

The NPTEL logo is a circular emblem. It features a stylized flower or star shape in the center, composed of several overlapping loops in shades of pink and orange. Surrounding this central motif is a ring made of many small, rectangular segments, some of which are colored in a gradient from orange to pink. The entire logo is rendered in a light, semi-transparent style.

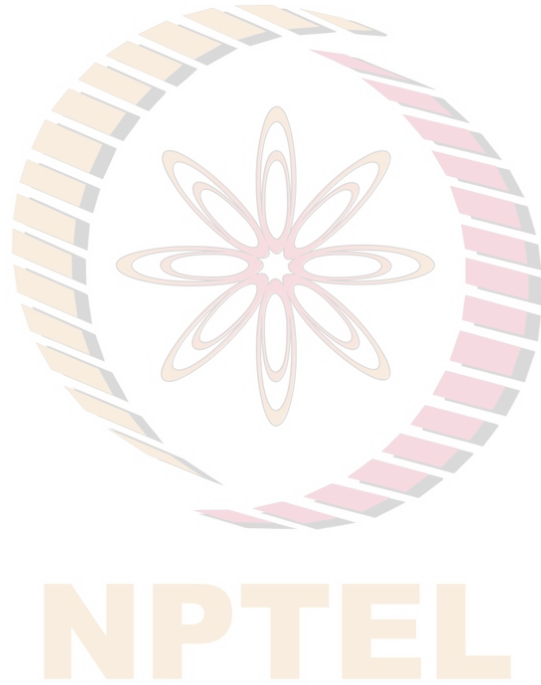
Email Security

Dr. Neminath Hubballi

NPTEL

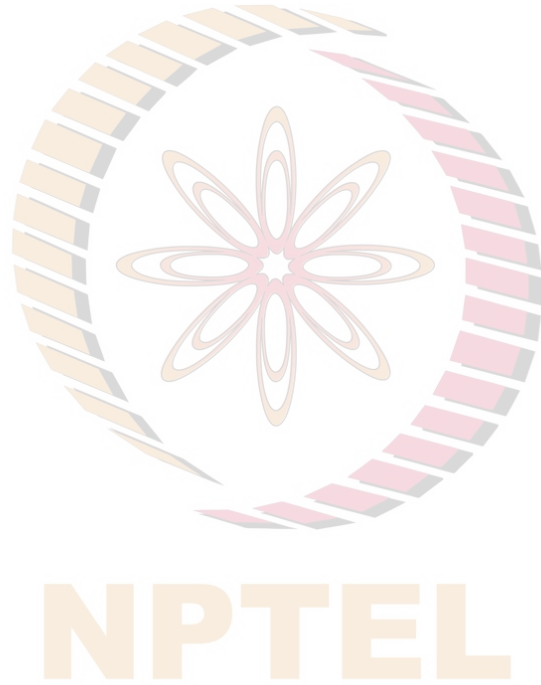
Overview

- ☐ Security Requirements
- ☐ S/MIME
- ☐ DKIM

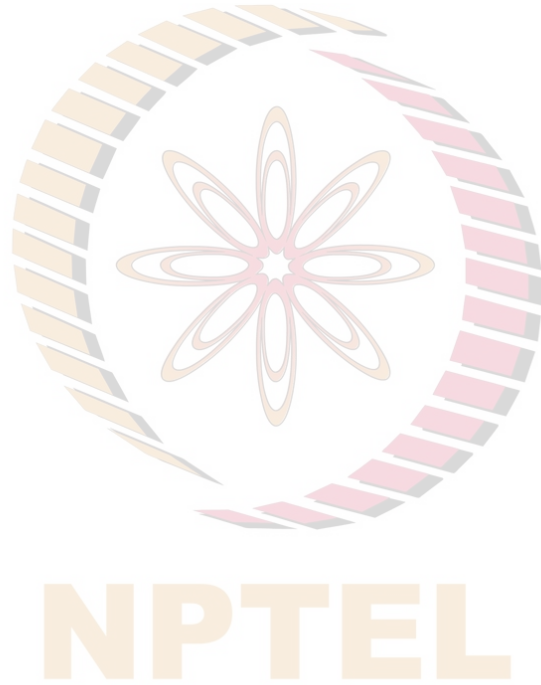


Security Requirements

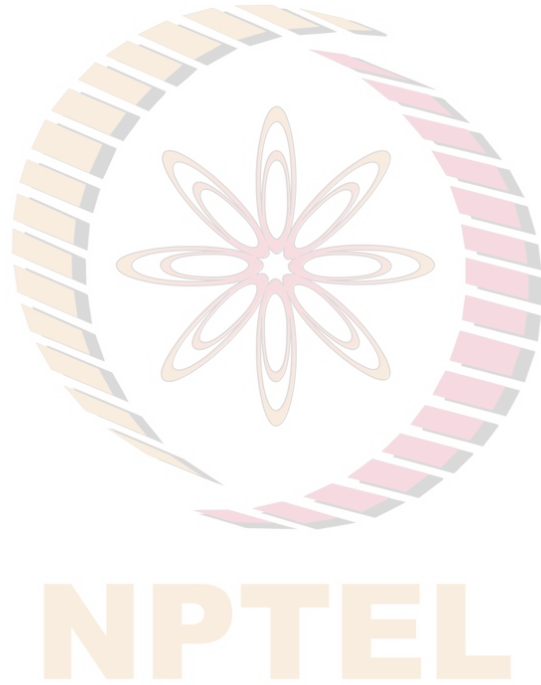
- ☐ Confidentiality of Data
- ☐ Integrity of the Data
- ☐ Authenticity of the Data



