کدهای اسکی ارسال می‌کند.
- SMTP هیچ امنیتی برای داده‌های ارسال شده فراهم نمی‌کند.
- داده‌ها در طول مسیر می‌توانند خوانده شده یا تغییر داده شوند.
- آدرس فرستنده براحتی قابل تغییر است.

MIME (Multipurpose Internet Mail Extensions)

- MIME یک قرارداد پست الکترونیکی است که برای رفع محدودیت‌های SMTP و پیغام‌های متنی پیاده‌سازی شد.
- MIME هیچ‌گونه امنیتی فراهم نمی‌کند.

فهرست مطالب

- امنیت پست الکترونیکی
- **پروتکل PGP**
  - **ویژگی‌های PGP**
  - سرویس‌های PGP
  - انواع کلیدهای مورد استفاده
  - مدیریت کلید
- پروتکل S/MIME

ویژگیهای PGP

- ارائه شده توسط Philip Zimmermann.
- استفاده گسترده از آن بعنوان سرویس پست الکترونیکی امن.
- استفاده از بهترین الگوریتم‌های رمزنگاری موجود و ترکیب آنها در یک برنامه کاربردی چند منظوره.
- قابلیت اجرای مستقل از ماشین و پردازنده (Unix، PC، Macintosh و ...).
- عدم انحصار توسط دولت یا شرکت خاص.
- دسترسی کد و بسته نرم افزاری آن مجانی است.
  - نسخه تجاری آن نیز در حال حاضر تولید شده است.

فهرست مطالب

- امنیت پست الکترونیکی
- **پروتکل PGP**
  - ویژگی‌های PGP
  - **سرویس‌های PGP**
  - انواع کلیدهای مورد استفاده
  - مدیریت کلید
- پروتکل S/MIME

سرویس های پایه در PGP

- کنترل صحت (عدم تغییر)
- محرمانگی
- احراز اصالت
- فشرده‌سازی
- حفظ سازگاری
- قطعه‌بندی

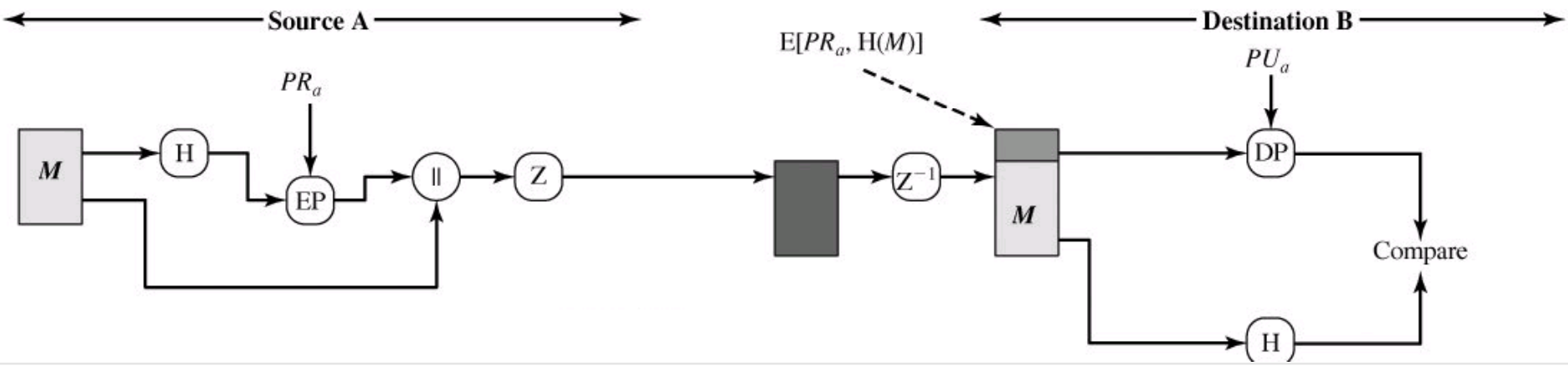
سرویس‌های PGP

کنترل صحت (عدم تغییر)

- تولید چکیده ۱۶۰ بیتی از پیام اولیه با استفاده از SHA-1
- استفاده از RSA و کلید خصوصی فرستنده برای رمز کردن چکیده
- الحاق چکیده رمز شده به انتهای پیام
- استفاده از RSA با کلید عمومی فرستنده برای بازیابی چکیده در سمت گیرنده
- تولید چکیده پیام جدید توسط گیرنده و مقایسه آن با چکیده بازیابی شده
- (از الگوریتم امضای دیجیتال DSS نیز می‌تواند استفاده کند.)

سرویس‌های PGP

- کنترل صحت (عدم تغییر)



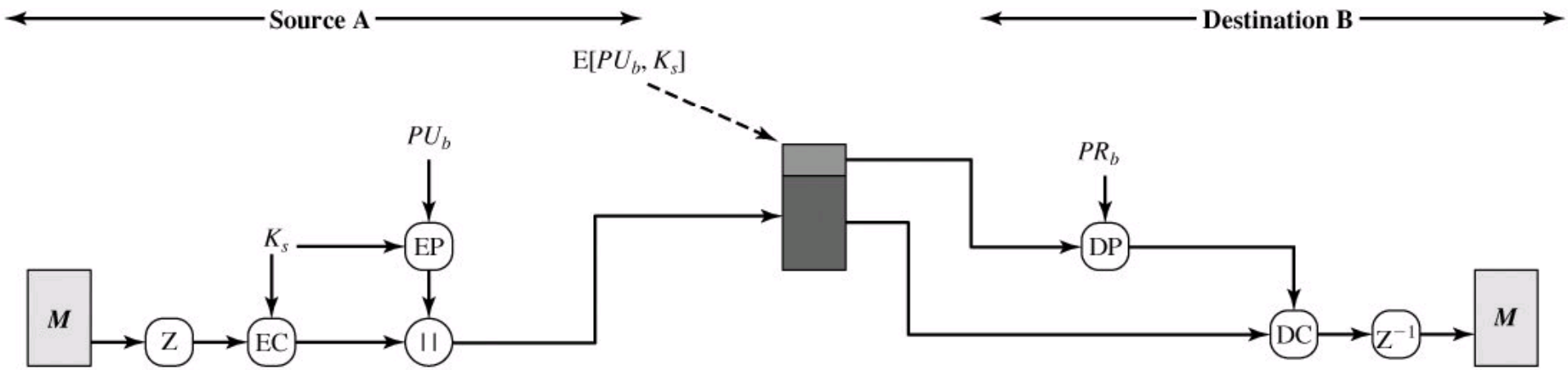
سرویس‌های PGP

محرمانگی

- استفاده از عدد تصادفی ۱۲۸ (۱۶۰) بیتی به عنوان کلید جلسه پیام جاری
- رمزکردن پیام با استفاده از CAST-128 (یا IDEA یا 3DES) و کلید جلسه تولید شده
- رمزکردن کلید جلسه با استفاده از الگوریتم RSA (یا El-Gamal) و کلید عمومی گیرنده
- الحاق کلید رمزشده به پیام و ارسال آن
- استفاده از RSA (یا El-Gamal) با کلید خصوصی گیرنده برای رمزگشایی و بازیابی کلید جلسه
- رمزگشایی پیام دریافت شده با استفاده از کلید جلسه

