Web Security

Email security

How Mails are Sent and Delivered ?

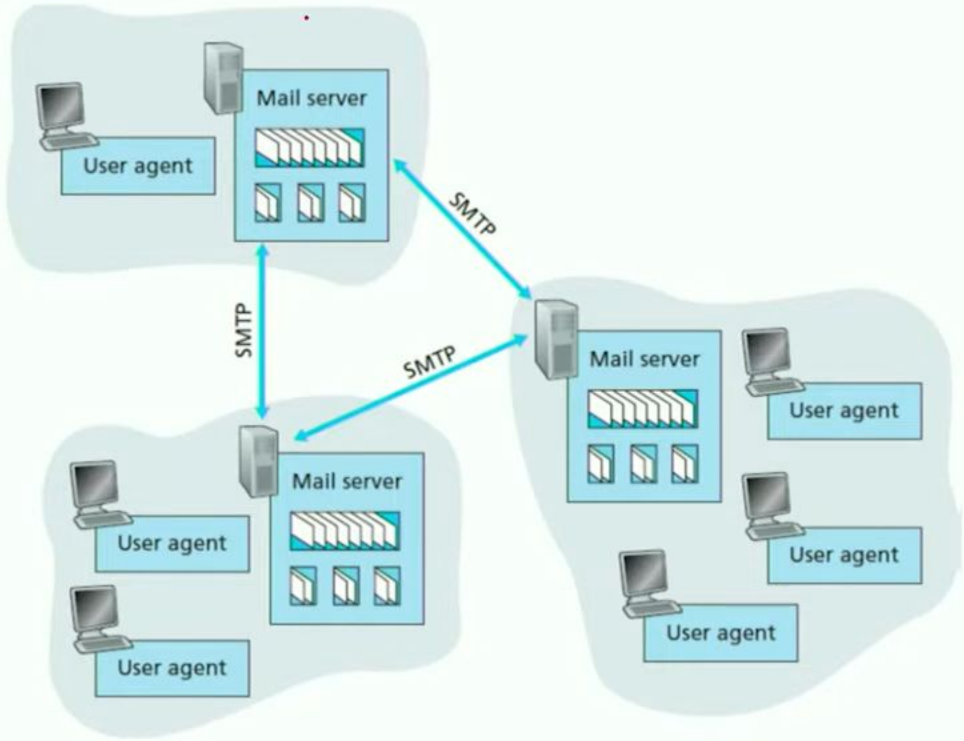
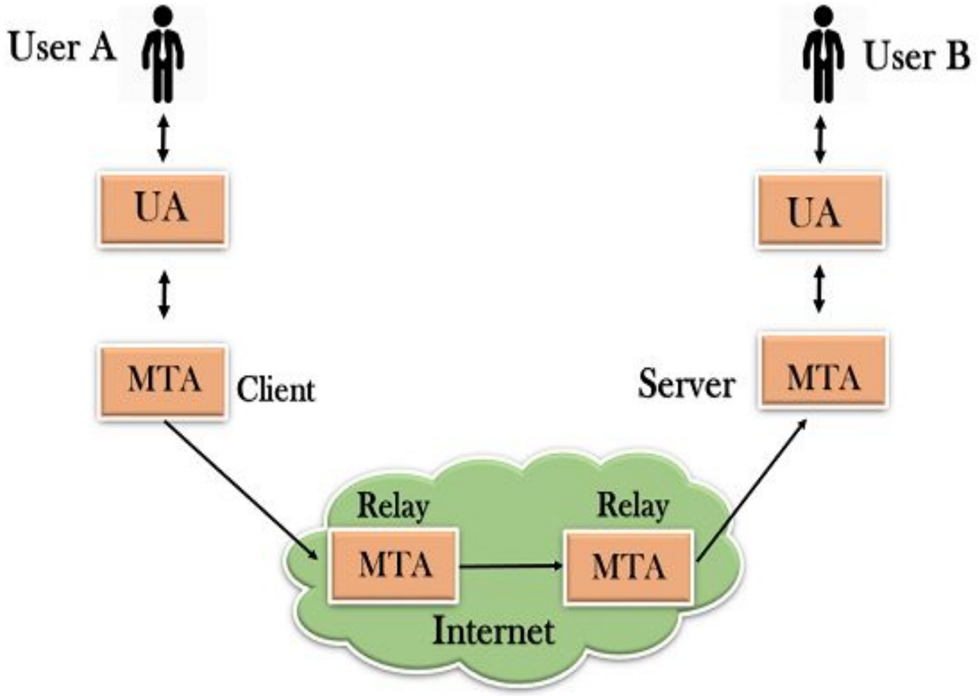


Image Courtesy- Computer Networks: A Top Down Approach, Jim Kurose

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.
```

Components of SMTP



Working of SMTP

Break the SMTP client and SMTP server into two components as :

user agent **(UA)** and mail transfer agent **(MTA).**

- The user agent (UA) prepares the message, creates the envelope and then puts the message in the envelope.
- The mail transfer agent (MTA) transfers this mail across the internet.

- The relaying system without TCP/IP protocol can also be used to send the emails to users, and this is achieved by the use of the mail gateway. The mail gateway is a relay MTA that can be used to receive an email.

Working of SMTP

1. **Composition of Mail:**

2. **Submission of Mail:** After composing an email, the mail client then submits the completed e-mail to the SMTP server by using SMTP on TCP port 25.
