Email communication

Manish Kumar Arya

OUTLINE

- Background
- Mail system components
- Standards
- Mail communication decoded
- Decoding mail header
- Access your emails
- Security extensions
- Relevance of email communication
- Open source email software
- Further links
- Q&A

Manish Kumar Arya m@mka.in

BACKGROUND

- Electronic mail is there since early 90s in public domain
- Email is digital exchange of messages over internet/intranet
- Email RFCs for message transport (SMTP) and access (POP3, IMAP) were introduced in 80s

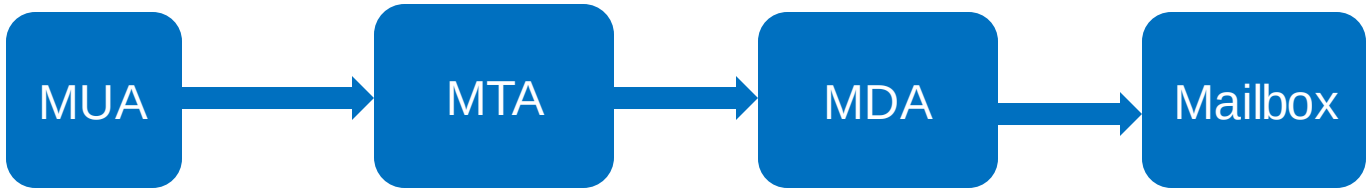
Manish Kumar Arya m@mka.in

EMAIL SYSTEM COMPONENTS

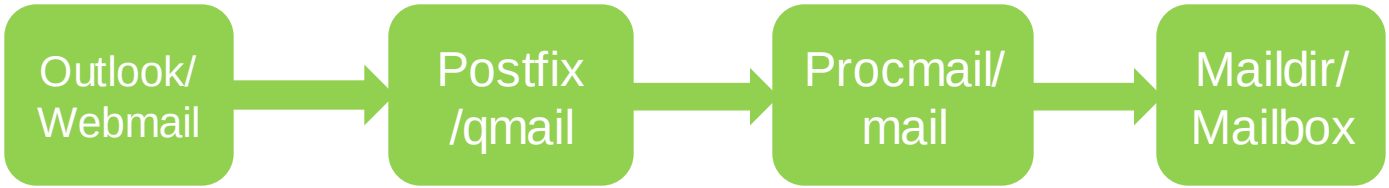
- Mail User Agent (thunderbird, webmail, outlook)
- Mail Transfer Agent (qmail, postfix, sendmail)
- Mail Delivery Agent (procmail, maildrop, bin/mail)