سرویس‌های PGP

محرمانگی

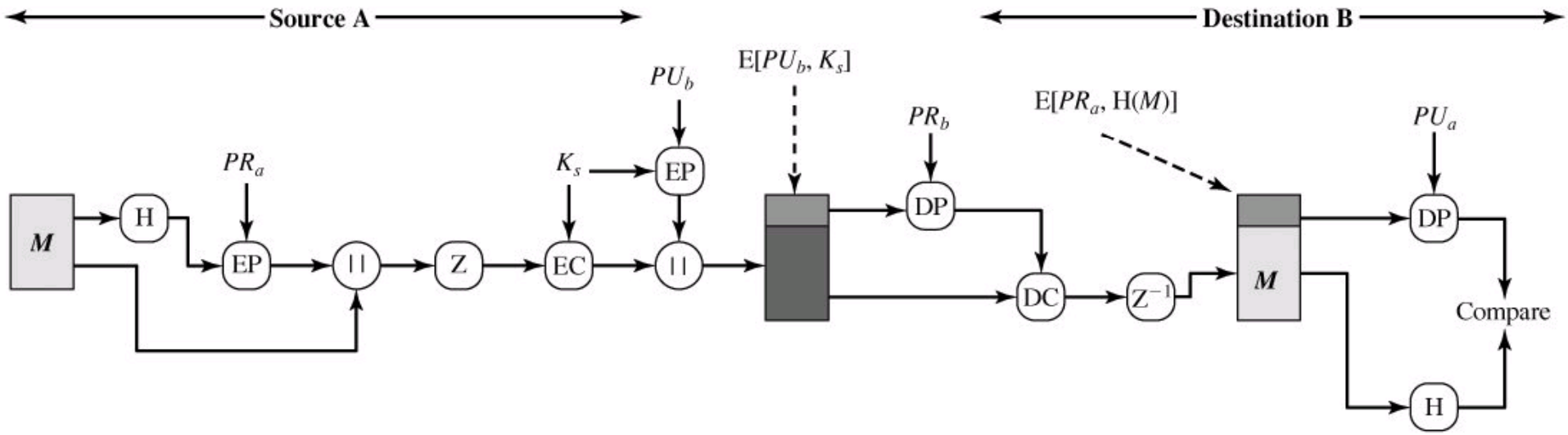


سرویس‌های PGP

- **محرمانگی + احراز اصالت**
  - تولید امضاء و الحاق آن به متن
  - رمز کردن مجموعه امضاء و متن با استفاده از CAST-128 (یا IDEA یا 3DES)
  - الحاق کلید جلسه رمزشده با الگوریتم RSA (یا El-Gamal) به مجموعه فوق
- چرا اول امضاء رقمی انجام می‌شود و سپس رمزگذاری؟
  - با این روش شخص ثالث برای وارسی امضاء (به طور مثال برای حکمیت یک موضوع) نیازی به دانستن کلید جلسه ندارد.

سرویس‌های PGP

- محرمانگی + احراز اصالت



سرویس‌های PGP

فشرده‌سازی

- به صورت پیش‌فرض، فشرده‌سازی، پس از امضاء و قبل از رمزگذاری انجام می‌شود.
- چرا پس از امضاء؟
  - باید بتوان پیام و امضاء را برای تایید بعدی و بدون نیاز به فشرده‌سازی و یا بازگشایی مجدد ذخیره نمود.
- چرا قبل از رمزگذاری؟
  - کاهش حجم و افزونگی متنی که باید رمز شود و کاهش اطلاعات آماری پیام.

سرویس‌های PGP

حفظ سازگاری

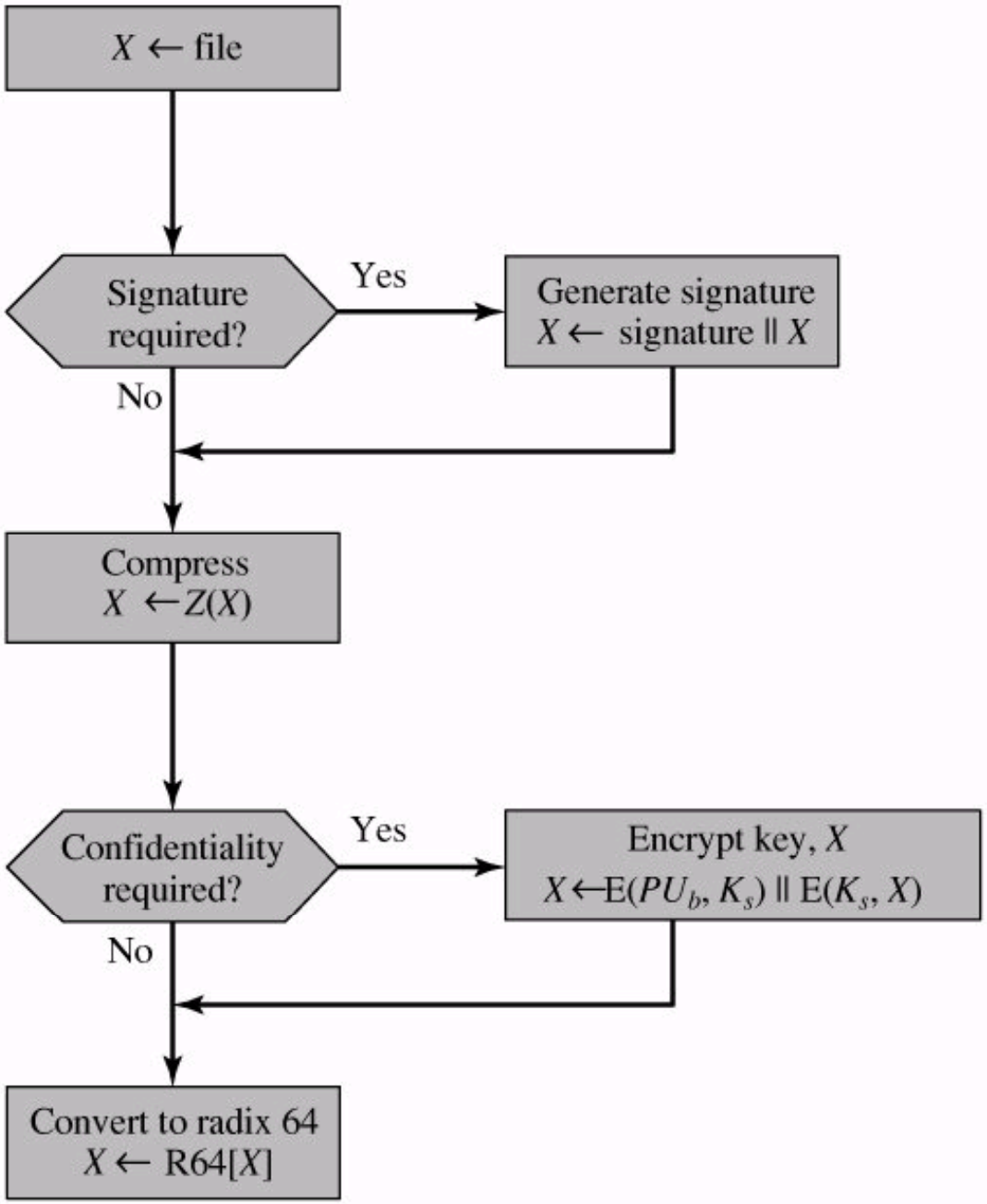
- مشکل:
  - فرستادن داده‌های باینری از طریق سرویس‌های پست الکترونیکی که تنها برای ارسال متن اسکی طراحی شده‌اند.
- راه حل:
  - تبدیل داده های خام باینری به متن اسکی:
    - استفاده از الگوریتم Radix-64
      - تبدیل ۳ بایت به ۴ کاراکتر قابل چاپ اسکی
      - اضافه کردن CRC به انتهای آن
  - افزایش اندازه متن به میزان ۳۳٪ به دلیل استفاده از Radix-64 و کاهش اندازه آن با فشرده‌سازی به میزان ۵۰٪ ⇐ ۰/۶۶۵= ۰/۵ × ۱/۳۳
  - نتیجه: فشرده سازی به اندازه یک سوم