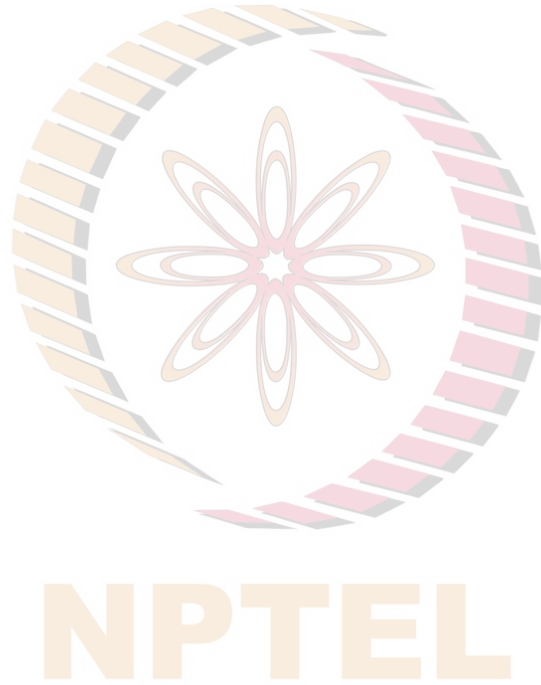
Basics of Cryptography



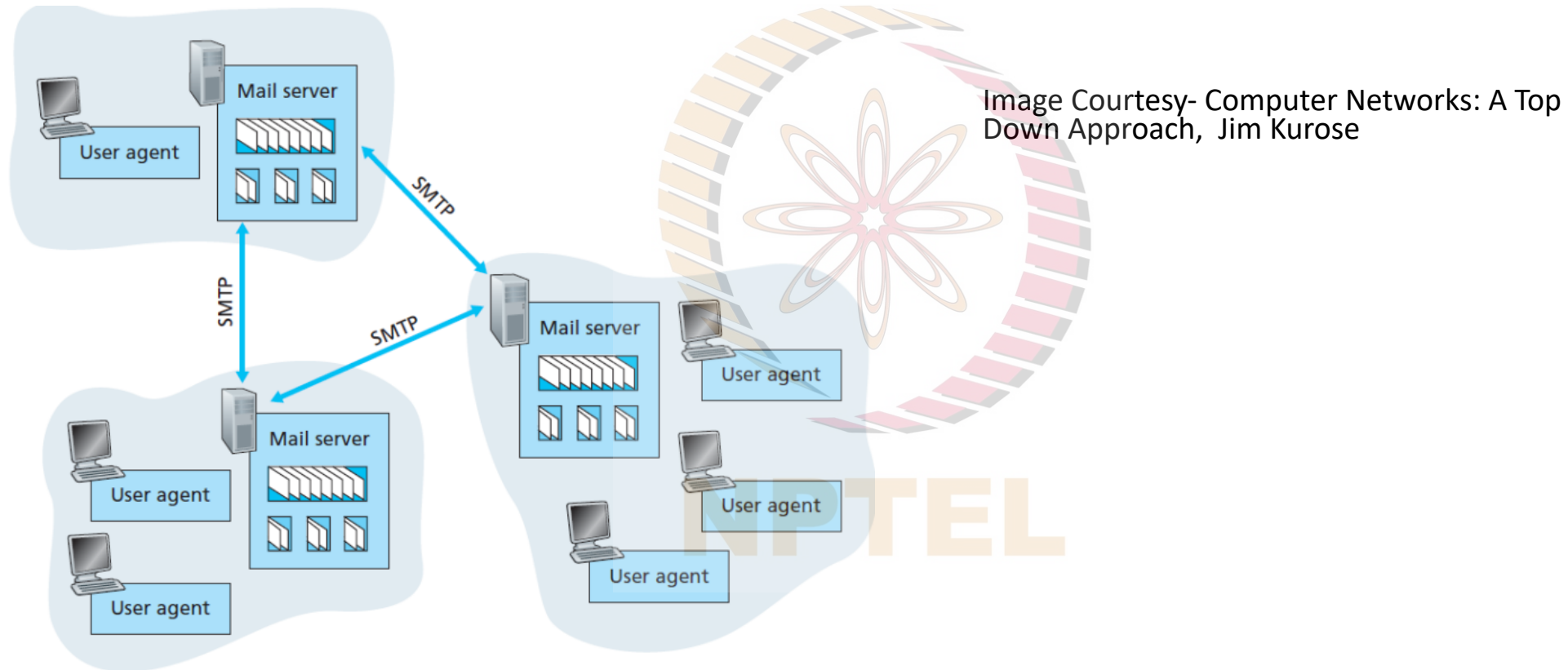
Basics of Cryptography



Basics of Cryptography



How Mails are Sent and Delivered ?



Email Structure

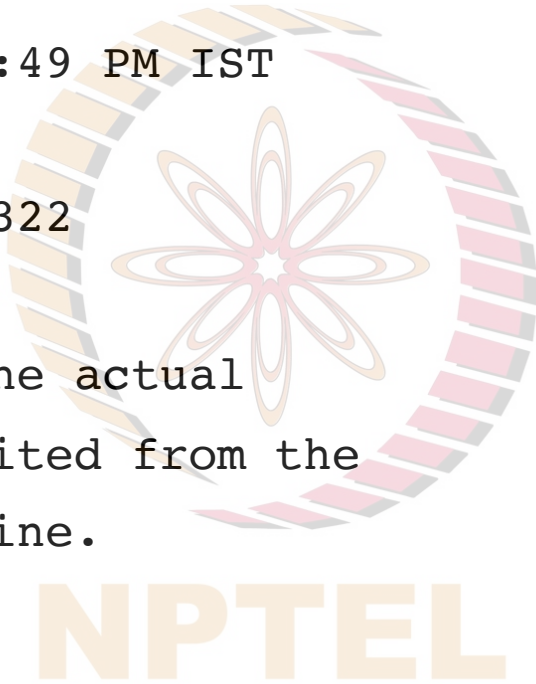
Date: December 21, 2021 2:15:49 PM IST

From: xyz <xyz@gmail.com>

Subject: The Syntax in RFC 5322

To: pqr@outlook.com

Hello. This section begins the actual message body, which is delimited from the message heading by a blank line.



Simple Mail Transfer Protocol

- ☐ Can't transmit executable files
- ☐ Emails now exchange
 - ☐ Image
 - ☐ Video
 - ☐ Audio
 - ☐ Non English text
 - ☐ Files of various types
 - ☐ Non ASCII text
- ☐ Mails of size beyond a limit



Multipurpose Internet Mail Extensions (MIME)

- ☐ Defines five new header fields to be added to email
- ☐ Adds many content types
- ☐ Defines transform encoding



