

Announcements

- Reading
 - 7.5-7.6
- Project #5 is due on Monday
- Signups for demos was circulated
 - Schedule is at <http://www.cs.umd.edu/~hollings/cs417/f01/prog5/demoSchedule.html>
 - If you missed class, please email hollings@cs.umd.edu

Message Body

- Under RFC822
 - raw ascii text with no semantic meaning
- MIME: Multipurpose Internet Mail Extension
 - provides an interface to send non-ascii text in mail
 - envelop not changed, so only user agents need to be modified
 - supports multiple languages
 - supports multi-media and file attachments
 - headers:
 - MIME-Version
 - Content-Description: human readable description
 - Content-Id: unique id for this part of the message
 - Content-Transfer-Encoding:
 - text: ascii, and 8bit characters
 - binary: may not get there since it is a non-conforming body
 - base64: 26 binary bits-> 4 ascii characters
 - quoted printable: only use base64 for “special” characters
 - Content-Type: what is this

Mime Types

- There is a standard set of type (these are from RFC1521)
 - text/plain
 - text/richtext: based on SGML and similar to HTML
 - image/gif
 - image/jpeg
 - audio/basic
 - video/mpeg
 - application/octet-stream: no semantic meaning
 - application/postscript: Postscript printer files
 - message/rfc822: a full email message with envelop
 - message/partial: part of a multi-message message
 - message/external-body
 - multipart/mixed
 - multipart/alternative: alternative formats for a body (text, postscript)
 - multipart/parallel: all parts must be viewed together
 - multipart/digest: collection of messages (sort of an array type)

Transferring Messages

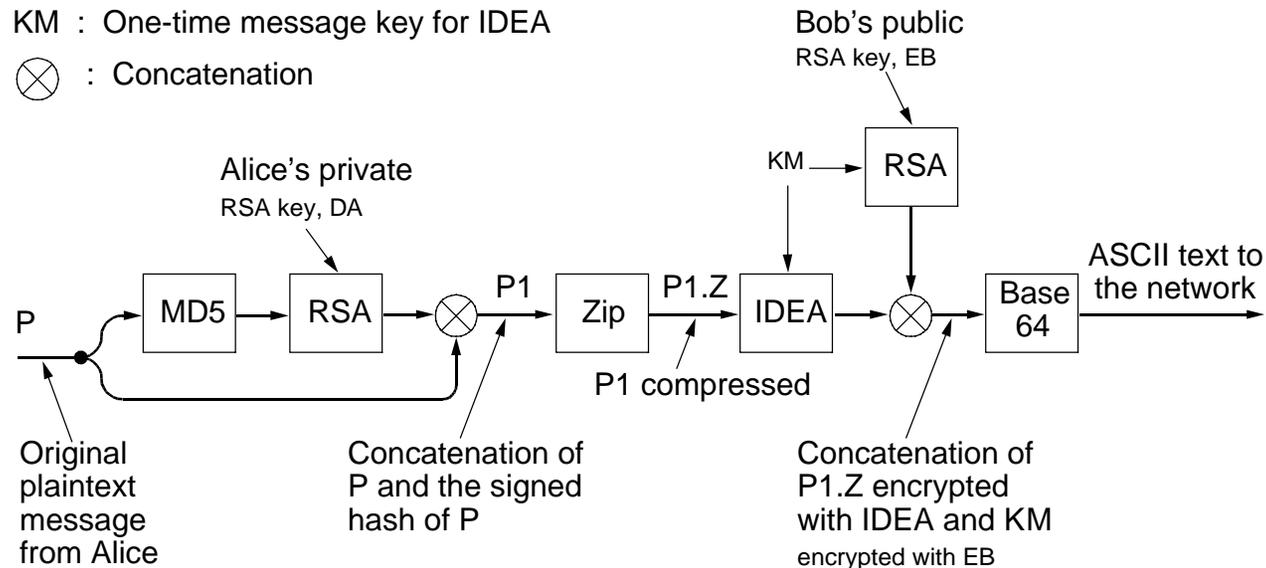
- SMTP Agents listen on TCP port 25
- Protocol consists of a series of 4 character commands
 - HELO: exchange identity
 - MAIL FROM: indicate origin of mail
 - RCPT TO: destination for mail
 - DATA: start of mail message (envelop and body)
 - QUIT: end of mail message
- Email gateways
 - Still many other mail systems out there
 - may use other formats
 - May want only a limited number of “public” mail servers
 - provides application level firewalls
 - hides interior topology of network

Pretty Good Privacy: PGP

- Developed by a single person
 - uses RSA, IDEA, and MD5
- Provides: privacy, compression, and digital signatures
- Has a collection of key servers for public key registration
- Uses three different key lengths (384, 512, and 1024 bits)

KM : One-time message key for IDEA

⊗ : Concatenation



From: *Computer Networks*, 3rd Ed. by Andrew S. Tanenbaum, (c)1996 Prentice Hall.

Privacy Enhanced Email (PEM)

- Internet Standard
- Uses MD5 for hashing and DES for encryption
- Key Management:
 - collection of certificate authorities
 - authorities are certified by Policy Certificate Authorities
 - define policies to be followed by certificate authorities
 - PCAs are certified by Internet Policy Registration Authority

News

- Large Collection of newsgroups
 - currently a hierarchical namespace (used to be rather flat)
 - can be moderated: must be approved before being posted
- Messages
 - have a unique id
 - are associated with one or more newsgroups
 - contain a superset of RFC822 fields
- Transport of news
 - a site a list of one or more sites it gets is newsfeed from
 - a site periodically polls its newsfeeds for news
 - newsfeeds can also push new news out
 - UUCP: Unix-to-Unix CoPy
 - historical path using dialup modems
 - NNTP: Net News Transfer Protocol (TCPport 119)