سرویسهای PGP

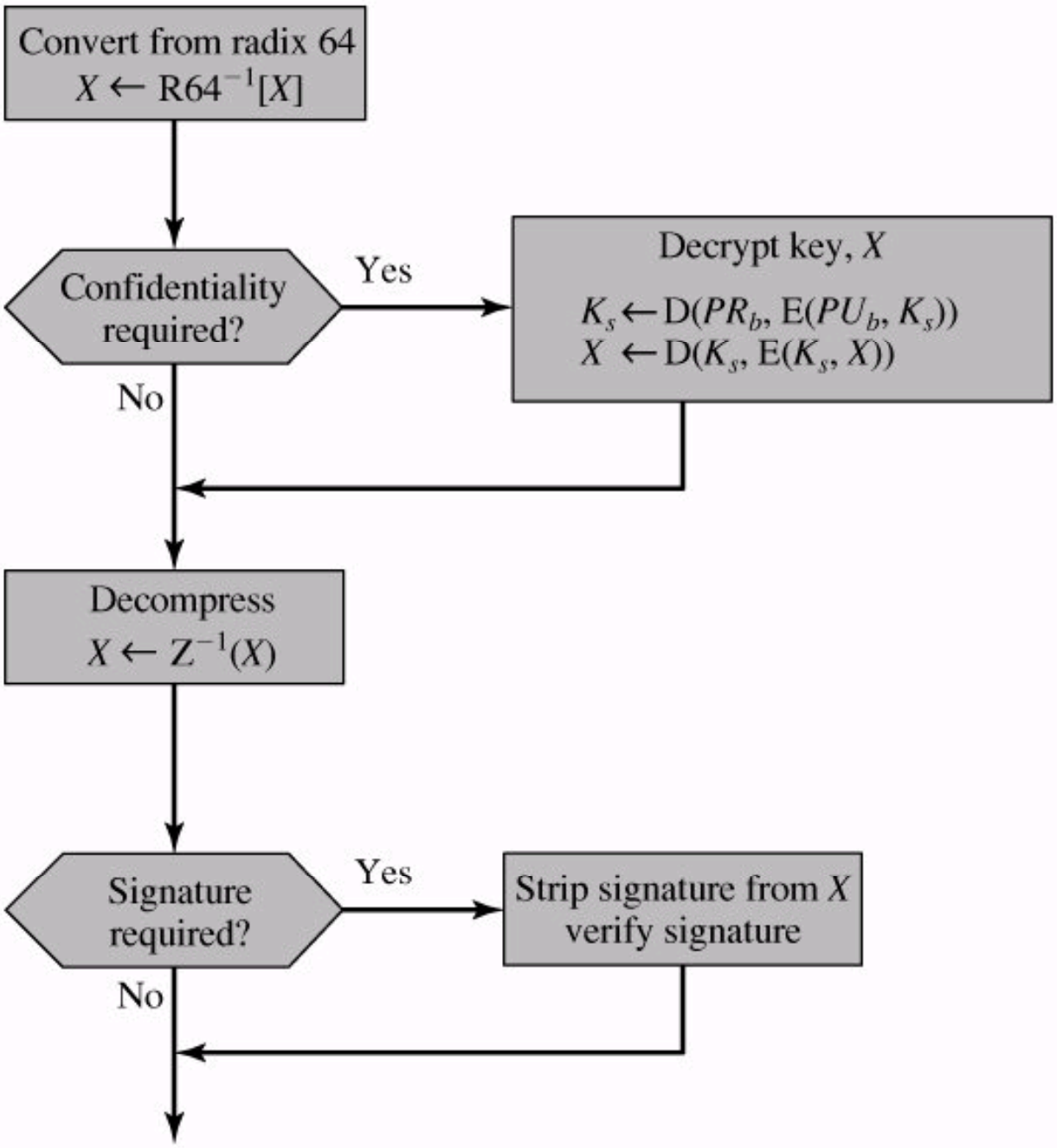
قطعه بندی

- محدودیت (۵۰۰۰۰۰ بایتی) اغلب سرویس‌دهنده‌های ایمیل در اندازه پیام ارسالی.
- انجام قطعه‌بندی توسط PGP به صورت خودکار، پس از انجام کلیه محاسبات و تبدیلات.
- ارسال کلید جلسه و امضاء رقمی فقط در ابتدای قطعه اول.
- بازیابی پیام اصلی از روی قطعه‌ها در سمت گیرنده (قبل از انجام هر پردازشی).

الگوریتم ارسال در PGP



الگوریتم دریافت در PGP



فهرست مطالب

- امنیت پست الکترونیکی
- **پروتکل PGP**
  - ویژگی‌های PGP
  - سرویس‌های PGP
  - **انواع کلیدهای مورد استفاده**
  - مدیریت کلید
- پروتکل S/MIME

کلیدهای مورد استفاده

- PGP از چهار نوع کلید بهره می برد:
  - کلید متقارن یکبار مصرف (کلید جلسه)
  - کلید عمومی
  - کلید خصوصی
  - کلید متقارن حاصل از گذرواژه (برای رمز کردن کلیدهای خصوصی)