Manish Kumar Arya m@mka.in

FLOW DIAGRAM

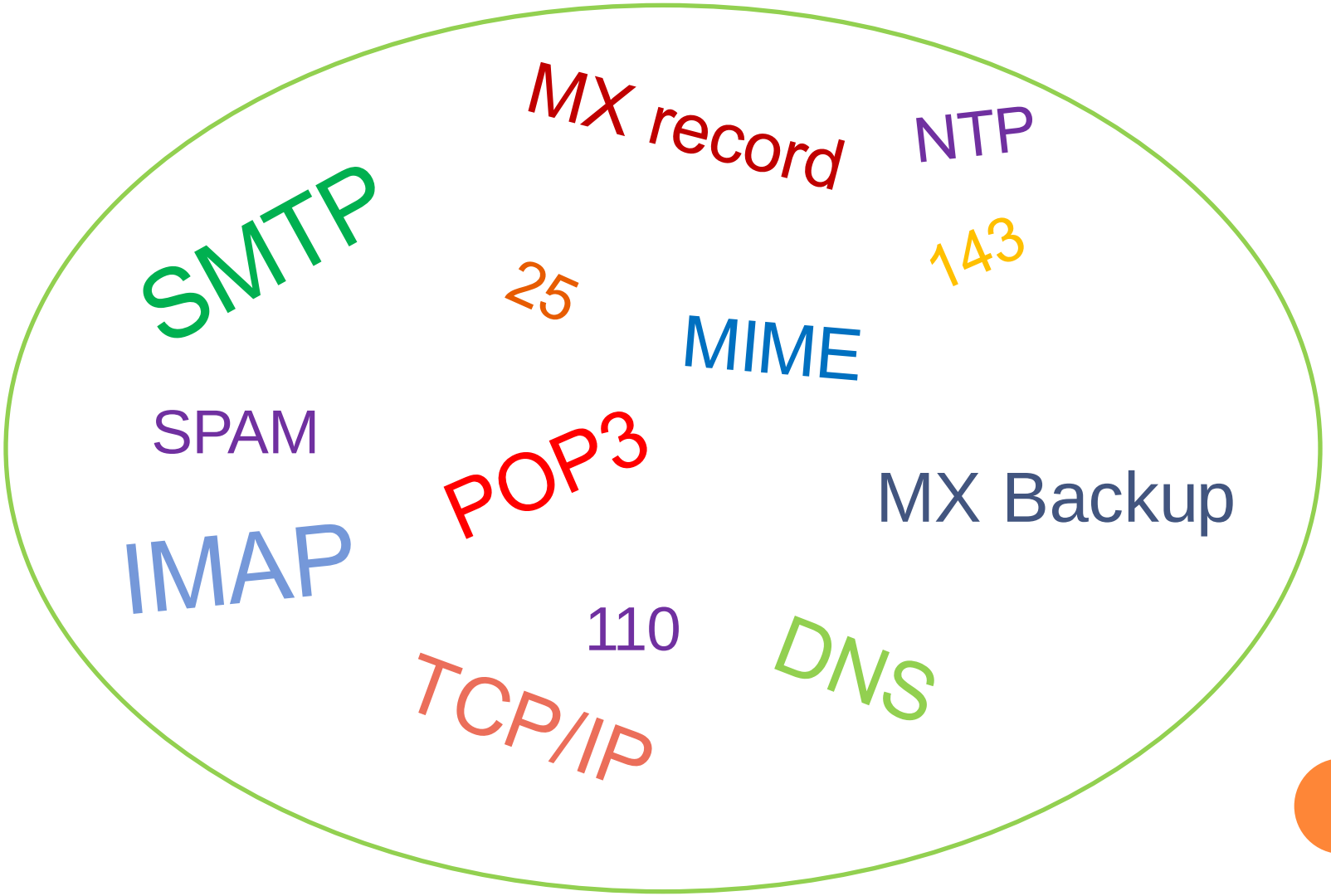


Mailbox access via
POP3 or IMAP MUA



Manish Kumar Arya m@mka.in

STANDARDS AND TERMS…



Manish Kumar Arya m@mka.in

SENDING A RAW EMAIL, HOW SMTP WORKS

```
telnet smtp1.xxx.xxx.xxx  25
Trying 10.5.2.11...
Connected to smtp1.xxx.xxx.xxx.
Escape character is '^]'.
220 ************************************
helo domain
250 smtp1.xxx.xxx.xxx.
mail from: test@test.com
250 Ok
rcpt to:m@mka.in
250 Ok
data
354 End data with <CR><LF>.<CR><LF>
Hello test message from test@test.com to m@mka.in
.
250 Ok: queued as 5C3F0362E8
quit
221 Bye
Connection to smtp1.xxx.xxx.xxx. closed by foreign host.
```

Manish Kumar Arya m@mka.in

What is happening at postfix mail server

manish@smtp1:~$ grep 5C3F0362E8 /var/log/maillog

Jan 27 07:29:41 smtp1.xxx.xxx.xxx postfix/smtpd[29332]: [ID 197553 mail.info]
5C3F0362E8: client=unknown[10.5.1.196]

Jan 27 07:30:05 smtp1.xxx.xxx.xxx postfix/cleanup[29111]: [ID 197553 mail.info]
5C3F0362E8: message-id=20140127072939.5C3F0362E8@smtp1.xxx.xxx.xxx

