Electronic Mail Security: PGP

Contents:

- What is PGP?
- What services can PGP provide?
- Mechanisms of PGP.
- About S/MIME

What is PGP?

- PGP stands for *Pretty Good Privacy*.
- Initially developed (in 1991) and large amount of work being done by Philip R. Zimmermann.
  - Cryptographic algorithm selection, both symmetric key and asymmetric key algorithms;
  - Integrate these algorithms into an application package.
  - Produce application package and its documentation.
- It has been supported by many individuals and corporations.
- It has become a de facto standard for personal email security.

Features of PGP

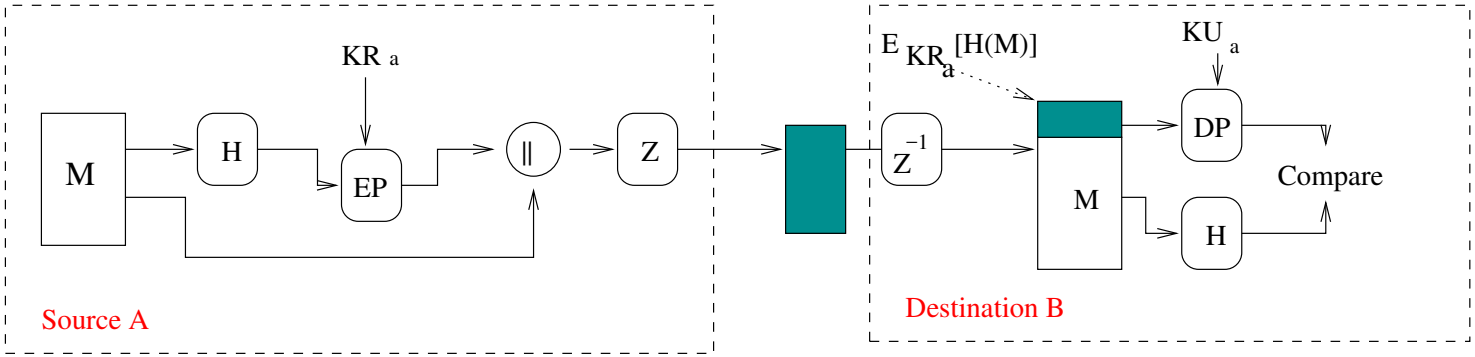
- Services that PGP can provide:
  - Data content confidentiality.
  - Data integrity.
  - Authentication (limited, as the public keys are not perfectly authenticated).
- Crypto algorithms used in PGP:
  - Symmetric block cipher, for message encryption.
  - Public key cipher, for key distribution and digital signatures.
  - Hash functions, for message integrity.
- Working platforms:
  - DOS/Windows; Macintosh; Unix; And many more.

Crypto Algorithms in PGP

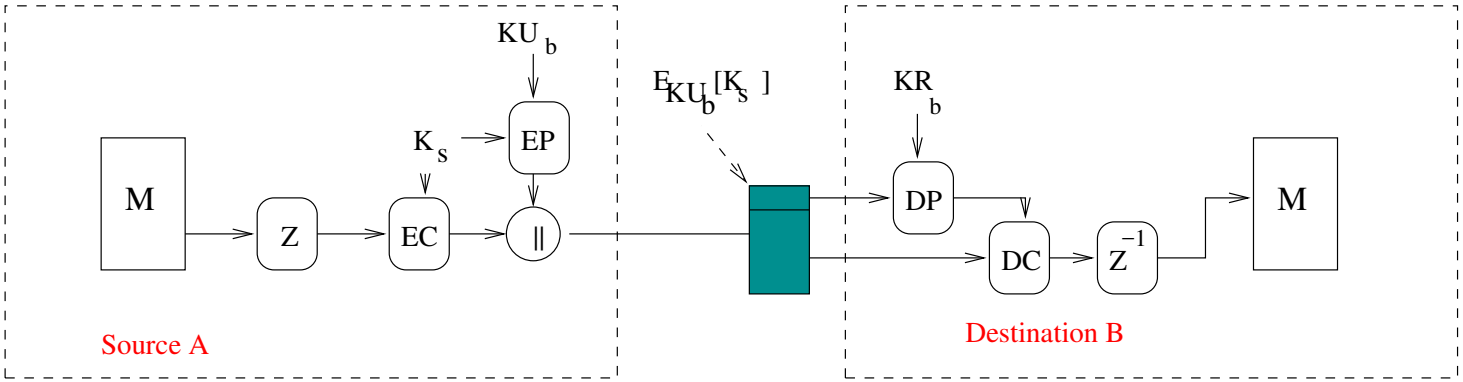
- Symmetric block ciphers for conventional encryption:
  - CAST-128;
  - IDEA;
  - Triple-DES;
  - Open features for new ones to join. ($\Leftarrow$ AES?)
- Public key ciphers for session key distribution:
  - Diffie-Hellman;
  - RSA;
- Public key ciphers for authentication via digital signatures:
  - RSA;
  - DSS.
- Hash functions for message integrity:
  - SHA-1.
- Optional security services:
  - Secrecy, authentication, or both.

