Email Security

Dr. Manas Khatua
Assistant Professor
Dept. of Computer Science & Engineering
Indian Institute of Technology Guwahati
URL: http://manaskhatua.github.io/
Email: manaskhatua@iitg.ac.in

Content

✓Internet Mail Architecture

✓Email Protocols

- SMTP
- POP3
- IMAP

✓Email Threats and Comprehensive Email Security

✓Email Security Protocols

- S/MIME
- STARTTLS

Internet Mail Architecture

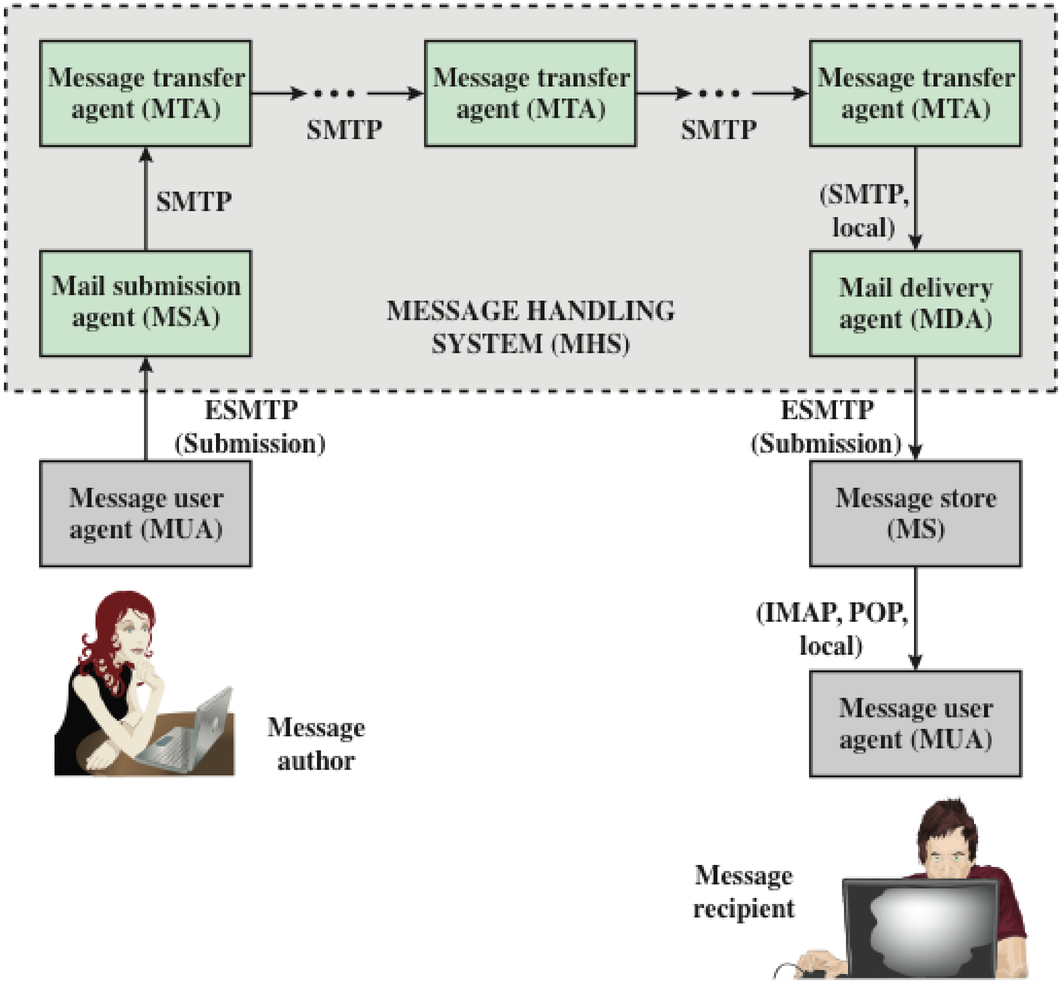
Electronic mail (email) is the most heavily used network-based application