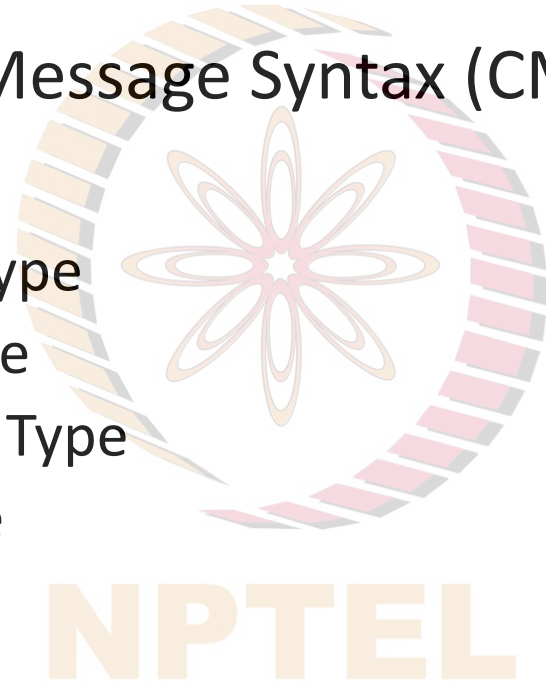
S/MIME Origin

- ☐ Verifying the senders identity
- ☐ Preventing Man-in-the-Middle attacks
- ☐ Message integrity verification