Jan 27 07:30:05 smtp1.xxx.xxx.xxx postfix/qmgr[28411]: [ID 197553 mail.info]
5C3F0362E8: from=<test@test.com>, size=385, nrcpt=1 (queue active)

Jan 27 07:30:10 smtp1.xxx.xxx.xxx postfix/smtp[24476]: [ID 197553 mail.info]
5C3F0362E8: to=<m@mka.in>, relay=aspmx.l.google.com[173.194.66.26],
delay=31, status=sent (250 2.0.0 OK 1390807810 td2si5835385wic.63 - gsmtp)

Jan 27 07:30:10 smtp1.xxx.xxx.xxx postfix/qmgr[28411]: [ID 197553 mail.info]
5C3F0362E8: removed

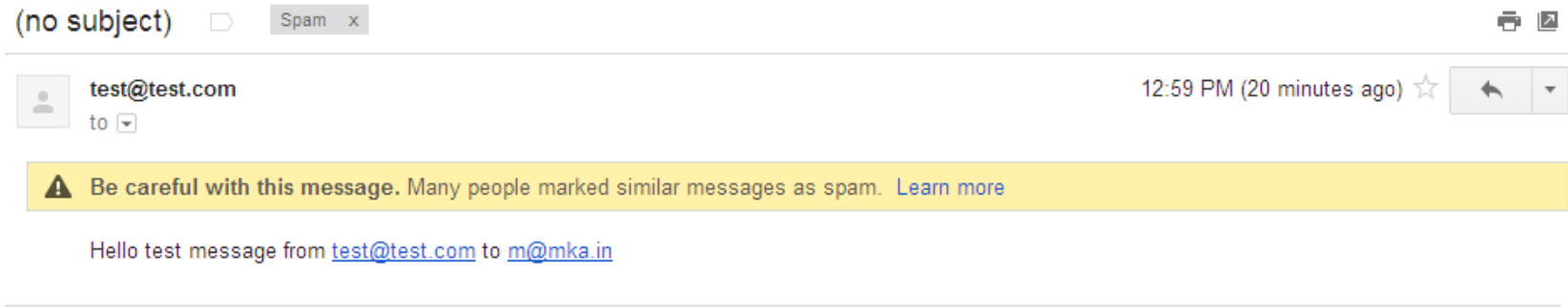
Manish Kumar Arya m@mka.in

How to finds recipient's mail server

```
manish@smtp1:~$ dig mx mka.in

; <<>> DiG 9.2.4 <<>> mx mka.in
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 228
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 4, ADDITIONAL: 0

;; QUESTION SECTION:
;mka.in.                        IN      MX

;; ANSWER SECTION:
mka.in.         1337    IN      MX      1 aspmx.l.google.com.
mka.in.         1337    IN      MX      5 alt1.aspmx.l.google.com.
mka.in.         1337    IN      MX      5 alt2.aspmx.l.google.com.
```

Manish Kumar Arya m@mka.in

DELIVERED !!



Manish Kumar Arya m@mka.in

DECODING EMAIL HEADER

Delivered-To: m@mka.in
Received: by 10.76.174.3 with SMTP id bo3csp96248oac;
Sun, 26 Jan 2014 23:30:11 -0800 (PST)
X-Received: by 10.194.173.163 with SMTP id bl3mr19045987wjc.10.1390807810934;
Sun, 26 Jan 2014 23:30:10 -0800 (PST)
Return-Path: <test@test.com>
Received: from smtp1.xxx.xxx.xxx (smtp1.xxx.xxx.xxx. [xxx.xxx.xxx.xxx])
by mx.google.com with ESMTP id td2si5835385wic.63.2014.01.26.23.30.10
for <m@mka.in>;
Sun, 26 Jan 2014 23:30:10 -0800 (PST)
Received-SPF: neutral (google.com: 212.74.77.125 is neither permitted nor denied by best guess record for domain of test@test.com) client-ip=xxx.xxx.xxx.xxx;
Authentication-Results: mx.google.com;
spf=neutral (google.com: xxx.xxx.xxx.xxx is neither permitted nor denied by best guess record for domain of test@test.com) smtp.mail=test@test.com
Received: from domain (unknown [10.5.1.196])
by smtp1.xxx.xxx.xxx (Postfix) with SMTP id 5C3F0362E8
for <m@mka.in>; Mon, 27 Jan 2014 07:29:39 +0000 (UTC)
Message-Id: <20140127072939.5C3F0362E8@smtp1.xxx.xxx.xxx>
Date: Mon, 27 Jan 2014 07:29:39 +0000 (UTC)
From: test@test.com
To: undisclosed-recipients:;