PGP Cryptographic Functions

- Authentication only.

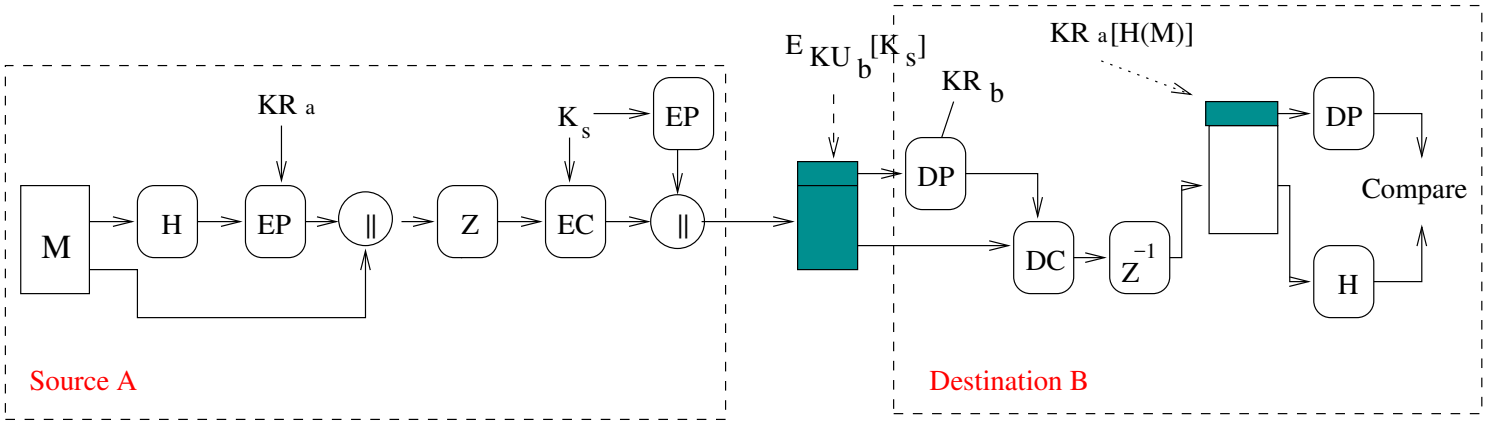


- Confidentiality only.



PGP Cryptographic Functions

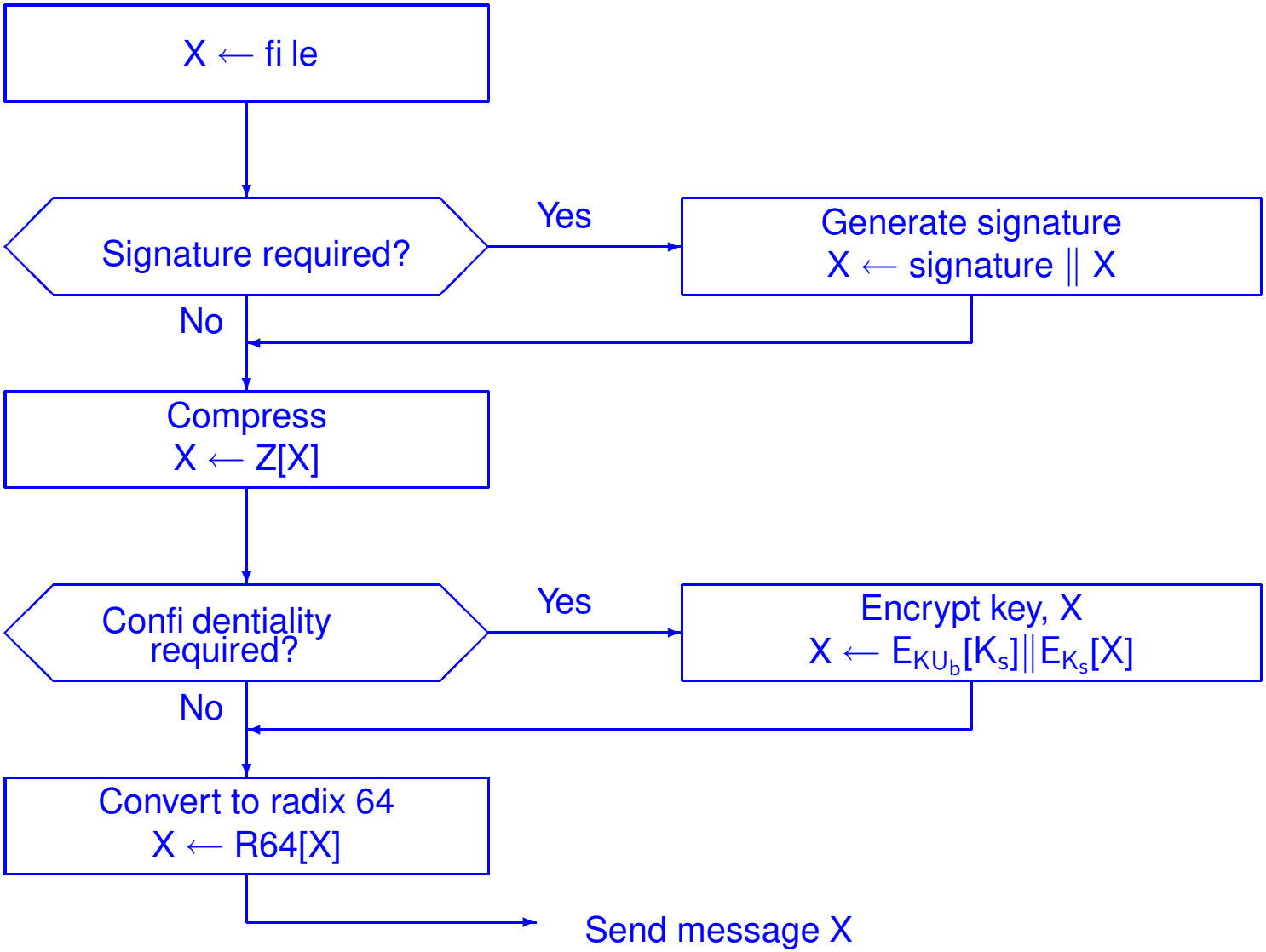
- Confidentiality and Authentication.