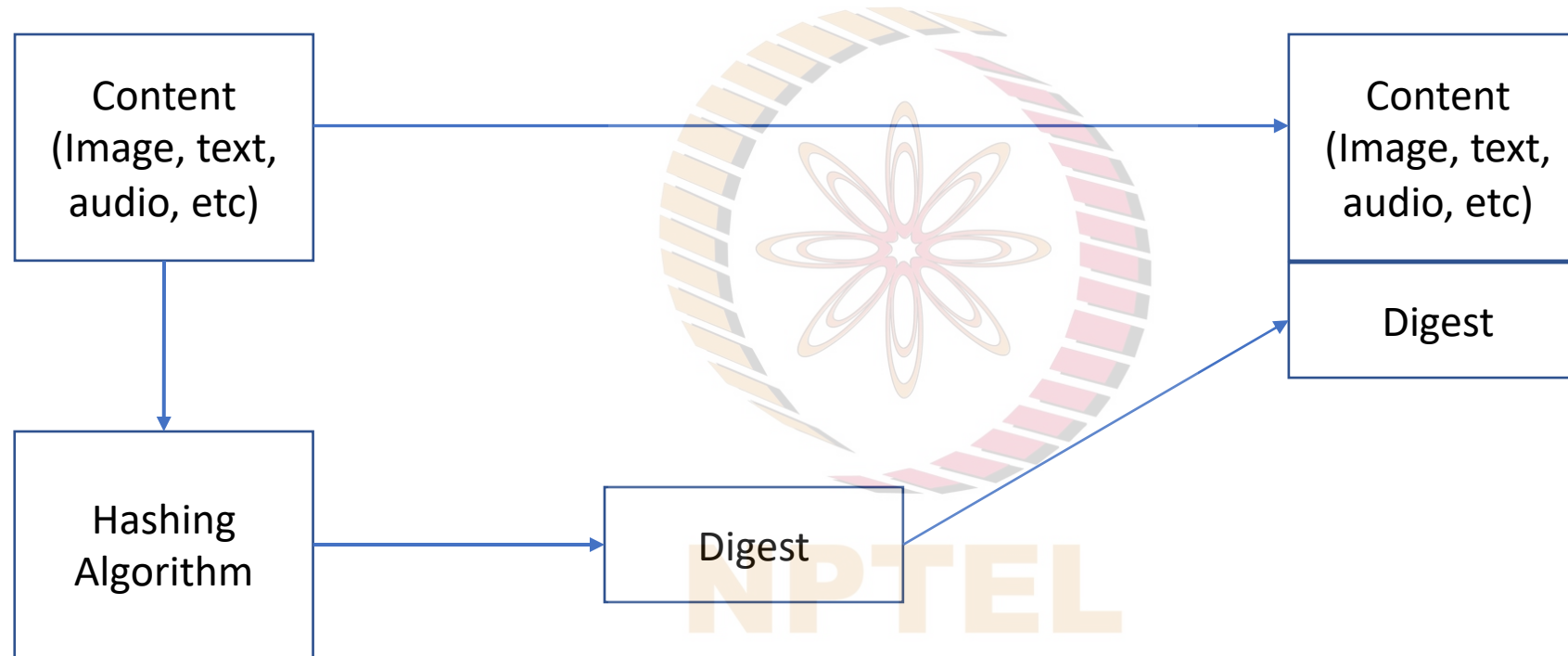


S/MIME Security

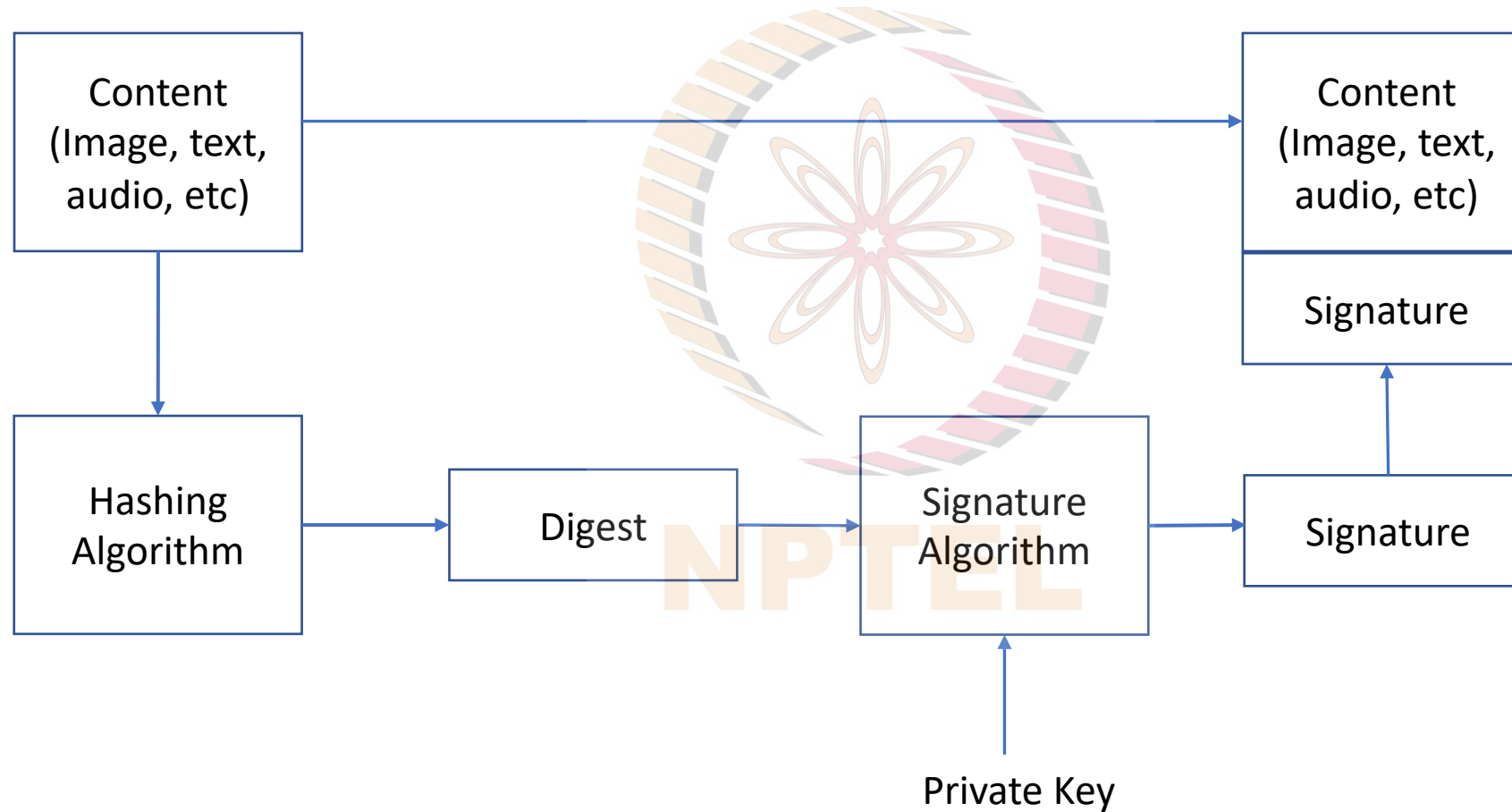
- ☐ Defines Cryptographic Message Syntax (CMS)
- ☐ Different Data Types
 - ☐ Digested Data Content Type
 - ☐ Signed Data Content Type
 - ☐ Enveloped Data Content Type
 - ☐ Authenticated Data Type