Hello test message from test@test.com to m@mka.in

Manish Kumar Arya m@mka.in

TYPICAL OUTLOOK MESSAGE HEADER

Received: from xxxxx.INTERNAL.xxx.xxxx ([fe80::d4ad:601a:c5a1:f60]) by xxxx.INTERNAL.xxx.xxx ([::1]) with mapi id 14.01.0355.002; Mon, 27 Jan 2014 08:33:51 +0000
Content-Type: application/ms-tnef; name="winmail.dat"
Content-Transfer-Encoding: binary
From: XX World <xxxx@xxxx.net>
To: xx xxx xxxxx <mka@xxxx.net>
Subject: test : test message
Thread-Topic: test : test message
Thread-Index: Ac8bOIVk2yVJvK1wScyba7CvMFd7GwAAfvBA
Date: Mon, 27 Jan 2014 08:32:34 +0000
Message-ID: <BDA212826FF5B94498C34C50A2A7D1956D371513@xxxxx.INTERNAL.xxxx.xxx>
Accept-Language: en-GB, en-US
Content-Language: en-US
X-MS-Has-Attach:
X-MS-Exchange-Organization-SCL: -1
X-MS-TNEF-Correlator:
<BDA212826FF5B94498C34C50A2A7D1956D371513@xxxx.INTERNAL.xxxx.xxx>
MIME-Version: 1.0
X-MS-Exchange-Organization-AuthSource: xxxxx.INTERNAL.xxxx.xxx
X-MS-Exchange-Organization-AuthAs: Internal
X-MS-Exchange-Organization-AuthMechanism: 03
X-Originating-IP: [10.100.42.4]
X-MS-Exchange-Organization-AVStamp-Mailbox: MSFTFF;1;0;0 0 0
X-Auto-Response-Suppress: DR, OOF, AutoReply

Why we need MX backup service?

- Primary MX is down or unreachable.
- Mail lands to MX backup server.
- MX backup attempts to deliver that email after certain intervals to primary MX server.
- MX backup retains emails till primary MX is up or maximum retention period expires.
- MX backup ensures that no mail is lost when primary MX is down.

Manish Kumar Arya m@mka.in

ACCESS EMAILS USING POP3 PROTOCOL

telnet pop3.xxx.xxx.xxx 110

USER m@mka.in

PASS xxxxxx

STAT
+OK 2 1445466

LIST
+OK 5 messages
1 1405
2 543
.
RETR msg#

TOP msg# #lines

DELE msg#

RSET
This resets (unmarks) any messages previously marked for deletion in this session so that the QUIT command will not delete them.