کلیدهای مورد استفاده

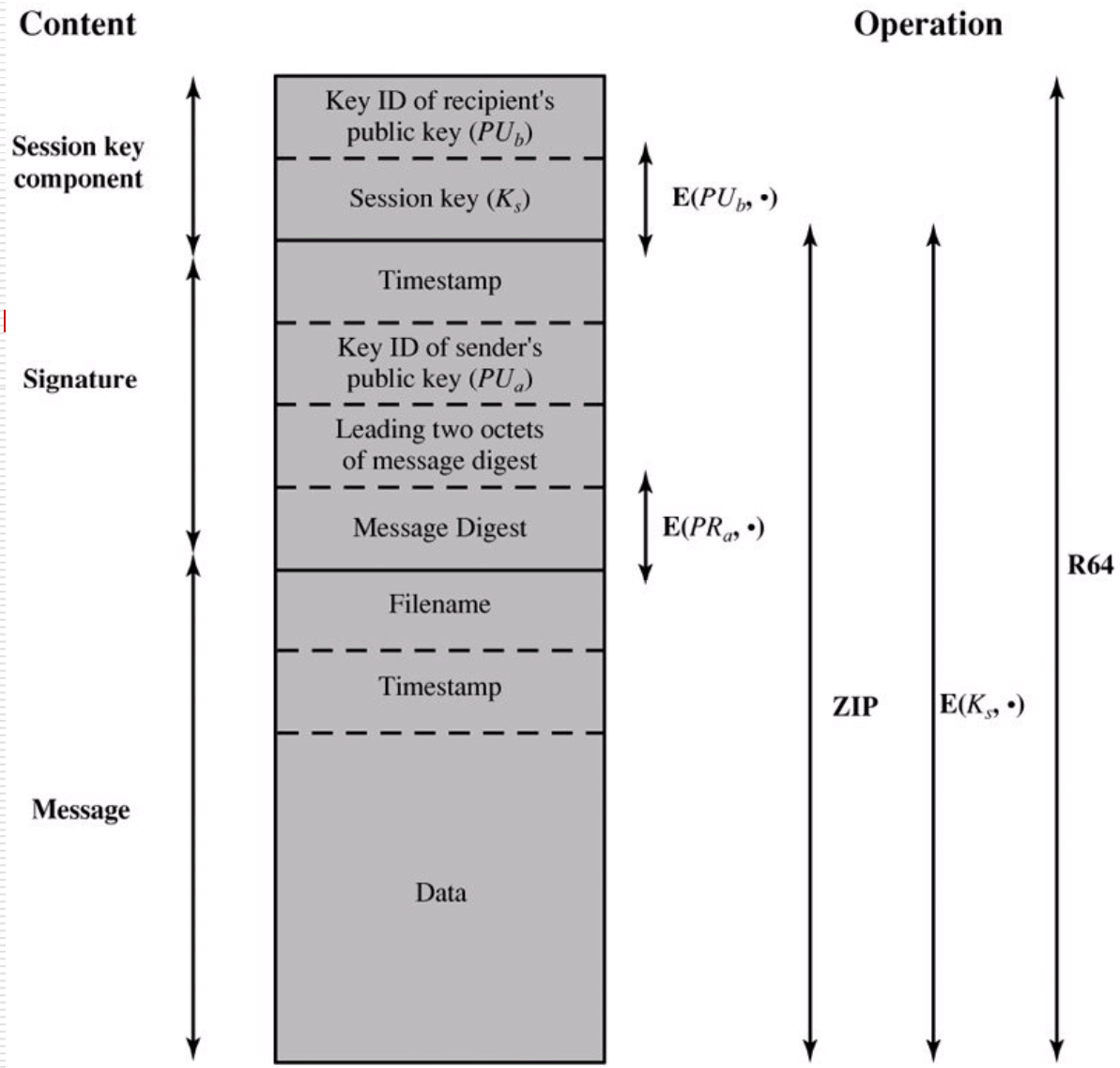
کلید جلسه

- به صورت تصادفی و یکبار مصرف ایجاد می‌گردد.
- الگوریتم تولید عدد تصادفی خود CAST-128 می‌باشد طبق استاندارد ANSI X12.17.
- الگوریتم از روی کلیدهای فشارداده شده روی صفحه کلید (و تاخیرهای زمانی در فشردن آنها) مقدار اولیه تصادفی می‌گیرد.
- سپس خروجی ۱۲۸ بیتی حاصل از رمزگذاری (با CAST-128) ورودی تصادفی (در دو قطعه ۶۴ بیتی) و کلید نشست قبلی در مُد CFB به عنوان کلید جلسه در نظر گرفته می‌شود.

کلیدهای مورد استفاده

- مسئله: امکان داشتن چند زوج کلید نامتقارن برای ارتباط با گروه‌های مختلف.
- راه حل: مشخص نمودن کلید استفاده شده بوسیله یک شناسه (Key Identifier)
- استفاده از ۶۴ بیت پایین کلید عمومی به عنوان شناسه
  - معادل $(PU_a \bmod 2^{64})$
  - احتمال برخورد بسیار پایین است.
  - شناسه برای کلید مربوط به امضاء و کلید مربوط به رمز کلید نشست.

قالب پیام در PGP



Notation:

$E(PU_b, \cdot)$ = encryption with user b's public key
$E(PR_a, \cdot)$ = encryption with user a's private key
$E(K_s, \cdot)$ = encryption with session key
ZIP = Zip compression function
R64 = Radix-64 conversion function

کلیدهای مورد استفاده

- دسته کلید خصوصی (Private Key Ring)
- برای مدیریت کلیدهای نامتقارن استفاده می‌شود. شامل موارد زیر است:

۱ - زمان تولید کلید ۲- شناسه کلید

۳ – کلید عمومی ۴-کلید خصوصی (بصورت رمزشده)

۵-شناسه مالک کلید

- کلید خصوصی توسط کلید متقارنی که از اِعمال یک تابع درهم‌ساز به گذرواژه کاربر حاصل می‌گردد، رمز می‌شود.
- جدول کلیدهای خصوصی روی ماشین صاحبش ذخیره می‌شود.

جدول 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
• • •	• • •	• • •	• • •	• • •

کلیدهای مورد استفاده

- دسته کلید عمومی (Public Key Ring)
- هر سطر جدول مربوطه یک گواهی کلید عمومی است که شامل موارد زیر است:

۱ - زمان تولید کلید ۲- شناسه کلید

۳ – کلید عمومی ۴- شناسه کاربر

۵- امضاهای کلید ۶- چند فیلد دیگر جهت امنیت بیشتر

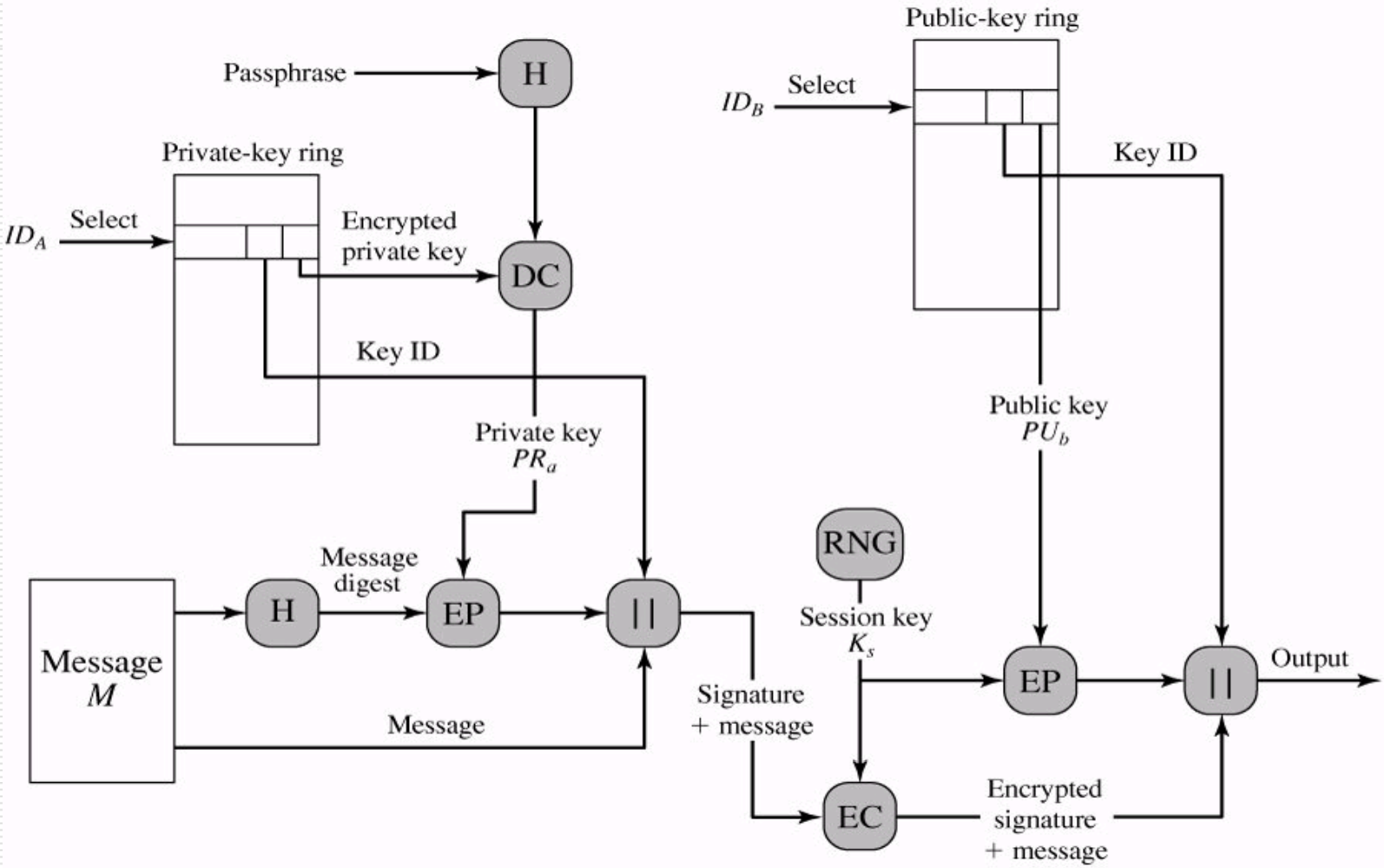
- این جدول شامل همه کلیدهای عمومی کاربران دیگر که برای این کاربر مشخص است، می‌باشد.