Digested Data Content Type



Signed Data Content Type



Signed Data Content Type

Content-Type: `application/pkcs7-mime; smime-type=signeddata;
name=smime.p7m`

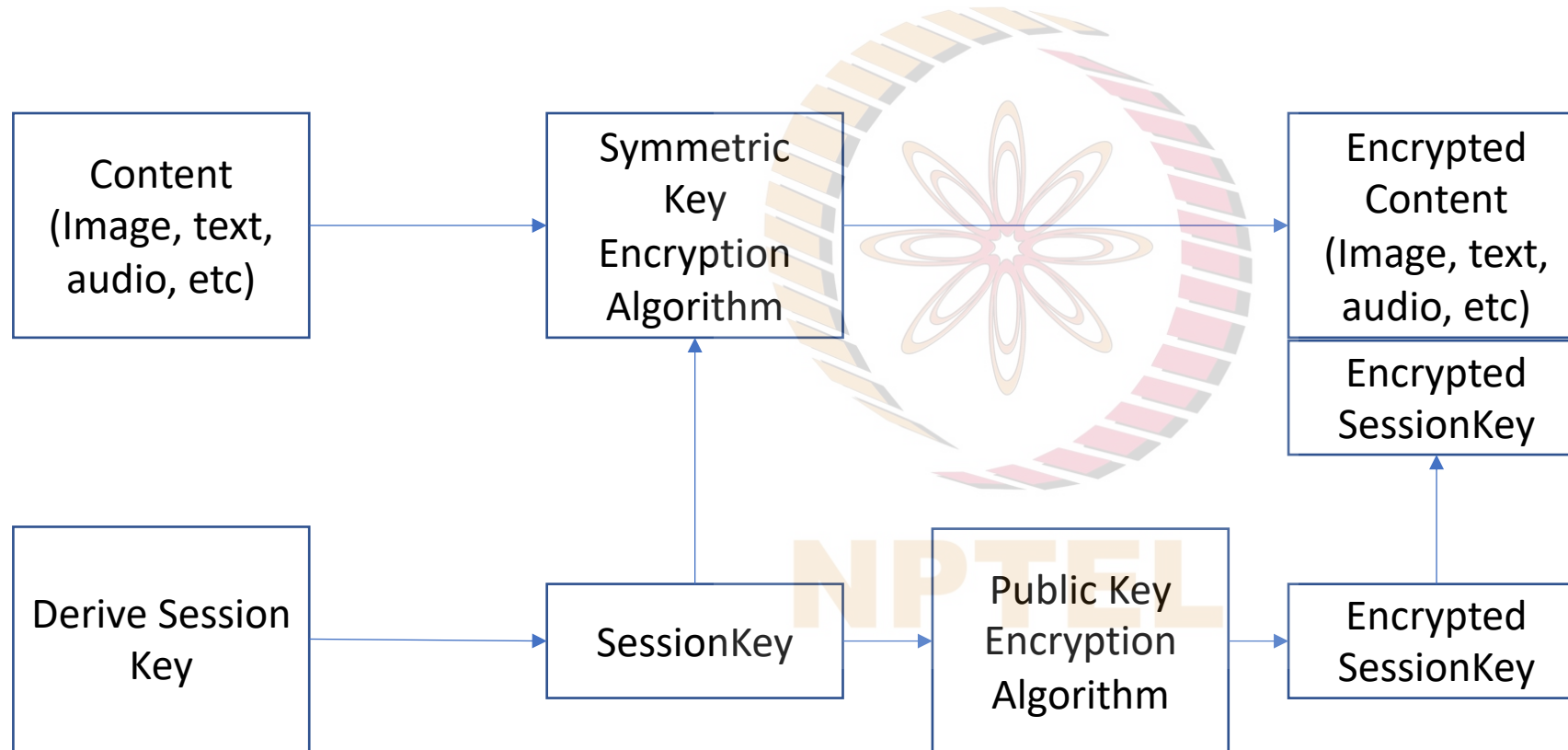
Content-Transfer-Encoding: `base64`

Content-Disposition: `attachment; filename=smime.p7m`

`567GhIGfHfYT6ghyHhHUujpfyF4f8HHGTrfvhJhjH776tbB9HG4VQbnj7
77n8HHGT9HG4VQpfyF467GhIGfHfYT6rfvbnj756tbBgHyHhHUujhJhjH
HUujhJh4VQpfyF467GhIGfHfYGTrfvbnjT6jH7756tbB9H7n8HHGghyHh
6YT64V0GhIGfHfQbnj75`

