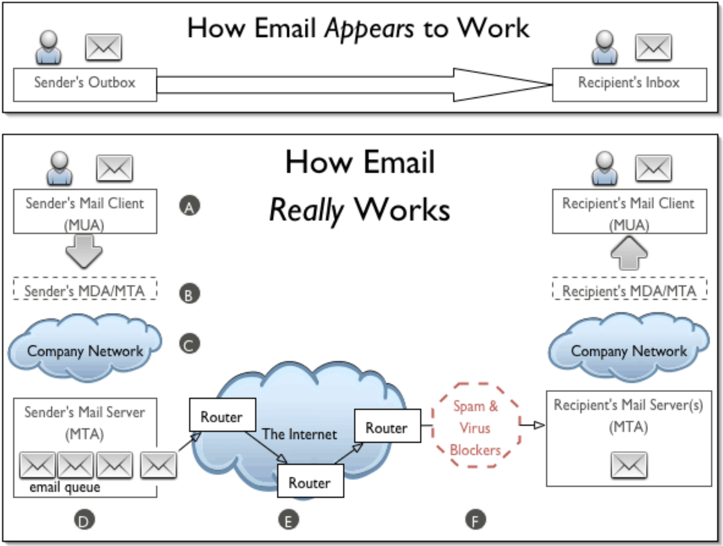
19CSE311 - COMPUTER SECURITY
UNIT-3- PART 1
Email Security

March 15, 2022

Dr.Remya S/ Mr. Sarath R
Assistant Professor
Department of Computer Science

AMRITA VISHWA VIDYAPEETHAM
DEEMED TO BE UNIVERSITY
School of Engineering

How an Email works?



1. Sender creates and sends an email
   - The originating sender creates an email in their Mail User Agent (MUA) and clicks 'Send'.
   - The MUA is the application the originating sender uses to compose and read email, such as Eudora, Outlook, etc
2. Sender's MDA/MTA routes the email
   - The sender's MUA transfers the email to a Mail Delivery Agent (MDA).
   - Frequently, the sender's MTA also handles the responsibilities of an MDA.
   - The MDA/MTA accepts the email, then routes it to local mailboxes or forwards it if it isn't locally addressed.
   - In the diagram, an MDA forwards the email to an MTA and it enters the first of a series of "network clouds," labeled as a "Company Network" cloud.

3. Network Cloud
    - An email can encounter a network cloud within a large company or ISP, or the largest network cloud in existence: the Internet.
    - The network cloud may encompass mail servers, DNS servers, routers and other devices and services
4. Email Queue
    - The email is addressed to someone at another company, so it enters an email queue with other outgoing email messages.
    - If there is a high volume of mail in the queue—either because there are many messages or the messages are unusually large, or both—the message will be delayed in the queue until the MTA processes the messages ahead of it.
5. MTA to MTA Transfer
    - When transferring an email, the sending MTA handles all aspects of mail delivery until the message has been either accepted or rejected by the receiving MTA.
    - As the email clears the queue, it enters the Internet network cloud, where it is routed along a host-to-host chain of servers.
    - Each MTA in the Internet network cloud needs to "stop and ask directions" from the Domain Name System (DNS) in order to identify the next MTA in the delivery chain.

6. Firewalls, Spam and Virus Filters
   - An email may be transferred to more than one MTA within a network cloud and is likely to be passed to at least one firewall before it reaches it's destination.
   - An email encountering a firewall may be tested by spam and virus filters before it is allowed to pass inside the firewall.
   - These filters test to see if the message qualifies as spam or malware. If the message contains malware, the file is usually quarantined and the sender is notified. If the message is identified as spam, it will probably be deleted without notifying the sender.

Why Email security?

- In virtually all distributed environments, electronic mail is the most heavily used network-based application.
- Users expect to be able to, and do, send e-mail to others who are connected directly or indirectly to the Internet, regardless of host operating system or communications suite. With the explosively growing reliance on e-mail, there grows a demand for authentication and confidentiality services.
- Two schemes stand out as approaches for widespread use:
  1. Pretty Good Privacy (PGP)
  2. S/MIME.