جدول کلید عمومی

Public-Key Ring

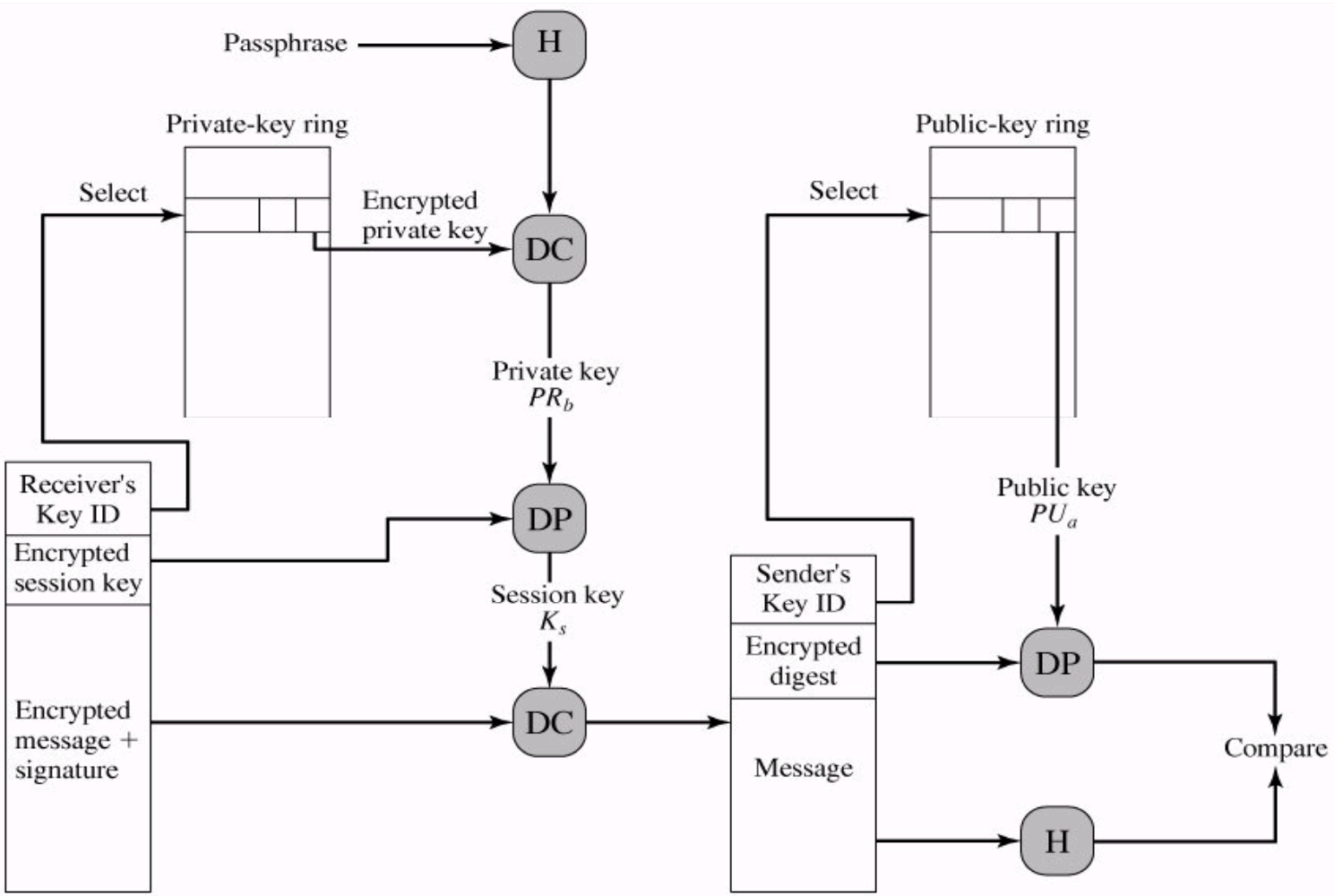
Timestamp	Key ID*	Public Key	Owner Trust	User ID*	Key Legitimacy	Signature(s)	Signature Trust(s)
• • •	• • •	• • •	• • •	• • •	• • •	• • •	• • •
T_i	$PU_i \bmod 2^{64}$	PU_i	trust_flag_i	User i	trust_flag_i		
• • •	• • •	• • •	• • •	• • •	• • •	• • •	• • •

تولید پیام در PGP



تولید پیام در PGP برای ارسال از A به B

دریافت پیام در PGP



دریافت پیام در PGP: دریافت از طرف A توسط B

فهرست مطالب

- امنیت پست الکترونیکی
- **پروتکل PGP**
  - ویژگی‌های PGP
  - سرویس‌های PGP
  - انواع کلیدهای مورد استفاده
  - **مدیریت کلید**
- پروتکل S/MIME

مدیریت کلید

- مشکل: در جدول کلیدهای عمومی A، یک کلید به ظاهر متعلق به کاربر B است، ولی در واقع متعلق به C است. در نتیجه C می‌تواند :
  - بجای B به A پیغام بفرستد.
  - پیام‌های ارسال شده از A به سمت B را بخواند.

مدیریت کلید عمومی در PGP

- ارسال کلید عمومی با امکان احراز اصالت
  - انتقال بصورت فیزیکی
    - در شبکه این روش غیرعملی است.
  - انتقال بصورت الکترونیکی و تایید توسط تلفن یا...
    - چکیده‌ای از کلید دریافتی از طریق تلفن با مالک بررسی شود.
  - انتقال توسط فرد مطمئنی که کلید عمومی وی در اختیار است.
    - کلید عمومی کاربر B توسط کاربر شناخته شده D امضاء و به کاربر A ارسال می‌شود.
  - انتقال بصورت گواهی تایید شده توسط مرجع قابل اعتماد.