3. **Delivery of Mail:** E-mail addresses contain two parts: username of the recipient and domain name. For example, abc123@gmail.com, where “abc123" is the username of the recipient and "gmail.com" is the domain name.

If the domain name of the recipient's email address is different from the sender's domain name, then MSA will send the mail to the Mail Transfer Agent (MTA).

To relay the email, the MTA will find the target domain. It checks the MX record from Domain Name System to obtain the target domain.

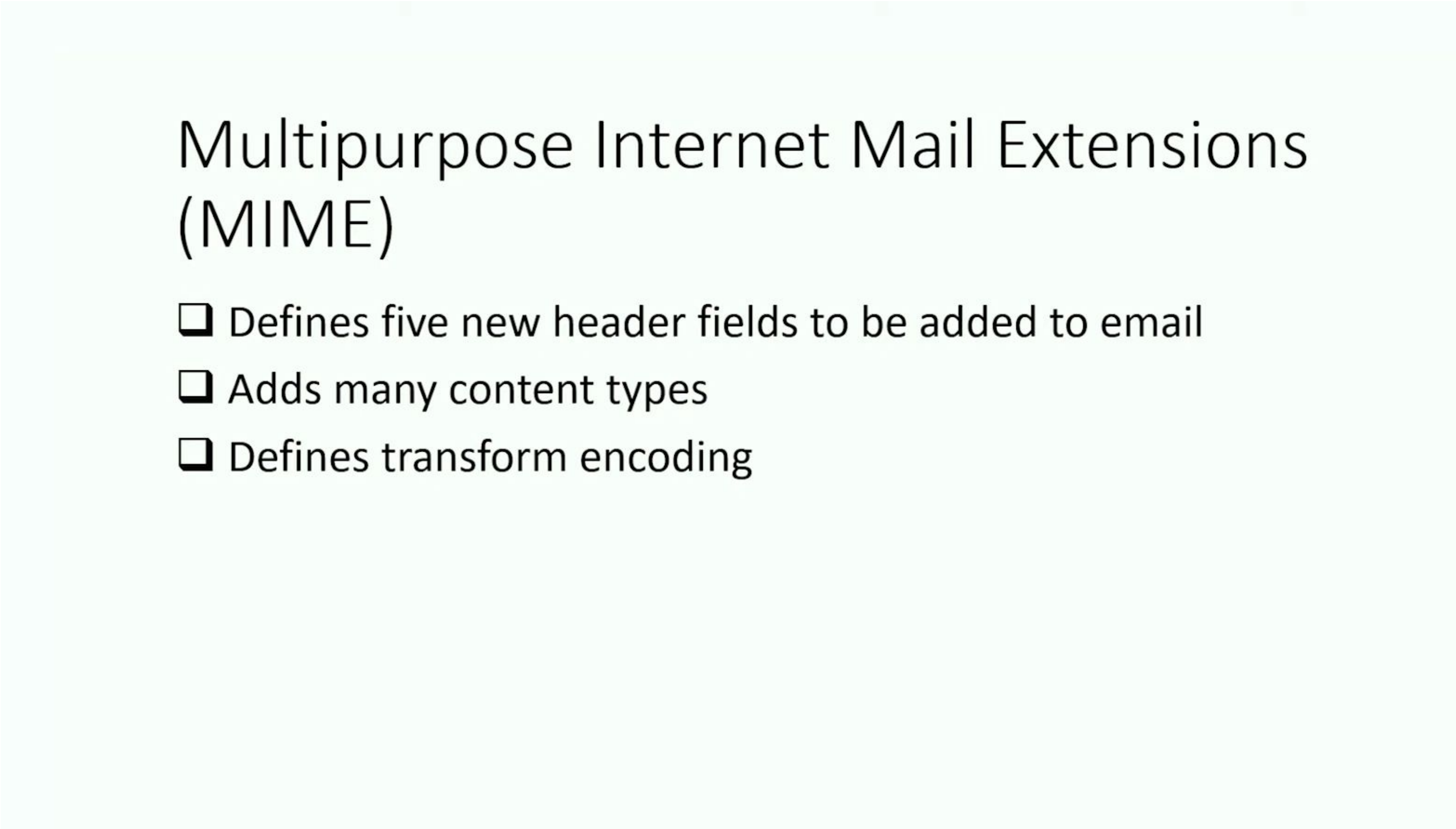
The MX record contains the domain name and IP address of the recipient's domain. Once the record is located, MTA connects to the exchange server to relay the message.

4. Receipt and Processing of Mail: Once the incoming message is received, the exchange server delivers it to the incoming server (Mail Delivery Agent) which stores the e-mail where it waits for the user to retrieve it.

5. Access and Retrieval of Mail: The stored email in MDA can be retrieved by using MUA (Mail User Agent). MUA can be accessed by using login and password.

