RIPEM 1.0:
A Beginning PEM Implementation

Mark Riordan

What Is RIPEM?
Features / Limitations
How To Use
Key Servers
Comparison with Internet PEM
Legal Issues
Platforms
How to Get RIPEM
RIPEM Future Possibilities

What Is RIPEM?

- Public key encryption program
- Based on RSAREF
- Resembles Internet PEM
- Free (non-commercial)

Features

- Keypair generation
- Encryption with DES-CBC & RSA
- Signature-only
- Mail header processing
- Key servers

Limitations

- Text only
- Message size limits
- Subset of PEM
- Not a mailer

How To Use

Command-line (God forbid)

ripem { -e | -d | -g | -c } <in >out
[-r recipient] [-u myusername]
[-m {encrypted | mic-only | mic-clear}]
[-h head] [-b #_of_bits_in_gen_key]
[-p publickey_infile] [-s privatekey_infile]
[-k key_to_private_key or -] [-T recip_opts]
[-P publickey_outfile] [-S privatekey_outfile]
[-y pub_key_server_name] [-Y key_sources]
[-i infile] [-o outfile]
[-D debug_level] [-Z debug_out_file]
[-R random_sources]
[-F random_input_file] [-C random_string]

Simple examples

ripem -e <mailmsg >mailmsg.enc

ripem -d <mailmsg.enc | more

Unix mail

`~e`

`pipe ripemd`

Mush

Single-keystroke macros

`D` = Decrypt

`R` = Decrypt & Reply

MH

Perl scripts

`send-ripem`

`display-ripem`

EMACS

EMACS functions

***`Esc`* `x ripem-encrypt`**

***`Esc`* `x ripem-receive`**

Key Servers

Key registration via Email

Create keypair via `ripem -g`

Mail result to

ripem-register-keys@ripem.msu.edu

FTP access to keyfile

ripem.msu.edu

Email access to keyfile

ripem-get-keys@ripem.msu.edu

UDP-based server

Changing keys

ripem-change-keys@ripem.msu.edu

ripem-remove-keys@ripem.msu.edu

Finger-based key exchange

Sample RIPEM ciphertext:

```
-----BEGIN PRIVACY-ENHANCED MESSAGE-----
Proc-Type: 2001,ENCRYPTED
DEK-Info: DES-CBC,EACFF9372889C60E
Originator-Name: mrr@scss3.cl.msu.edu
Originator-Key-Asymmetric:
  MFkwCgYEVQgBAQICAgYDSwAwSAJBMpWXPx/qTRUUKhwu ...
  j5A7IZgAeHQGuqmPMqbC6gxZl32xCJ488Mc/MHgRxkZ0 ...
MIC-Info: RSA-MD5,RSA,
  GmcGWixvwsmug5vQJjNPk4LhUimjhN2+PgNfjnAl7x5t ...
  6becx6YIxc+FNiRfULv8zjwVKYrbCh7Z
Recipient-Name: test
Key-Info: RSA,
  BCpKbRDqgKG4DA/6IxmmN2TXqPG2y88zRD+p4IY4sqs9 ...
  zl1q7/uV5BIn2A25GPCXou8=

FD1DW/TmJlW3V1i7tO3lzarAKKWoRI/AEVbRS7yN/EM=
-----END PRIVACY-ENHANCED MESSAGE-----
```

Internet PEM

Originator-Certificate:

Issuer-Certificate:

Recipient-ID-Asymmetric:

plus

Originator-ID-Symmetric:

Recipient-ID-Symmetric:

Proc-Type: **(2001)**

DEK-Info:

MIC-Info:

Key-Info:

Recipient-Name:

Originator-Name:

Originator-Key-Asymmetric:

RIPEM

Legal Issues

RIPEM is public-domain
But RSAREF isn't
Free for non-commercial use
No export

Platforms

Unix:

NeXTStep
SunOS 4.x
Solaris 2.x
IBM AIX (RS/6000, 370, 386)
HP/UX
DEC ULTRIX
Motorola System 88
SCO ODT
386BSD
Linux

MS-DOS: 8086 & 80386
OS/2 2.x
Macintosh

How to Get RIPEM

Anonymous FTP

rsa.com & others

Non-Anonymous FTP

ripem.msu.edu

See me afterward for diskettes

RIPEM Future Possibilities

Better local key management
Improved Mac version
Compression
Binary files
Support of Certificates
IDEA, Double-DES