مدیریت کلید

- PGP برای مدیریت کلیدهای عمومی بجای CA از مدلی بنام (Web of Trust) استفاده می‌کند.
- فیلدهای Trust (در بایتی تحت عنوان trust_flag نگهداری می شوند.)
  - فیلد key legitimacy: بیانگر میزان اعتماد به انتساب کلید عمومی به شناسه فرد.
  - فیلد signature trust: هر کلید عمومی ممکن است چند امضا داشته باشد. هر یک از این امضاها دارای یک درجه اعتماد هستند.
  - فیلد owner trust: بیانگر میزان اعتماد به صاحب کلید برای تایید اعتبار کلیدهای عمومی دیگر (گواهی) است.

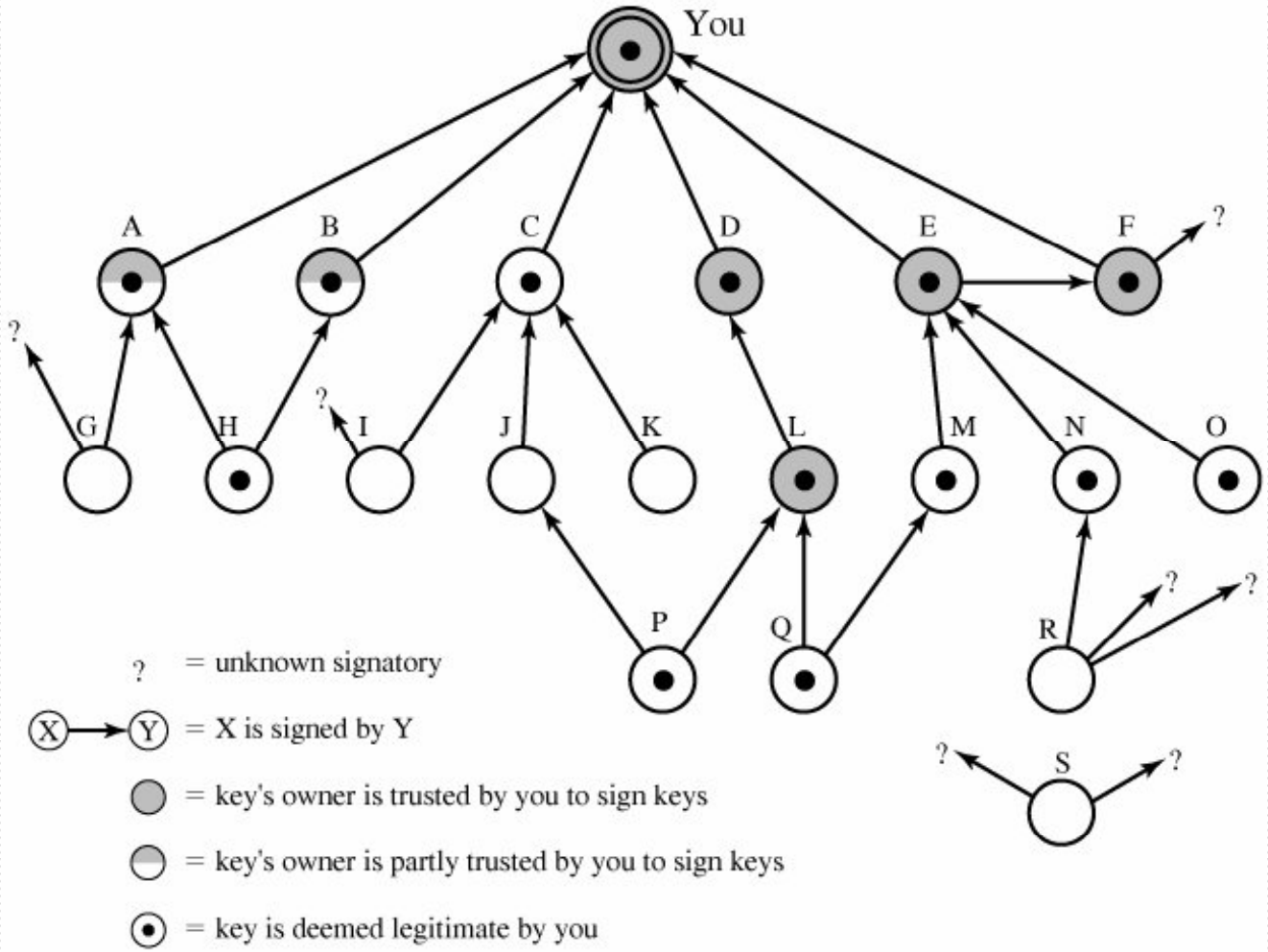
محاسبه مقادیر اعتماد

- با دریافت یک کلید عمومی توسط A، مقدار owner trust
  - اگر خود A مالک باشد: معادل ultimate trust
  - وگرنه، درخواست از A برای تعیین میزان اعتماد
- با درج کلید عمومی جدید به دسته کلید عمومی، مقدار signature trust هر امضاء
  - در صورت وجود مالک آن در دسته کلید، معادل owner trust مالک
  - در صورت عدم وجود مالک در دسته کلید، مقدار unknown user
- مقدار key legitimacy هر سطر کلید عمومی
  - اگر دارای یک امضاء با اعتماد ultimate باشد، معادل complete
  - وگرنه، جمع وزنی اعتماد امضاها: ضریب 1/x برای always trusted و ضریب 1/y برای usually trusted

محتوای بایت trust_flag

Trust Assigned to Public-Key Owner	Trust Assigned to Public Key/User ID Pair	Trust Assigned to Signature
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) **BUCKSTOP bit** • set if this key appears in secret key ring	**KEYLEGIT Field** • unknown or undefined trust • key ownership not trusted • marginal trust in key ownership • complete trust in key ownership **WARNONLY bit** • set if user wants only to be warned when key that is not fully validated is used for encryption	**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) **CONTIG bit** set if signature leads up a contiguous trusted certification path back to the ultimately trusted key ring owner

مثالی از مدل اعتماد در PGP



مدیریت کلید

- چند نکته در مورد شکل قبل
  - کلیدهای کاربرانی که مورد اعتماد یک کاربر می‌باشند، لزوما توسط وی امضاء نشده‌اند (مانند L).
  - اگر چند (x) کاربر که جزئاً قابل اعتماد هستند کلیدی را امضاء کنند، کلید مربوطه مورد تایید قرار می‌گیرد (H با امضای A و B).
  - کلیدی که تایید شده است، لزوماً نمی‌تواند برای تایید امضای کلید دیگری بکار رود (مانند N).
  - کلید کاربری که بطور غیرمستقیم امضاء شده است، ممکن است به صورت مستقیم نیز امضاء شود (مانند کلید E که توسط F و You به صورت غیرمستقیم و مستقیم امضا شده است).

ابطال کلید عمومی در PGP

- دلایل ابطال کلید عمومی
  - افشای کلید خصوصی
  - انقضای زمان استفاده از آن از دید مالک
- نحوه ابطال
  - تولید گواهی ابطال با امضای مالک (با همان کلید خصوصی)
  - انتشار گواهی ابطال توسط مالک در اولین فرصت به دیگر کابران
  - امکان سوء استفاده از این روش توسط مهاجم برای منع استفاده مالک از کلید، ولیکن این تهدید جدی نیست، چرا که دسترسی خود مهاجم نیز منع می‌شود.

