

## Email Security Protocols:

### PEM & S/MIME

- **PEM** (Privacy Enhanced Mail):  
Add encryption, authentication and integrity to ordinary *text* messages.
- **MIME** (Multipurpose Internet Mail Extensions):  
Is a standard for encoding *arbitrary data* in email (images, video, etc.).
- **S/MIME**:  
Incorporated many principles of PEM into MIME.

### Structure of a PEM Message

PEM marks its pieces with a *text string* before and after the piece as:

```
-----BEGIN PRIVACY ENHANCED MESSAGE-----
```

```
.....<data>....
```

```
-----END PRIVACY ENHANCED MESSAGE-----
```

The different types of pieces PEM can combine into a message are:

1. Ordinary, unsecured data.
2. Integrity-protected unmodified data (**MIC-CLEAR**).
3. Integrity-protected encoded data (**MIC-ONLY**).
4. Encoded encrypted integrity-protected data (**ENCRYPTED**).

Not only these types of data be combined in a message, but they can be *nested* inside one another.

E.g., Alice might enclose **MIC-CLEAR** message from Fred in an **ENCRYPTED message** to Bob.

### Example:

**From:** Alice  
**To:** Bob  
**Subject:** Colloquium  
**Date:** Mon Oct 7, 2008

Dear Bob:  
I would like to invite you to give a colloquium next Spring at ODU,  
if you accept, let us talk about the details.  
Alice

The above message may be sent in one following 3 forms:

### 1. MIC-CLEAR

**From:** Alice  
**To:** Bob  
**Subject:** Colloquium  
**Date:** Mon Oct 7, 2008

```
-----BEGIN PRIVACY ENHANCED MESSAGE-----  
Proc-Type: 4, MIC-CLEAR  
Content-Type: RFC822  
Originator-ID-Asymmetric: <certificate ID>  
MIC-Info: RSA-MD5, RSA, <encoded MIC>
```

Dear Bob:  
I would like to invite you to give a colloquium next Spring at ODU,  
if you accept, let us talk about the details.  
Alice

```
-----END PRIVACY ENHANCED MESSAGE-----
```

### 2. MIC-ONLY

**From:** Alice  
**To:** Bob  
**Subject:** Colloquium  
**Date:** Mon Oct 7, 2008

```
-----BEGIN PRIVACY ENHANCED MESSAGE-----  
Proc-Type: 4, MIC-ONLY  
Content-Type: RFC822  
Originator-ID-Asymmetric: <certificate ID>  
MIC-Info: RSA-MD5, RSA, <encoded MIC>
```

<encoded message>

-----END PRIVACY ENHANCED MESSAGE-----

### 3. ENCRYPTED

**From:** Alice  
**To:** Bob  
**Subject:** Colloquium  
**Date:** Mon Oct 7, 2008

-----BEGIN PRIVACY ENHANCED MESSAGE-----

Proc-Type: 4, ENCRYPTED  
Content-Type: RFC822  
DEK-Info: DES-CBC, IV  
Originator-ID-Asymmetric: <Originator certificate ID>  
Key-Info: RSA, <encoded message key encrypted with *originator* public key>  
MIC-Info: RSA-MD5, RSA, <encoded *encrypted* MIC>  
Recipient-ID-Asymmetric: <Recipient certificate ID>  
Key-Info: RSA, <encoded message key encrypted with *recipient* public key>

<encoded encrypted message using DES-CBC>

-----END PRIVACY ENHANCED MESSAGE-----

- Why we send the message key to *originator*?  
For CC purposes and if message is returned to sender due to some error.
- Why MIC is *encrypted*?  
Using the public-key of the Originator, a person can compute the message digest MD.  
Then he can use the MD to check his guess for the message e.g., **attack** or **retreat**.
- How to send an ENCRYPTED message to *multiple recipients*?  
Encrypt the message key once for each recipient:

Recipient-ID-Asymmetric: <Recipient-1 certificate ID>  
Key-Info: RSA, <encoded message key encrypted with *recipient-1* public key>

Recipient-ID-Asymmetric: <Recipient-2 certificate ID>  
Key-Info: RSA, <encoded message key encrypted with *recipient-2* public key>

key>

.....

**Recipient-ID-Asymmetric:** <Recipient-n certificate ID>

**Key-Info:** RSA, <encoded message key encrypted with *recipient-n* public key>

### **PEM Encoding:**

It is base-64 encoding, i.e., each 6 bits is encoded as 8-bit character in the set {**A-Z,a-z,0-9,+/,**}

When PEM sees a line that begins with **-** it is replaced with **-|**.

Thus the string in the text:

-----END PRIVACY ENHANCED MESSAGE-----

would appear as:

-|-----END PRIVACY ENHANCED MESSAGE-----

### **Forwarding & Enclosure:**

Only MIC-CLEAR and MIC-ONLY messages can be forwarded.

For ENCRYPTED messages, it must be **decrypted** and then **re-encrypted**.

### **Unprotected Information:**

**From:** Alice

**To:** Bob

**Subject:** Colloquium

**Date:** Mon Oct 7, 2008

To protect the **header** information, it should be included in the text.

### **Secret Key Variant:**

PEM can be used for both **public-key** and **secret-key** infrastructure.

A secret key between Alice and Bob can be established using

out-of-band mechanism (e.g., phone, Kerberos).  
There is no much interest in secret key based PEM.

### **Differences in S/MIME:**

**S/MIME is very similar to PEM.**

**One difference is:**

**boundary=----boundary marker**

**----boundary marker**

**...<Content>...**

**----boundary marker**