Email Security Enhancements

1. Confidentiality-protection from disclosure
2. Authentication of sender of message
3. Message Integrity- protection from modification
4. Non-repudiation of origin- protection from denial by sender

Pretty Good Privacy(PGP)

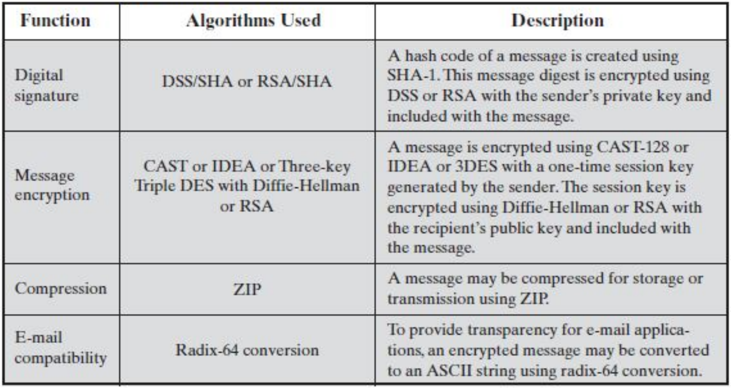
- Coined by Phil Zimmermann
- PGP is an open-source, freely available software package for e-mail security
- PGP encryption is a data encryption computer program that gives cryptographic privacy and authentication for online communication.
- It provides authentication through the use of digital signature, confidentiality through the use of symmetric block encryption, compression using the ZIP algorithm, and e-mail compatibility using the radix-64 encoding scheme.
- PGP incorporates tools for developing a public-key trust model and public-key certificate management
- It is often used to encrypt and decrypt texts, emails, and files to increase the security of emails.
- PGP encryption uses a mix of data compression, hashing, and public-key cryptography.

- It also uses symmetric and asymmetric keys to encrypt data that is transferred across networks. It combines features of private and public key cryptography.
- When plaintext is encrypted with PGP, it first compresses the plaintext. Data compression saves transmission time, disk space, and reinforces cryptographic security.

PGP Services

1. Authentication
2. Confidentiality
3. Compression
4. E-mail compatibility

Table 18.1 Summary of PGP Services

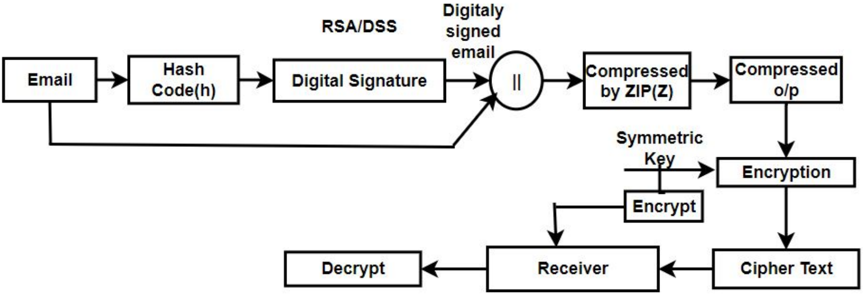


Function	Algorithms Used	Description
Digital signature	DSS/SHA or RSA/SHA	A hash code of a message is created using SHA-1. This message digest is encrypted using DSS or RSA with the sender's private key and included with the message.
Message encryption	CAST or IDEA or Three-key Triple DES with Diffie-Hellman 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.