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

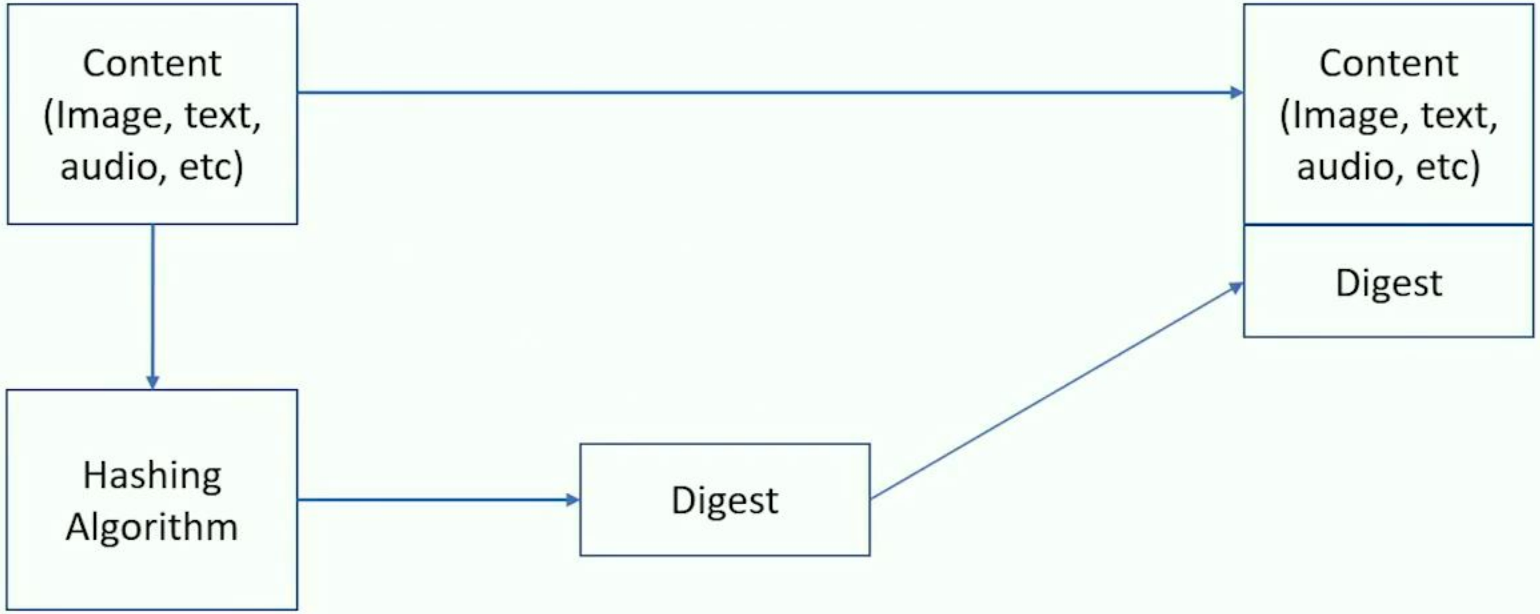
❑ Preventing Man-in-the-Middle attacks

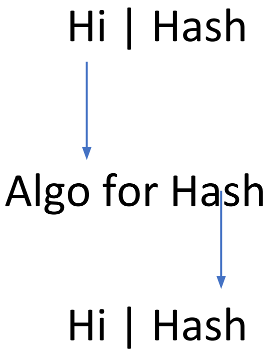
❑ Message integrity verification

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


Content (Image, text, audio, etc)
Hashing Algorithm
Digest
Content (Image, text, audio, etc)
Digest

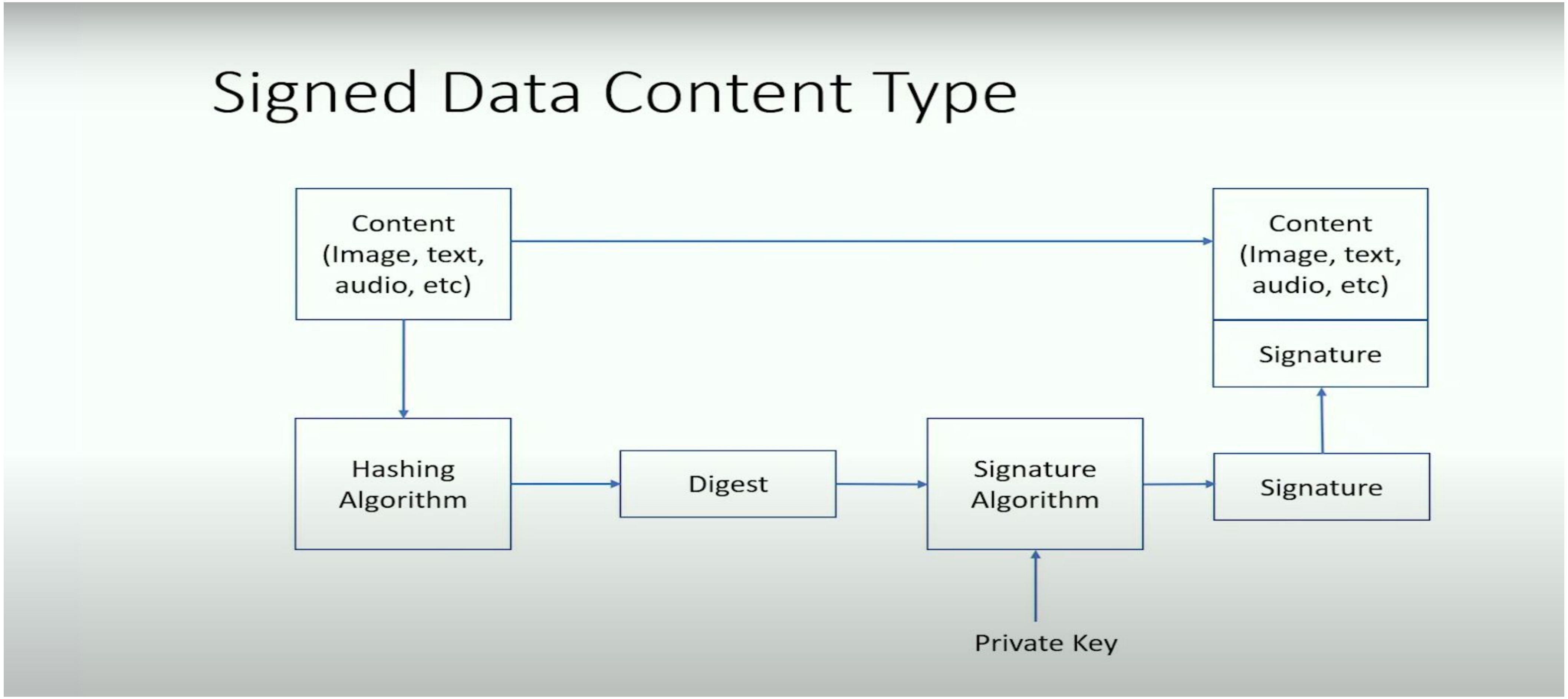


Hi | Hash

Algo for Hash