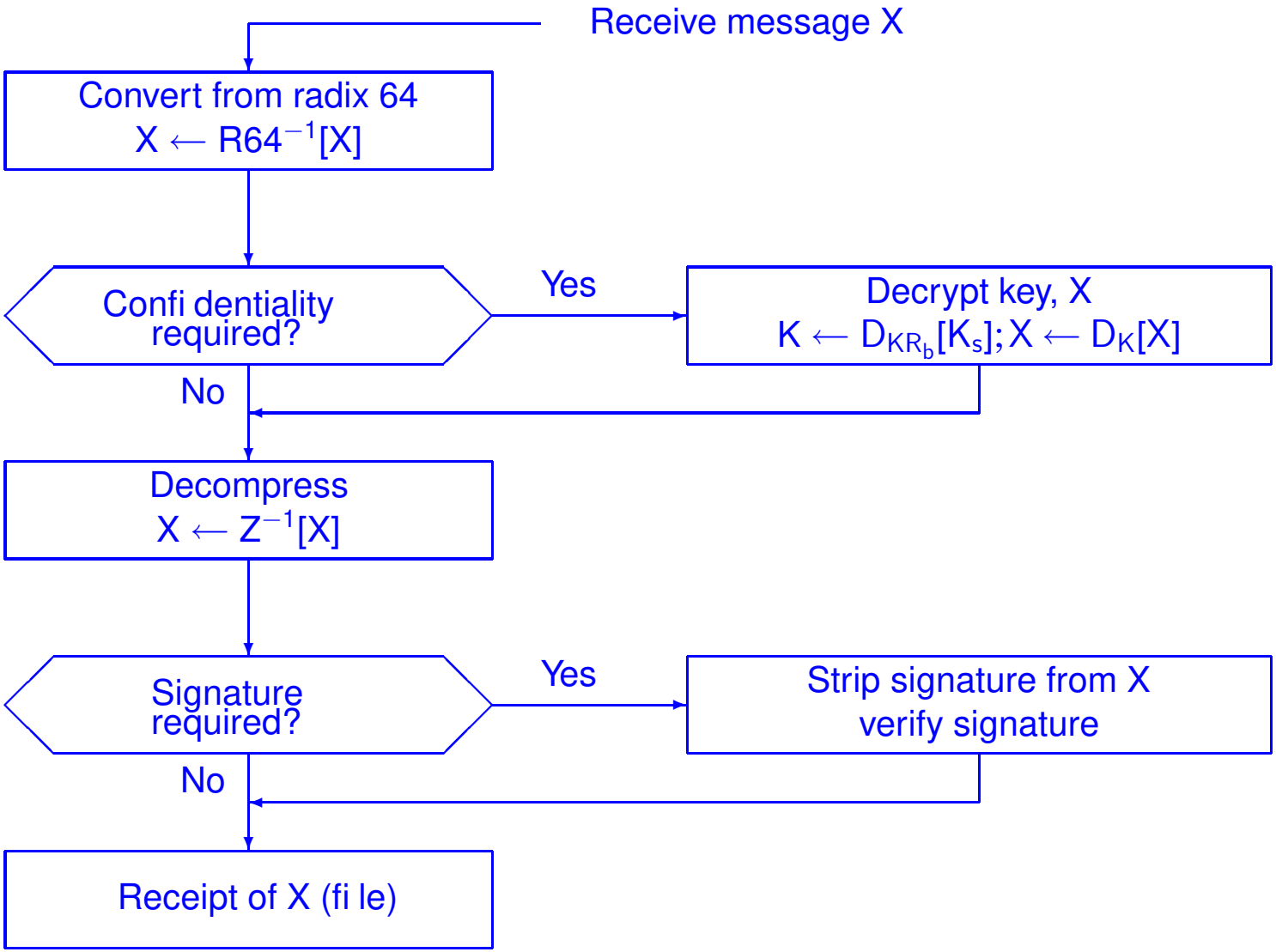
PGP Functions

- Signature:
  - SHA-1 + DSS/RSA.
- Message encryption:
  - one-time session key;
  - session key encrypted using D-H/RSA;
  - message encrypted using CAST-128/IDEA/3DES.
- Compression:
  - ZIP
- Email compatibility:
  - Radix 64-conversion. It expands a message by 33% on average.
- Segmentation and re-assembling:
  - maximum length 50,000 octets.

PGP message Transmission



PGP message Reception



PGP keys

- One-time session key: random number generator.
- Public/private keys: multiple choices.
- Management: a file with private key and public key pairs (private keys are in encrypted form).
- Key identifier
  - attach public key to the message?
  - Key ID? Key management burdensome.
  - KU_a mod 2^{64}, a semi key ID.

PGP Key Rings

- Consider Sender is sending a message to Receiver using PGP. Each has a local server (node, in network terms).
- Each node has 2 data structures A and B.
  - A: public/private key pairs owned by the node.
  - B: public keys of others known to this node.
- Private keys are in encrypted form.
- Data structures A and B are referred to as **private-key ring** and **public-key ring**.

About S/MIME

- Electronic Mail Transfer Protocols:
  - Simple Mail Transfer Protocol (SMTP);
  - Multipurpose Internet Mail Extensions (MIME).
- S/MIME: stands for *Secure/Multipurpose Internet Mail Extension*.
- Security enhanced version of MIME Internet email standard.
- Targeting at industry standard.
- Compared with PGP, format more fixed (less flexibility).
- Utilizes X.509 protocol for key management.

Features of SMTP

- Text type: text mail messages only.
- Text format:
  - envelope: header information.
  - message body: content of email.
  - Headers and body are separated by a blank line.
- Header fields:
  - Date: Time the message was sent.
  - From: Sender's name.