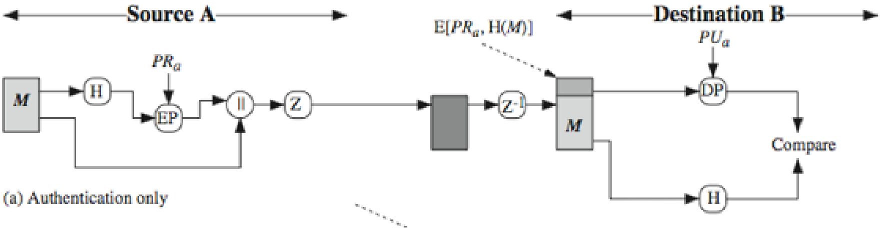
PGP-3 Cases

- Authentication only
- Confidentiality only
- Authentication+Confidentiality

PGP-generalized procedure



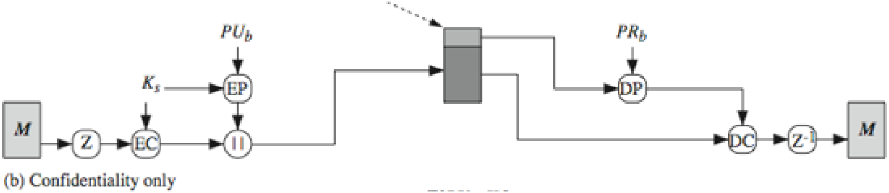
Authentication



(a) Authentication only

1. The sender creates a message.
2. SHA-1 is used to generate a 160-bit hash code of the message.
3. The hash code is encrypted with RSA using the sender's private key, and the result is prepended to the message.
4. The receiver uses RSA with the sender's public key to decrypt and recover the hash code.
5. The receiver generates a new hash code for the message and compares it with the decrypted hash code. If the two match, the message is accepted as authentic

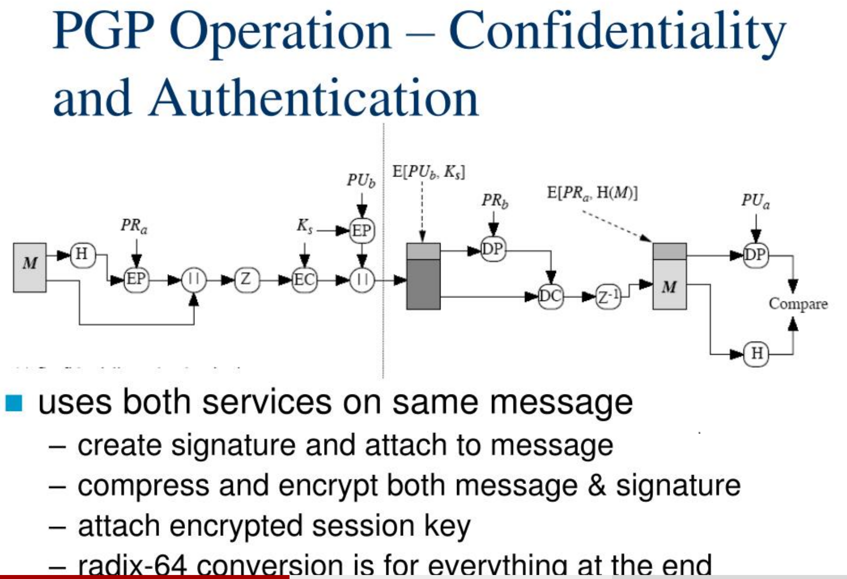
Confidentiality



(b) Confidentiality only

1. The sender generates a message and a random 128-bit number to be used as a session key for this message only.
2. The message is encrypted using CAST-128 (or IDEA or 3DES) with the session key.
3. The session key is encrypted with RSA using the recipient's public key and is prepended to the message.
4. The receiver uses RSA with its private key to decrypt and recover the session key.
5. The session key is used to decrypt the message.