Users expect to be able to, and do, send email to others

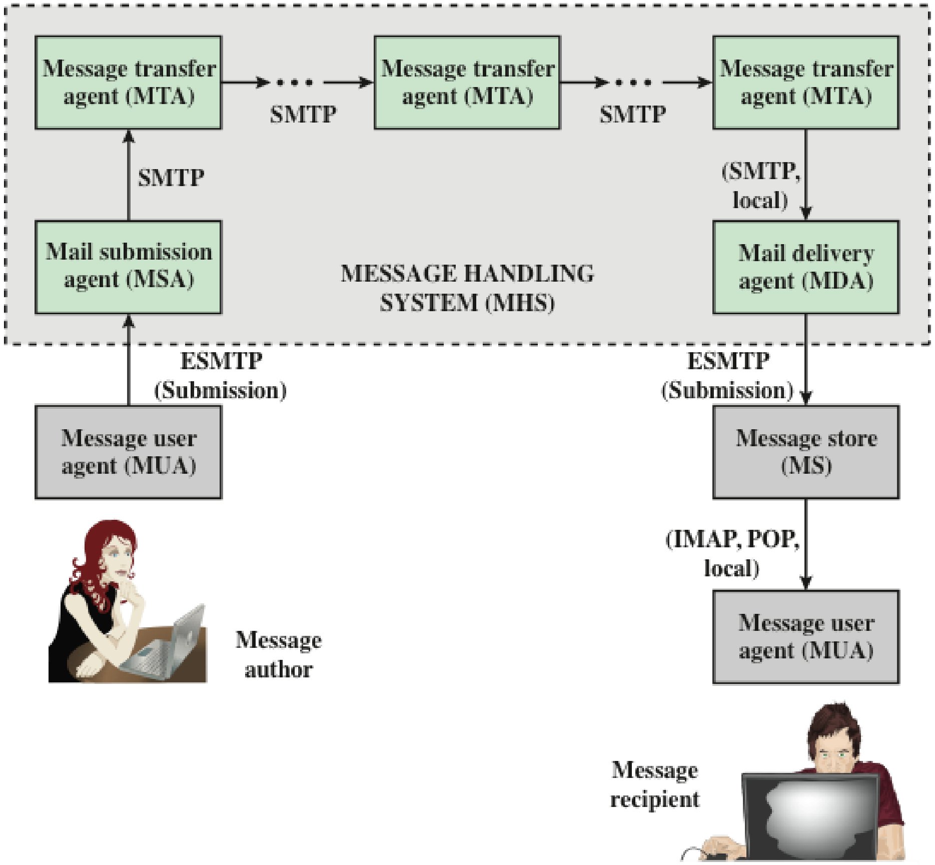
- ➢ Users and others are connected directly or indirectly to the Internet, regardless of host operating system or communications suite.

Key Components:

- ➢ Message User Agent (MUA)
  - Typically client email program
- ➢ Message Submission Agent (MSA)
  - Accepts message submitted and enforce policies of hosting domain
  - Could be located together with MUA
- ➢ Message Transfer Agent (MTA)
  - Relays mail to move the message closure to the receipients
- ➢ Message Delivery Agent (MDA)
  - Transfer message from MHS to MS
- ➢ Message Store (MS)
  - Typically an entity in remote server of MUA



Internet Mail Architecture



Three types of interoperability in this architecture

- directly between users (i.e. MUAs)
  - ✓ MUA-to-MUA exchange
- between the MUA and the MHS
  - ✓ when a message is posted from the source MUA
  - ✓ when a message is delivered to the destination MUA
- among the MTA components
  - ✓ MTA-to-MTA exchange

ADMD (administrative management domain) is an Internet email provider

- e.g. ISP that operates a public shared email service
- e.g. IT dept. that operates an enterprise mail relay
- e.g. dept. that operates a local mail relay (MTA)