فهرست مطالب

- امنیت پست الکترونیکی
- پروتکل PGP
  - ویژگی‌های PGP
  - سرویس‌های PGP
  - انواع کلیدهای مورد استفاده
  - مدیریت کلید
- **پروتکل S/MIME**

پروتکل S / MIME

- S/MIME نسخه امن‌سازی شده پروتکل تبادل ایمیل MIME است.
- برای بررسی S/MIME، ابتدا باید پروتکل‌های RFC 822 و MIME را بررسی نمود.
- مبتنی بر تکنولوژی ارائه شده توسط RSA Data Security.

قالب پیام RFC 822

- RFC 822 قالب پیام‌های متنی قابل ارسال از طریق ایمیل را تعریف می‌نماید.
- هر پیام شامل دو بخش است:
  - Envelop: شامل اطلاعات لازم برای ارسال و دریافت ایمیل است.
  - Content: شامل هر آنچه که باید ارسال شود، است.
- Content خود شامل دو بخش اصلی است:
  - Header: شامل تعدادی واژه کلیدی به همراه علامت (:) و مقدار مرتبط با واژه کلیدی.
  - Body: حاوی متن پیام که با یک خط خالی از Header جدا شده است.

قالب پیام RFC 822

Date: Tue, 9 May 2009 10:37:17 (EST)

From: “Morteza Amini” <m_amini@ce.sharif.edu>

Subject: Paper Submission

To: mycolleague@sharif.edu

Cc:

خط خالی

Dear colleague,

I hope this email finds you healthy and happy.

We need to revise our prepared paper before the submission.

Can we have a meeting ....

پروتکل MIME

- Multipurpose Internet Mail Extensions = **MIME**
- برای رفع محدودیت‌ها و مشکلات SMTP و قالب RFC 822 ارائه شده است.
- مهم ترین محدودیت‌ها و مشکلات:
  - عدم امکان ارسال داده‌های باینری (نیاز به تبدیل به داده‌های متنی)
  - عدم امکان ارسال داده‌های اسکی با کد ۱۲۸ و یا بالاتر (پشتیبانی از ASCII-7 که ۷ بیتی است)
  - محدودیت اندازه ایمیل ارسالی
  - ناسازگاری برخی از پیاده‌سازی‌های SMTP با استاندارد RFC 821

پروتکل MIME

- پنج فیلد جدید به سرآیند قالب RFC 822 اضافه شده است.
- چند قالب برای ارسال ایمیل‌های چندرسانه ای تدارک دیده شده است.

سرآیند MIME

- MIME Version: در حال حاضر باید 1.0 باشد.
- Content-Type: توصیف نوع داده ارسالی و مکانیزم و یا عامل موردنیاز برای باز کردن آن (مثال: video/quicktime).
- Content-Transfer-Encoding: نوع کدگذاری داده ارسالی (مثال: binary).
- Content-ID: برای شناسایی موجودیت‌های MIME در زمینه‌های مختلف.
- Content-Description: توصیفی از داده ارسالی (برای داده های صوتی که قابل مشاهده نیستند، مناسب است).

Content-Type در MIME

Type	Subtype	Description
Text	Plain	Unformatted text; may be ASCII or ISO 8859.
	Enriched	Provides greater format flexibility.
Multipart	Mixed	The different parts are independent but are to be transmitted together. They should be presented to the receiver in the order that they appear in the mail message.
	Parallel	Differs from Mixed only in that no order is defined for delivering the parts to the receiver.
	Alternative	The different parts are alternative versions of the same information. They are ordered in increasing faithfulness to the original, and the recipient's mail system should display the "best" version to the user.
	Digest	Similar to Mixed, but the default type/subtype of each part is message/rfc822.
Message	rfc822	The body is itself an encapsulated message that conforms to RFC 822.
	Partial	Used to allow fragmentation of large mail items, in a way that is transparent to the recipient.
	External-body	Contains a pointer to an object that exists elsewhere.
Image	jpeg	The image is in JPEG format, JFIF encoding.
	gif	The image is in GIF format.
Video	mpeg	MPEG format.
Audio	Basic	Single-channel 8-bit ISDN mu-law encoding at a sample rate of 8 kHz.
Application	PostScript	Adobe Postscript.
	octet-stream	General binary data consisting of 8-bit bytes.

قالب پیام MIME

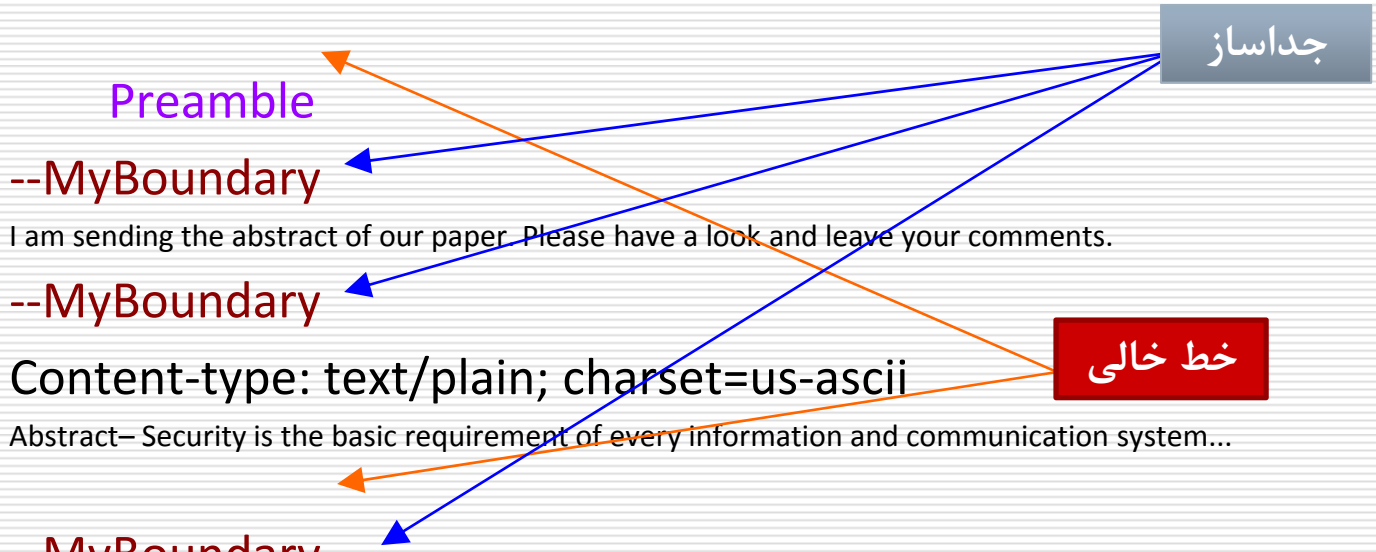
From: “Morteza Amini” <m_amini@ce.sharif.edu>

To: “My Colleague” <mycolleague@gmail.com>

Subject: Paper Submission

MIME-Version: 1.0

Content-type: multipart/mixed; boundary=“MyBoundary”



کدگذاری در MIME

7bit	کد اسکی ۷ بیتی
8bit	کد اسکی ۸ بیتی که ممکن است حاوی کاراکترهای غیراسکی نیز باشد.
binary	باینری
quoted-printable	تبدیل به کاراکترهای قابل چاپ به گونه‌ای که تاحد ممکن متن قابل فهم باشد. به جای کاراکترهای خاص، کد هگزای آنها ارسال می‌شود.
base64	تبدیل هر ۶ بیت ورودی به ۸ بیت اسکی قابل چاپ در خروجی (همان کدگذاری Radix-64)
x-token	کدگذاری غیراستاندارد دلخواه

قالب کانونی

- یکی از مفاهیم اساسی در MIME و S/MIME قالب کانونی داده‌ها است.
- قالب کانونی، قالبی مناسب نوع داده (Content-Type) است، که برای استفاده بین سیستم‌های مختلف استاندارد شده است.
- ممکن است شامل تبدیل مجموعه کاراکترها، EOL، تبدیل داده‌های صوتی، فشرده‌سازی و ... باشد.