Hi | Hash

Matches



Signed Data Content Type

Content (Image, text, audio, etc)

Hashing Algorithm

Digest

Signature Algorithm

Private Key

Signature

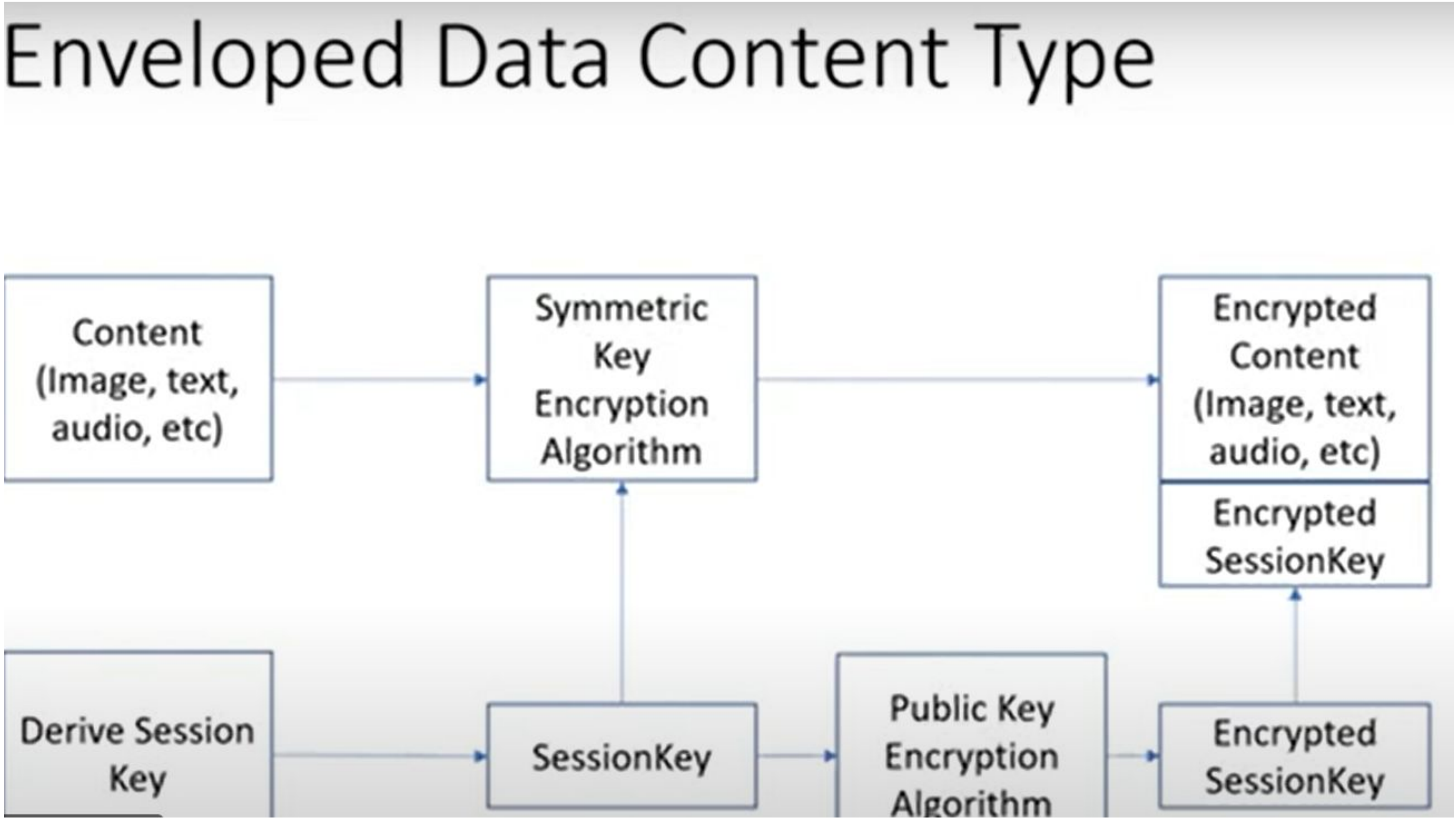
Content (Image, text, audio, etc)

Signature

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



Enveloped Data Content Type

Content (Image, text, audio, etc)

Symmetric Key Encryption Algorithm

Encrypted Content (Image, text, audio, etc)