  - Sender: Email address of the actual sender.
  - To: Primary Receiver's address(es).
  - Subject: A short title about the message.
  - Many other fields.
- Message processing:
  - **user agent**, for sending and reading emails, and
  - **delivery agent**, or **message transfer agent**, for moving the messages from the source to destinations.

Features of MIME

- Apart from the features from SMTP, MIME also has the following features:
  - handling none ASCII characters, such as
    - Messages in languages with accents (e.g. French and German);
    - Messages in nonLatin alphabets (e.g. Hebrew and Russian);
    - Message in languages without alphabets (e.g. Chinese and Japanese);
    - Messages not containing text at all (e.g. audio and video).
  - More flexible on size limitation from SMTP and other amendments.
- Added Header Fields.
  - MIME Version.
  - Content-Type.
    - Text, image, audio, video, application, multipart.
  - Content-Transfer-Encoding.
    - base64 Encoding, quoted-printable encoding, etc.
  - Content-ID.
  - Content-Description.

S/MIME Functionality

- enveloped data: message content is encrypted.
- signed data: message digest signed, then content + signature are encoded using Base64 encoding.
- Clear signed data: only signature is encoded, recipients without S/MIME capability can view the message.
- Signed and enveloped data: both of the above functionality involved.
- Cryptographic algorithms used: 3DES, SHA/MD5.

S/MIME Key Management

- Use X.509 type of certification hierarchy, but the *trust* to the certification authority is a pre-condition.
- *VeriSign* is one of the certification authorities.
- Use of certificate is based on the trust assumption on the CAs.
- Certificates can be forged (e.g. MicroSoft certificates). So use them at your own risk.
- There is no absolute trust anyway. A reputable business goodwill perhaps worths trust.