قابلیت های S / MIME

- S/MIME قابلیت‌هایی مشابه قابلیت‌های PGP را فراهم می‌آورد.
- چهار قابلیت ارائه شده توسط S/MIME:
  - Enveloped data: متن رمز شده همراه با کلید
  - Signed data: داده همراه با امضاء که با base64 کدگذاری شده‌اند.
  - Clear-Signed data: داده همراه با امضاء که در آن صرفاً امضاء کدگذاری شده است.
  - Signed & Enveloped data: ترکیبی از داده رمز شده و امضاء است.

الگوریتم های S/MIME

- DSS: الگوریتم امضاء توصیه شده
- DH (ElGamal): توصیه شده برای رمز کلید جلسه
- RSA: برای امضاء و یا رمزنگاری
- 3DES/RC2 (40 bits): برای رمزگذاری پیام
- SHA-1/MD5: برای تولید چکیده پیام

- در S/MIME تعدادی قاعده برای انتخاب الگوریتم درنظر گرفته شده است (قواعد الزام- MUST و قواعد اختیار- SHOULD).

Content-Type در S/MIME

Type	Subtype	smime Parameter	Description
Multipart	Signed		A clear-signed message in two parts: one is the message and the other is the signature.
Application	pkcs 7-mime	signedData	A signed S/MIME entity.
	pkcs 7-mime	envelopedData	An encrypted S/MIME entity.
	pkcs 7-mime	degenerate signedData	An entity containing only public- key certificates.
	pkcs 7-mime	CompressedData	A compressed S/MIME entity
	pkcs 7-signature	signedData	The content type of the signature subpart of a multipart/signed message.

Enveloped Data

- مراحل ایجاد یک موجودیت MIME از نوع Enveloped Data:
  - تولید یک عدد شبه تصادفی به عنوان کلید جلسه (رمز 3DES یا RC2/40)
  - رمز کلید جلسه با کلید عمومی هر یک از گیرندگان ایمیل
  - برای هر گیرنده ایجاد یک بلوک RecipientInfo حاوی
    - شناسه گواهی کلید عمومی گیرنده
    - شناسه الگوریتم رمز به کار رفته برای رمز کلید جلسه
    - کلید جلسه رمز شده
  - رمز محتوای پیام با کلید جلسه
- بلوکهای RecipientInfo به همراه محتوای رمز شده، پیام envelopedData را حاصل می‌نماید، که با base64 کد شده است.

Signed Data

- مراحل ایجاد یک موجودیت MIME از نوع Signed Data:
  - انتخاب الگوریتم درهم ساز (SHA-1 یا MD5) و محاسبه چکیده پیام
  - رمز چکیده با کلید خصوصی فرستنده
  - ایجاد یک بلوک SignerInfo حاوی
    - گواهی کلید عمومی فرستنده
    - شناسه الگوریتم درهم ساز تولید چکیده و شناسه الگوریتم رمز تولید امضاء
    - چکیده رمز شده
- بلوک SignerInfo به همراه پیام امضاء شده (گاهی همراه با زنجیره گواهی‌های تا ریشه) ، یک موجودیت signedData را حاصل می‌نمایند، که با base64 کد شده است.

Clear Signing

- پیام قابل مشاهده توسط کارگزارهای MIME (که از S/MIME پشتیبانی نمی‌کنند).
- استفاده از پیام از نوع multipart/signed حاوی دو قطعه:
  - قطعه اول: پیام آشکار که باید در طی ارسال بدون تغییر بماند، لذا در صورت نیاز باید (قبل از امضاء) تبدیل لازم بر روی آن صورت گیرد.
  - قطعه دوم: امضای پیام از نوع application/pkcs7-signature کد شده با base64.

درخواست ثبت گواهی کلید عمومی

- درخواست ثبت گواهی کلید عمومی می‌تواند با استفاده از موجودیت MIME با نوع application/pkcs10 ارسال شود.
- درخواست گواهی شامل موارد زیر است:
  - بلوک CertificateRequestInfo که خود حاوی
    - نام عامل متقاضی گواهی
    - رشته کلید عمومی متقاضی
  - شناسه الگوریتم رمزگذاری کلید عمومی
  - امضای بلوک CertificateRequestInfo با استفاده از کلید خصوصی فرستنده.

پیام گواهی

- Certificate-Only Message
- یک پیام حاوی صرفاً گواهی‌ها و یا لیست گواهی‌های باطل شده به عنوان پاسخ درخواست گواهی.
- این پیام از نوع application/pkcs7-mime با پارامتر degenerate است.
- مراحل ایجاد این پیام مشابه ایجاد signedData است، با این تفاوت که محتوای پیام خالی است و فیلد signerInfo خالی است.

گواهی‌های کلید عمومی در S / MIME

- S/MIME از گواهی کلید عمومی X.509 V3 پشتیبانی می‌کند.
- بهره گیری از روشی مرکب از روش PGP و روش PKI برای مدیریت کلید
- مدیریت کلیدها و گواهی‌های کلید عمومی به صورت محلی صورت می‌پذیرد ولیکن هر گواهی امضای یک مرکز CA را دارد.

مدیریت کلید در S/MIME

- تولید کلید:
  - کاربر باید با روشی مناسب کلیدهای تصافی مودنیاز را تولید کرده، کلیدهای خصوصی را به صورت امن نگهداری نماید.
- ثبت گواهی کلید عمومی:
  - کاربر باید کلید عمومی خود را در یک مرکز CA ثبت نموده، گواهی X.509 کلید عمومی مورد نظر را دریافت نماید.
- ذخیره و بازیابی گواهی‌های کلید عمومی:
  - کاربر باید به گواهی‌ها و لیست گواهی‌های باطل شده به صورت محلی دسترسی داشته باشد.
  - مدیر می‌تواند برای تعدادی از کاربران یک لیست محلی نگهداری نماید.

پایان

مرکز امنیت داده و شبکه شریف

http://dnsl.ce.sharif.edu

پست الکترونیکی

m_amini@ce.sharif.edu

شبکه آموزشی- پژوهشی مادسیج
با هدف بهبود پیشرفت علمی
و دسترسی راحت به اطلاعات
برای جامعه بزرگ علمی ایران
ایجاد شده است

madsg.com

مادسیج

IRan Education & Research NETwork
(IRERNET)