NPTTEL

Enveloped Data Content Type



Enveloped Data Content Type

Content-Type: **application/pkcs7-mime; smime-type=envelopeddata;**
name=smime.p7m

Content-Transfer-Encoding: base64

Content-Disposition: attachment; filename=smime.p7m

rfvbnj756tbBghyHhHUujhJhjH77n8HHGT9HG4VQpfyF467GhIGfHfYT6
7n8HHGghyHhHUujhJh4VQpfyF467GhIGfHfYGTTrfvbnjT6jH7756tbB9H
f8HHGTTrfvhJhjH776tbB9HG4VQbnj7567GhIGfHfYT6ghyHhHUujpfyF4
0GhIGfHfQbnj756YT64V

NPTTEL

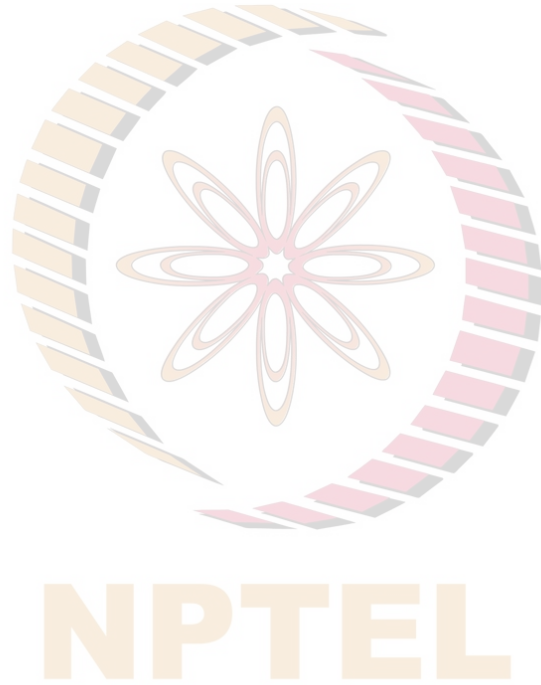
S/MIME Limitation

- ☐ Usability issues
 - ☐ Very few people understand the cryptography
- ☐ Receiver nonrepudiation
- ☐ Sending encrypted and signed mails to multiple receivers is complex
- ☐ Email header protection is missing (up to ver 3.0)
- ☐ Use of bogus name in sender's name

DomainKeys Identified Mail (DKIM)

- ☐ It is a standard that help protect recipient from
 - ☐ Spam
 - ☐ Phishing
- ☐ Authenticity of the mail can be verified by the recipient
- ☐ Uses public key cryptography
- ☐ **Idea:** Attach a digital signature to a domain name with each outgoing email from that domain

DomainKeys Identified Mail (DKIM)



DomainKeys Identified Mail (DKIM)

Dkim Signature:

v=1; a=rsa-sha256; c=relaxed/relaxed; d=truckpages.co.uk; s=default; t=1582021898;
bh=47DEQpj8HBSa+/TImW+5JCeuQeRkm5NMpJWZG3hSuFU=; l=0; h=From:Subject:To;
b=MPFUuibC74qh+qpzlligznS8MsPZpUMSAFjaYAP7IQUUVG5Ky4qBBk8NS4qYagh5i
aHaVjjReSbnosa8RDB/4z474by89mEJuGwoBZGDr33QxSddZjyws476o8c5q7UuLDI
XDylAoAs3VRp3PgDwBUFsYRI0GTAHyi3c8V/2SgA=

v-version

a-algorithm

c-canonicalization

d-domain

h-headers included in the hash sum

s-selector: which public key to use

bh-hash of the canonicalized body

b-signature of the data



Absence of DKIM Signature-Implications

- ☐ Absence of a DKIM signature
 - ☐ Many organizations do not use it
- ☐ A compromised machine within the sender's domain can send large number of spam messages
- ☐ Spammer can setup a fake domain and sign all the emails

NPTEL