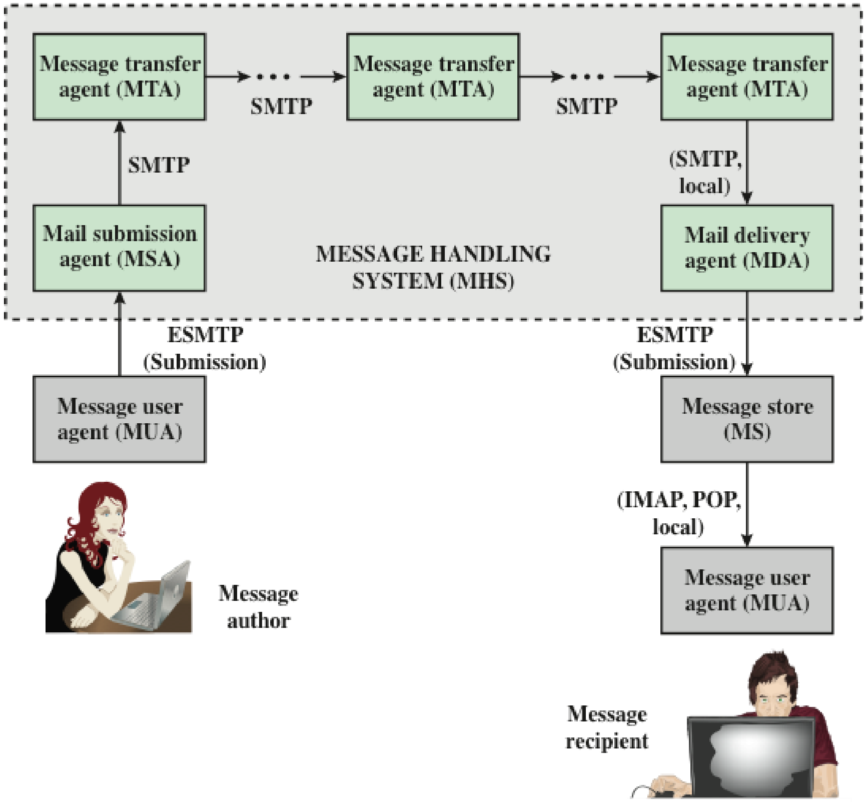
Each ADMD can have different operating policies and trust-based decision making.

Email Protocols

Two types of protocols are used for transferring email:

- Used to move messages through the Internet from source to destination
  - Simple Mail Transfer Protocol (SMTP)

- Used to transfer messages between mail servers
  - Internet Mail Access Protocol (IMAP)
  - Post Office Protocol (POP)



SMTP

- It is a text-based client-server protocol
- Originally specified in 1982 as RFC 821 and has undergone several revisions.
- Last one is: RFC 5321 published in 2008.
- Extended SMTP (ESMTP) is used to refer to these later versions of SMTP

- **Purpose**:
  - Encapsulates an email message in an envelope and is used to relay the encapsulated messages from source to destination through multiple MTAs

- General Operation structure:
  - ✓client contacts the server (next-hop recipient), and
  - ✓issues a set of commands to tell the server about the message to be sent, then
  - ✓sending the message itself.

SMTP Operation

The interchange begins with the client establishing a TCP connection to TCP port 25 on the server.

This causes the server to activate SMTP and send a 220 reply to the client.

Command & Text

Reply code & Text

```
S: 220 foo.com Simple Mail Transfer Service Ready
C: HELO bar.com
S: 250 OK
C: MAIL FROM:<Smith@bar.com>
S: 250 OK
C: RCPT TO:<Jones@foo.com>
S: 250 OK
C: RCPT TO:<Green@foo.com>
S: 550 No such user here
C: RCPT TO:<Brown@foo.com>
S: 250 OK
C: DATA
S: 354 Start mail input; end with <CRLF>.<CRLF>
C: Blah blah blah...
C: ...etc. etc. etc.
C: <CRLF><CRLF>
S: 250 OK
C: QUIT
S: 221 foo.com Service closing transmission channel
```

Mail Access Protocols

POP3

- ✓ Post Office Protocol
- ✓ Allows a local email client to download an email from an remote email server
- ✓ POP3 user agents (UA) connect via TCP to the server (typically port 110)
- ✓ After authorization, the UA can issue POP3 commands to retrieve and delete mail