QUIT
This deletes any messages marked for deletion and then logs offs from pop3 server

Manish Kumar Arya m@mka.in

IMAP COMMANDS

Default port for IMAP is 143

LOGIN [username] [password]

LIST [flags] [folder separator] [search term]

STATUS [mailbox] [flags]

SELECT [mailbox]

FETCH [first]:[last] flags

FETCH [mail number] body[header]

FETCH [mail number] body[text]

LOGOUT

Manish Kumar Arya m@mka.in

SECURITY EXTENSIONS

- SMTP, IMAP and POP3 protocols are also available with SSL extensions
- These extensions ensure secure traffic on wire between two nodes
- Default port for SSL IMAP is 993
- Default port for SSL POP3 is 995
- Default port for SSL SMTP is 465 or 587
- IMAP SSL command line connection and commands can be found at http://delog.wordpress.com/2011/05/10/access-imap-server-from-the-command-line-using-openssl/

Manish Kumar Arya m@mka.in

SMTP AUTHORIZATION AND AUTHENTICATION

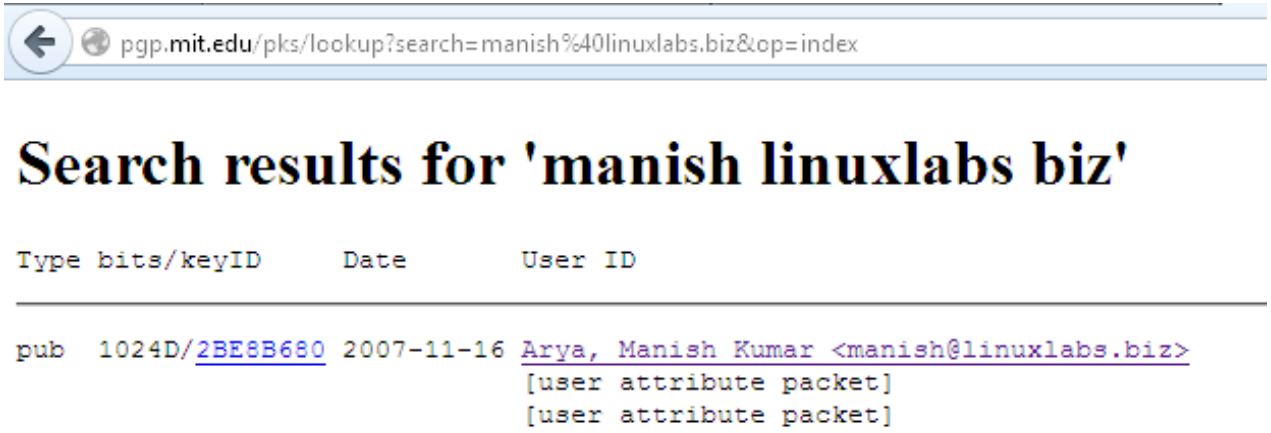
- Host and/or network authorization
- SMTP User authentication

```
manish@daffy ~ $ openssl s_client -connect smtp.gmail.com:465
220 mx.google.com ESMTP oa3sm37520675pbb.15 - gsmtp
HELO
250 mx.google.com at your service
auth login
334 VXNlcm5hbWU6
bWFuaNXoQDCpbnV4bGFicy5iaXo= (base64 encoded username)
334 UGFzc3dvcmQ6
JGdrCWZtWg== (base64 encoded password)
235 2.7.0 Accepted
```