Encrypted SessionKey

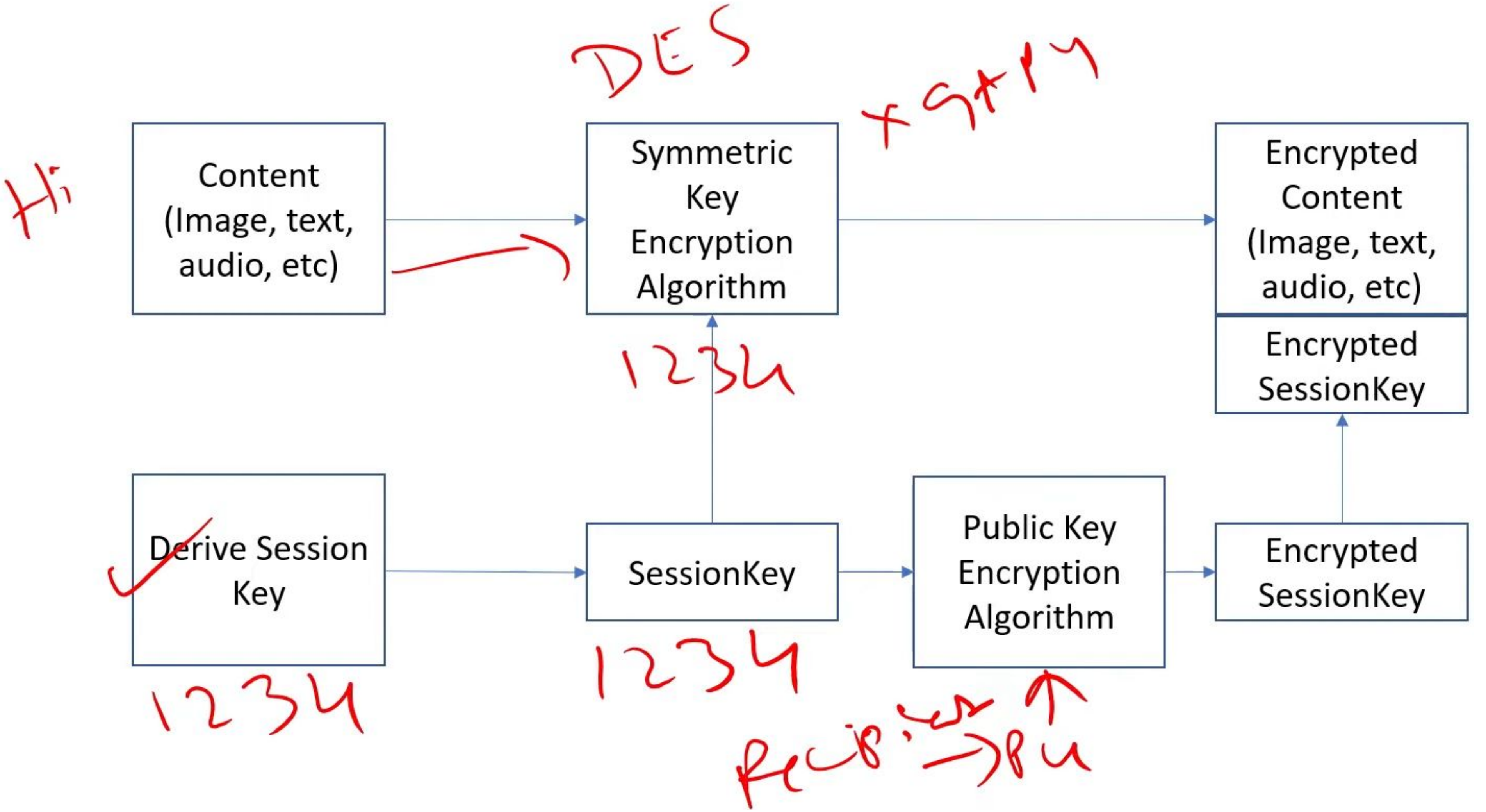
Derive Session Key

SessionKey

Public Key Encryption Algorithm

Encrypted SessionKey

Enveloped Data Content Type



Content (Image, text, audio, etc)

Symmetric Key Encryption Algorithm

Encrypted Content (Image, text, audio, etc)

Encrypted SessionKey

Derive Session Key

SessionKey

Public Key Encryption Algorithm

Encrypted SessionKey