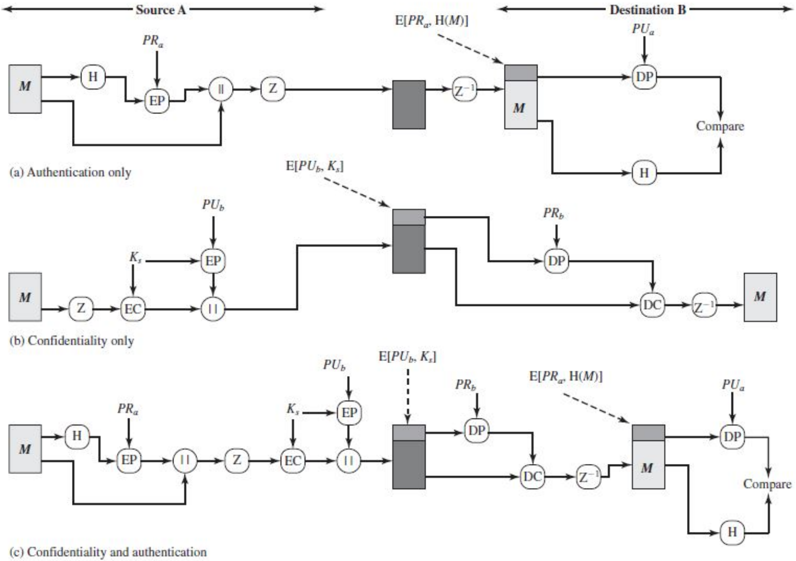
Authentication+Confidentialty



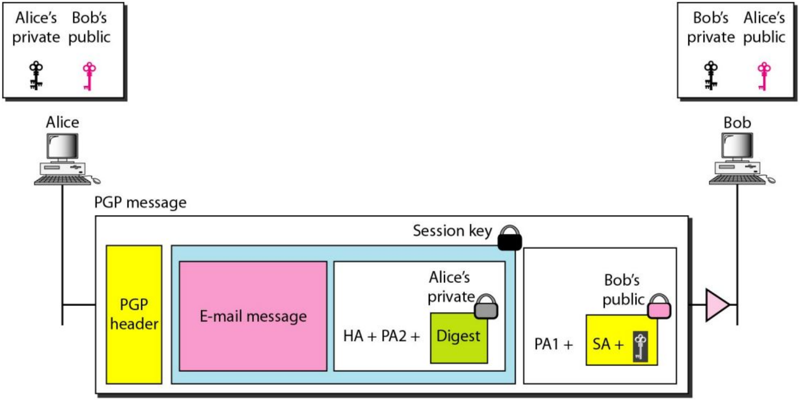
PGP Operation – Confidentiality and Authentication

- uses both services on same message
  - create signature and attach to message
  - compress and encrypt both message & signature
  - attach encrypted session key
  - radix-64 conversion is for everything at the end

PGP-3 Cases



Source A
Destination B
$E[PR_a, H(M)]$
PR_a
PU_a
M
H
EP
||
Z
Z^{-1}
DP
Compare
(a) Authentication only
$E[PU_b, K_s]$
PU_b
K_s
PR_b
EC
DC
(b) Confidentiality only
(c) Confidentiality and authentication



PA1: Public-key algorithm 1 (for encrypting session key)
PA2: Public-key algorithm (for encrypting the digest)
SA: Symmetric-key algorithm identification (for encrypting message and digest)
HA: Hash algorithm identification (for creating digest)

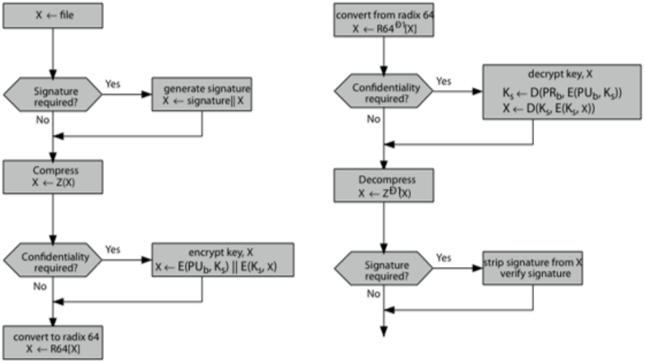
Compression

- As a default, PGP compresses the message after applying the signature but before encryption.
- This has the benefit of saving space both for e-mail transmission and for file storage.
- The signature is generated before compression for the following reasons:
  1. It is preferable to sign an uncompressed message so that one can store only the uncompressed message together with the signature for future verification. If one signed a compressed document, then it would be necessary either to store a compressed version of the message for later verification or to recompress the message when verification is required
  2. Even if one were willing to generate dynamically a recompressed message for verification, PGP's compression algorithm presents a difficulty.
  3. Message encryption is applied after compression to strengthen cryptographic security. Because the compressed message has less redundancy than the original plaintext, cryptanalysis is more difficult.