Manish Kumar Arya m@mka.in

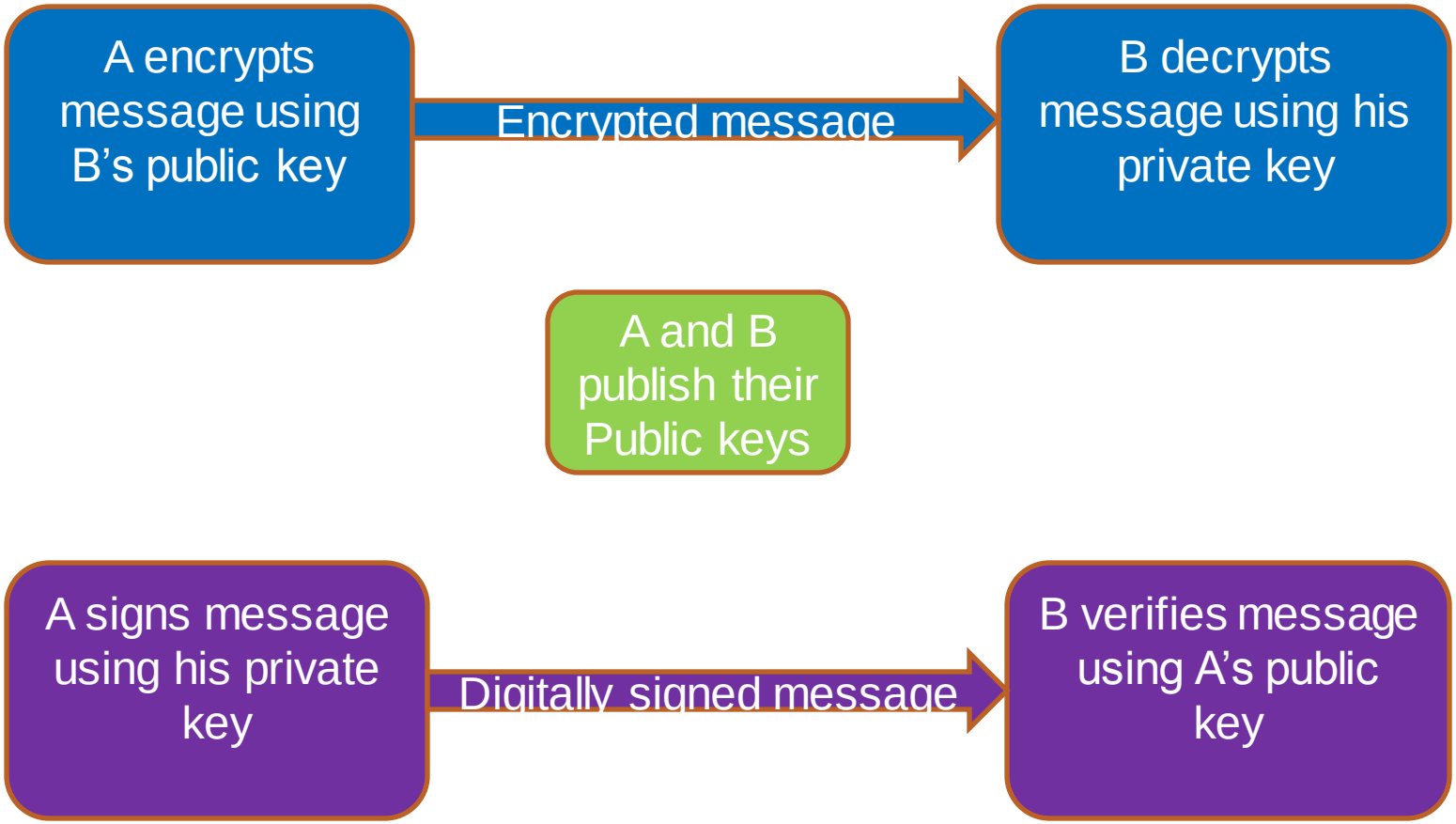
GPG AND PGP

- Gnu Privacy Guard
- Pretty Good Privacy
- Both are used to sign and/or encrypt emails
- GPG user guide
  http://www.gnupg.org/documentation/manuals/gnupg/
- Both GPG and PGP are based on PKI
- Public keys can be published on any public key server like
  http://pgp.mit.edu/



Manish Kumar Arya m@mka.in

SIGNING AND ENCRYPTION



Manish Kumar Arya m@mka.in

Relevance of email communication

Open for forum to discuss

Manish Kumar Arya m@mka.in

Open source Email software

- MTA Sendmail, postfix, qmail, exim
- MUA many webmail, evolution, mutt
- MDA procmail, maildrop

Manish Kumar Arya m@mka.in

Further links

- www.sf.net sourceforge for open source projects
- www.postfix.org
- www.qmail.org
- www.sendmail.com

Manish Kumar Arya m@mka.in

Questions

Manish Kumar Arya m@mka.in

Manish Kumar Arya m@mka.in