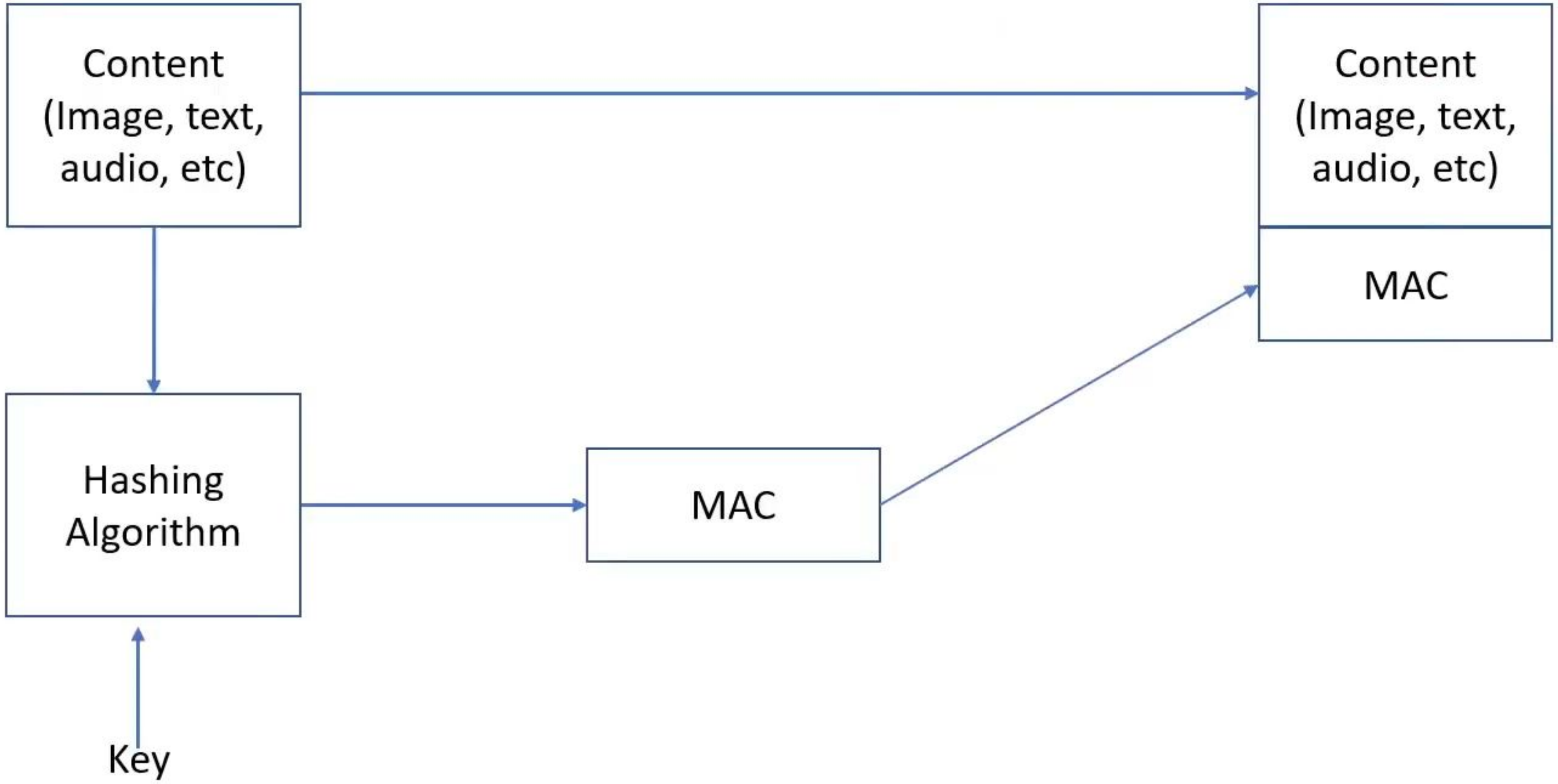
X9+PY | 5678

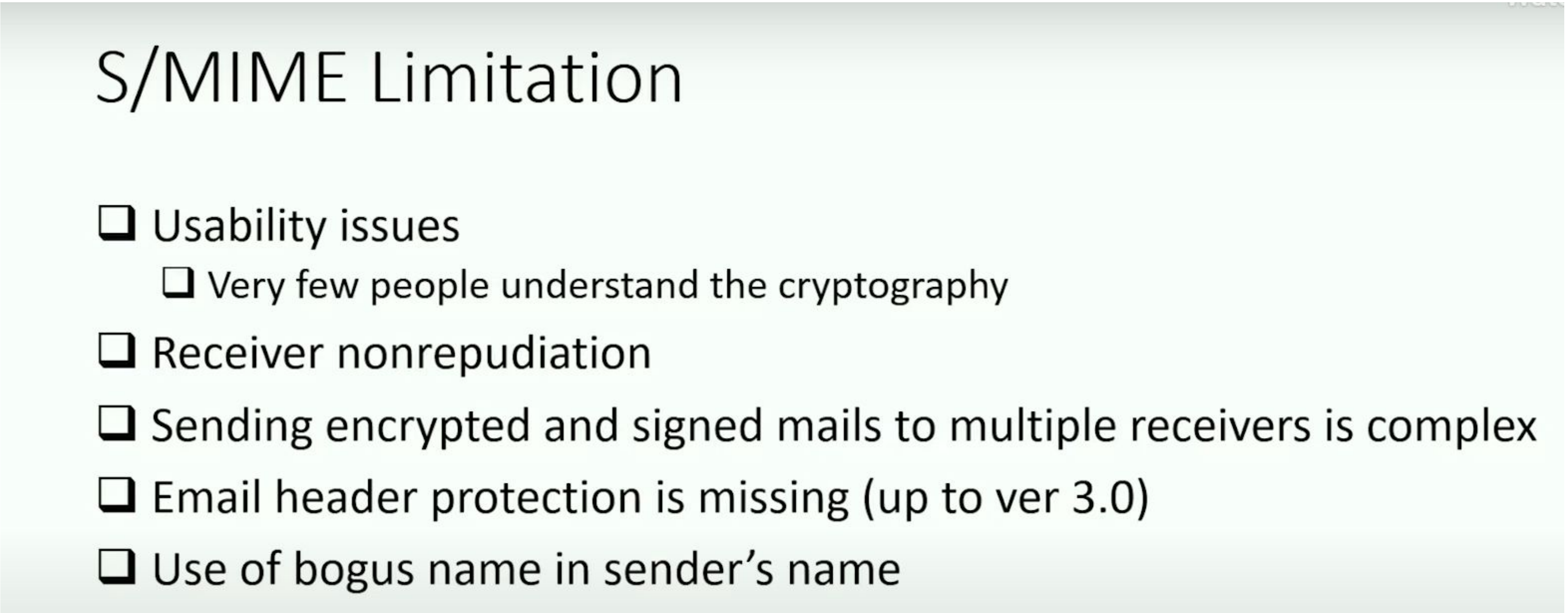
5678

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
7n8HHGghyHhHUujhJh4VQpfyF467GhIGfHfYGTrfvbnjT6jH7756tbB9H
f8HHGTrfvhJhjH776tbB9HG4VQbnj7567GhIGfHfYT6ghyHhHUujpfyF4
0GhIGfHfQbnj756YT64V
```

Authenticated Data Content Type


Content (Image, text, audio, etc)
Hashing Algorithm
Key
MAC
Content (Image, text, audio, etc)
MAC