Email Compatibility

- when using PGP will have binary data to send (encrypted message etc)
- however email was designed only for text
- hence PGP must encode raw binary data into printable ASCII characters
- uses radix-64 algorithm
- PGP also segments messages if too big

PGP-summary



(a) Generic Transmission Diagram (from A)

(b) Generic Reception Diagram (to B)

S/MIME

- Another security service designed for electronic mail is Secure/Multipurpose Internet Mail Extension (S/MIME).
- The protocol is an enhancement of the Multipurpose Internet Mail Extension (MIME) protocol.
- S/MIME will probably emerge as the industry standard.
- Previously, emails could be sent only in NVT 7 bit ASCII format(ie, Audio, video, images etc could not be sent)
- Therefore MIME is introduced
- MIME is an add-on which allows us to transfer non ASCII data over mail
- S/MIME(Secure/MIME) encrypts email and provides security
- S/MIME allows to digitally sign on our email
- uses asymmetric key cryptography

Functions of S/MIME

1. Authentication
2. Message Integrity
3. Non repudiation(using digital signature)
4. Privacy
5. Data security(using encryption)

- S/MIME provide 2 security services
  1. Digital signature(provides authentication+non repudiation
  2. Message encryption(provides confidentiality+ data integrity)

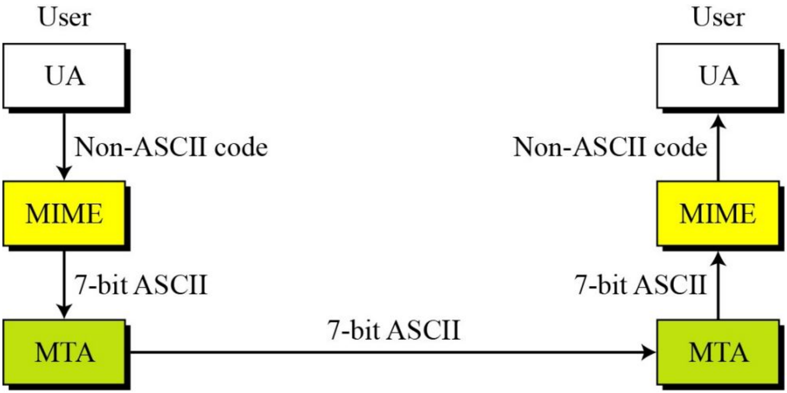
MIME

- MIME is a standard proposed by BELL communications in 1991 in order to expand the limited capabilities of email
- Email has a simple structure. Email can send messages only in NVT(Network Virtual Terminal) 7 bit ASCII format
- MIME is a supplementary protocol or add on which allows non ASCII data to be send through email using SMTP
- Email messages with MIME formatting are typically transmitted with the standard protocol like SMTP, POP & IMAP
- Although MIME was designed mainly for SMTP, its content types are also important in other communication protocols
- Eg: In HTTP protocol for WWW, servers insert a MIME header file at the beginning of the transaction

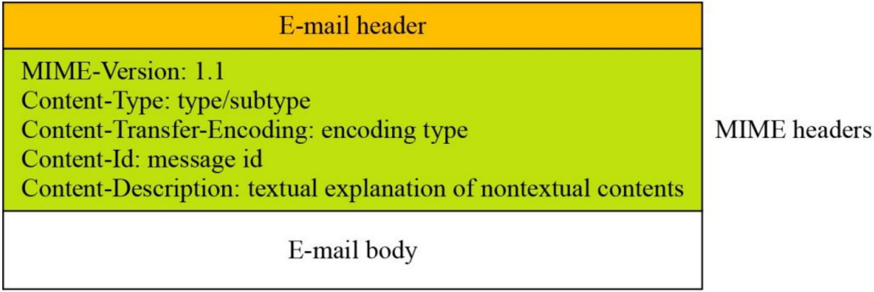
Why MIME?
Limitations of SMTP protocol

- SMTP has a very simple structure
- SMTP can only send the messages in NVT 7 bit ASCII format
- It cannot be used for languages that do not support 7 bit ASCII format such as French, German etc. So in order to make SMTP more broad we use MIME
- It can not be used to send binary files or video or audio data

MIME


User
UA
Non-ASCII code
MIME
7-bit ASCII
MTA
7-bit ASCII
User
UA
Non-ASCII code
MIME
7-bit ASCII
MTA

MIME Header



E-mail header

MIME-Version: 1.1
Content-Type: type/subtype
Content-Transfer-Encoding: encoding type
Content-Id: message id
Content-Description: textual explanation of nontextual contents

MIME headers

E-mail body