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)

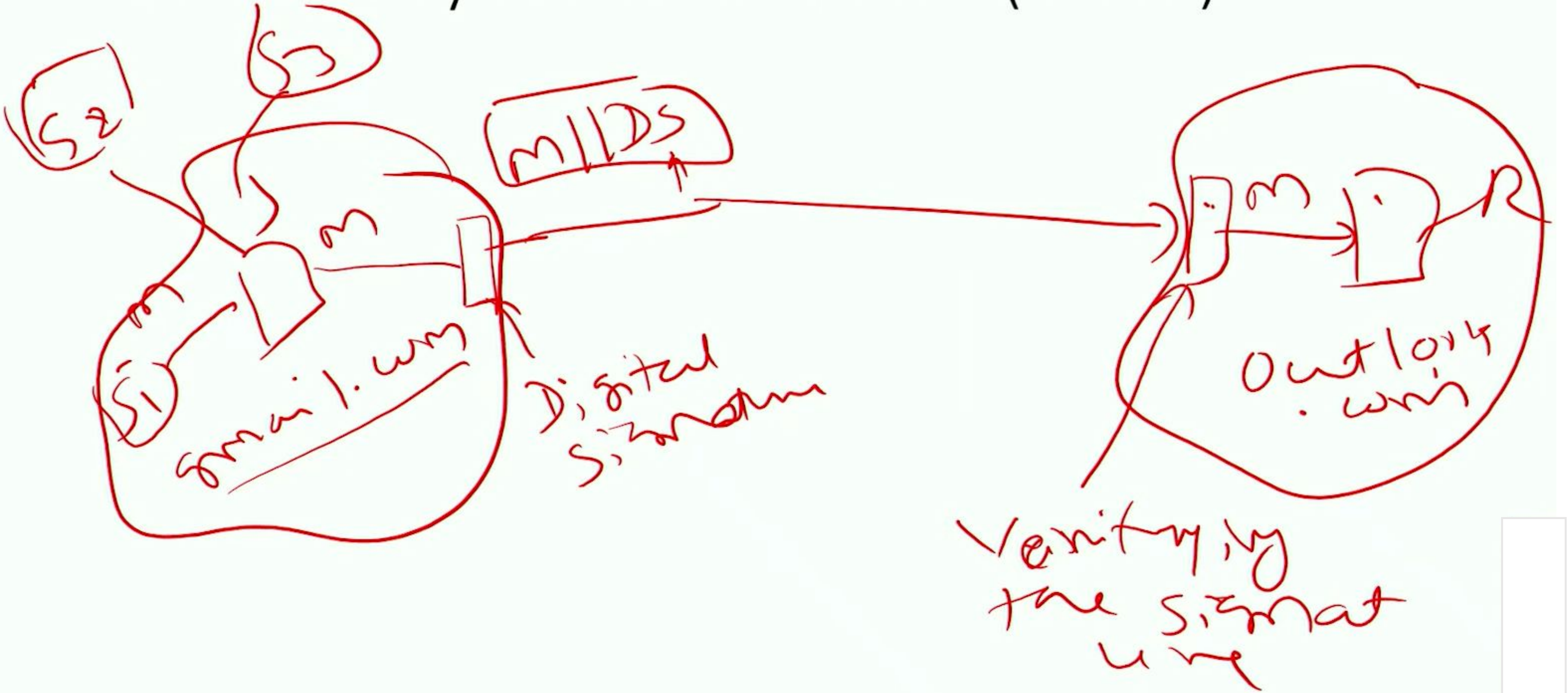
❑ It is a standard that help protect recipient from
  - ❑ Spam
  - ❑ Phishing

❑ 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+qpzIIigznS8MsPZpUMSAFjaYAP7lQUUVG5Ky4qBBk8NS4qYagh5i
aHaVjjReSbnosa8RDB/4z474by89mEJuGwoBZGDr33QxSddZjyws476o8c5q7UuLDl
XDyIAoAs3VRp3PgDwBUFsYRI0GTAHyi3c8V/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

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+qpzIIigznS8MsPZpUMSAFjaYAP7lQUUVG5Ky4qBBk8NS4qYagh5i
aHaVjjReSbnosa8RDB/4z474by89mEJuGwoBZGDr33QxSddZjyws476o8c5q7UuLDl
XDyIAoAs3VRp3PgDwBUFsYRI0GTAHyi3c8V/2SgA=
```

v-version

a-algorithm

c-canonicalization

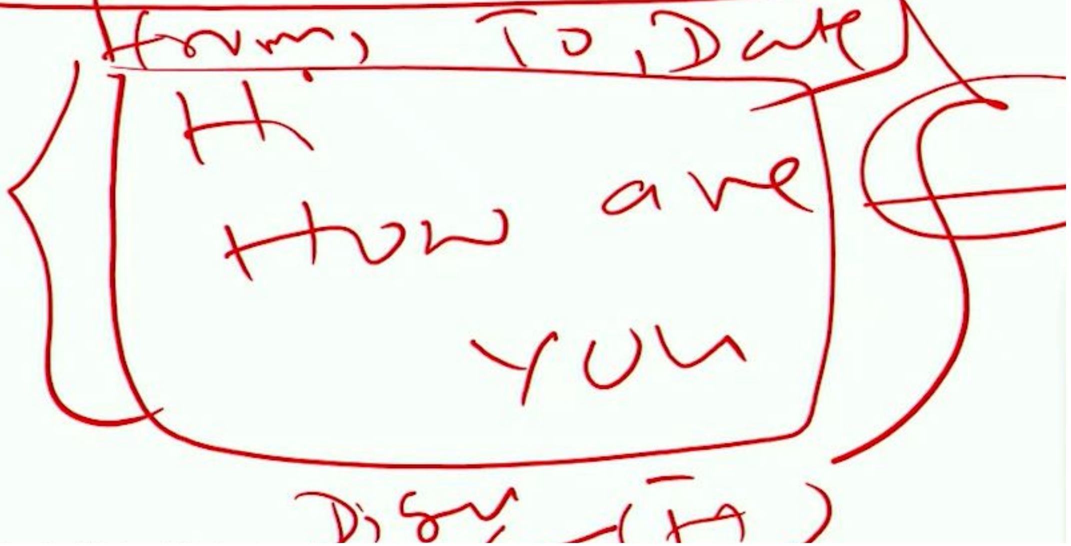
d-domain

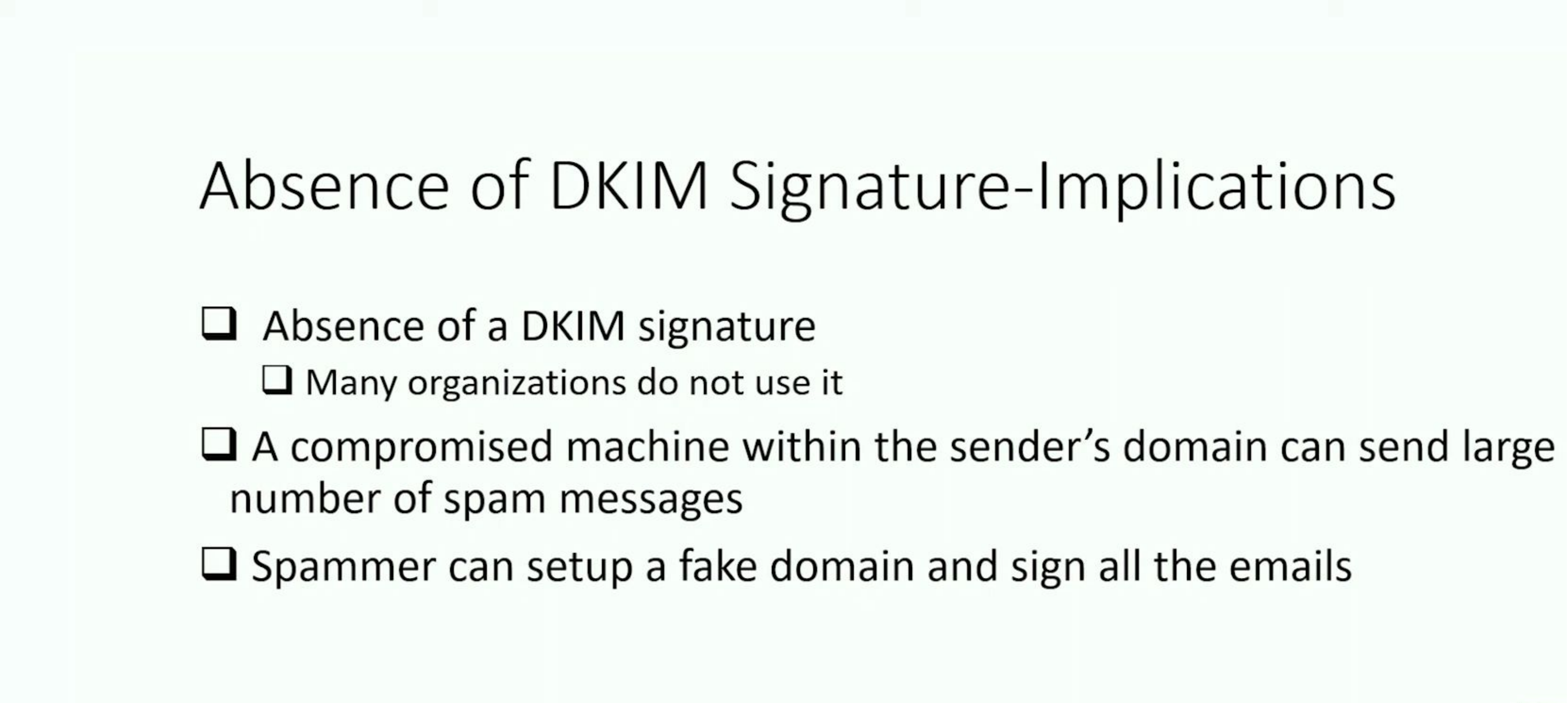
h-headers included in the hash sum

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