IMAP

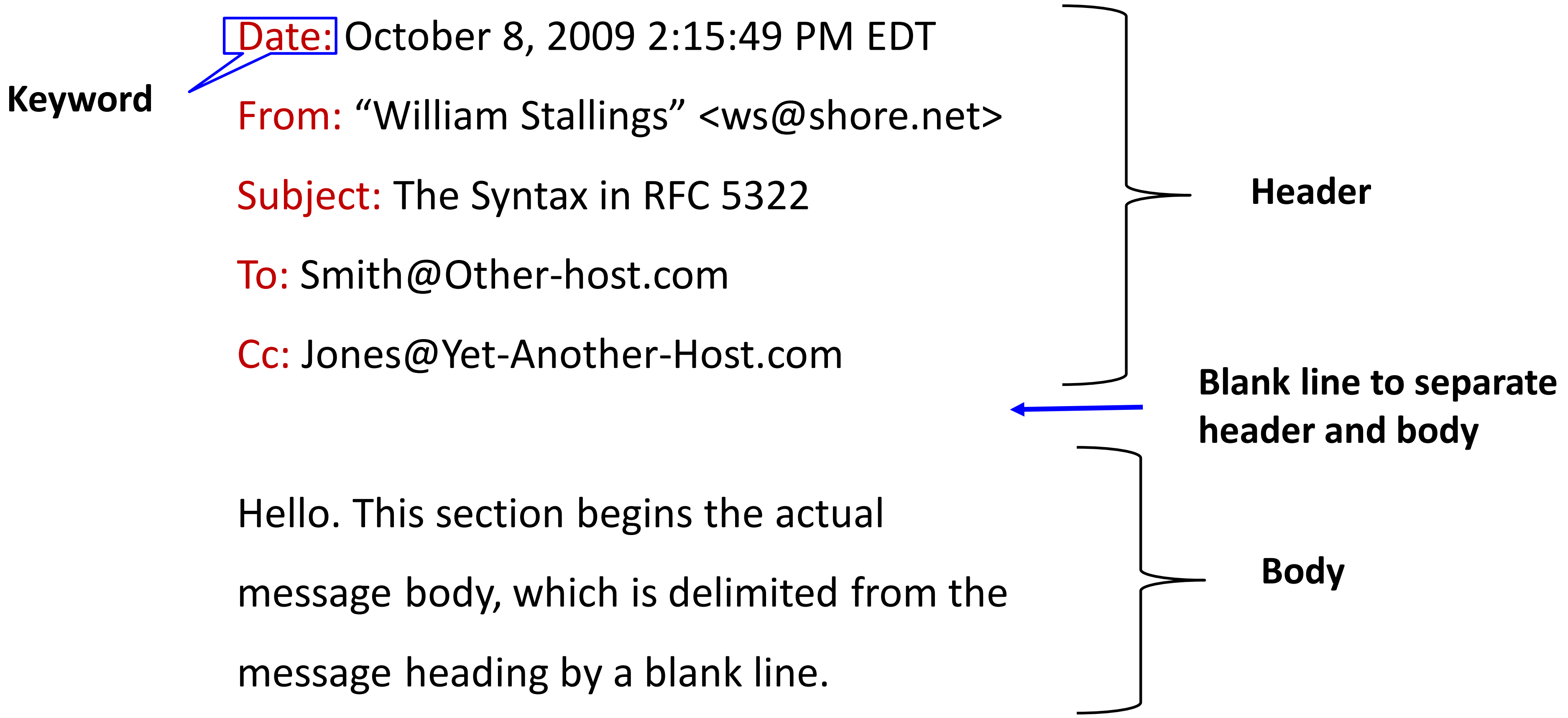
- ✓ Internet Mail Access Protocol
- ✓ Enables an email client to access their emails directly from the server and read them
- ✓ Also uses TCP, with server TCP port 143
- ✓ Provides stronger authentication than POP3
- ✓ Provides many other functions not supported by POP3
  - allows multiple devices at a time to access and read the available mails.
  - A user can update or create emails on the mail server

E-mail Format (RFC 5322)

- It defines a format for text messages that are sent using electronic mail system
- Messages are **viewed as** having an **envelope** and **contents**
  - The **envelope** contains whatever information is needed to accomplish transmission and delivery
  - The **contents** compose the object to be delivered to the recipient
- RFC 5322 standard applies only to the contents
  - The content standard includes a set of header fields that may be used by the mail system to create the envelope

Example Message Format

Keywords, followed by a colon, followed by the keywords' arguments



Date: October 8, 2009 2:15:49 PM EDT

From: "William Stallings" <ws@shore.net>

Subject: The Syntax in RFC 5322

To: Smith@Other-host.com

Cc: Jones@Yet-Another-Host.com

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

Keyword

Header

Blank line to separate header and body

Body

Limitations of use of SMTP

Few Limitations of the use of SMTP:

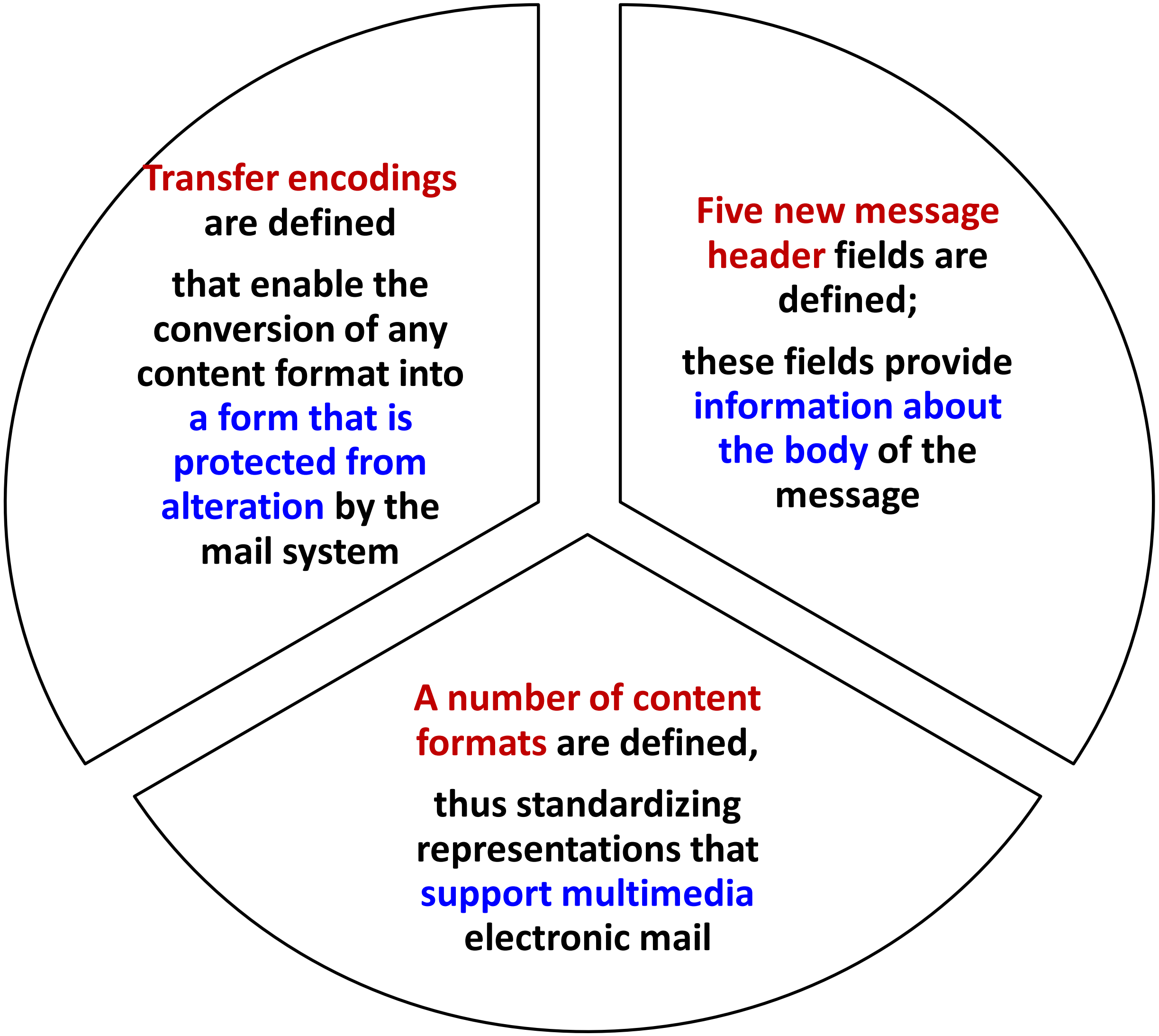
- cannot transmit executable files or other binary objects
- servers may reject mail message over a certain size
- cannot transmit text data that includes national language characters (commonly uses Unicode style)
  - (as SMTP is limited to 7-bit ASCII)
- gateways that translate between ASCII to EBCDIC do not use a consistent set of mappings, resulting in translation problems
- gateways to X.400 e-mail networks cannot handle non-textual data included in X.400 messages
  - X.400 is another email messaging systems
- implementations may not adhere completely to the SMTP standards

Multipurpose Internet Mail Extensions (MIME) [RFC 2045 – 2049]

- is an extension to the RFC 5322 (Internet Message Format) framework
- addressed some issues of SMTP (RFC 5321)

MIME Specification

MIME specification includes the following elements:



Transfer encodings are defined

that enable the conversion of any content format into a form that is protected from alteration by the mail system

Five new message header fields are defined;

these fields provide information about the body of the message

A number of content formats are defined,

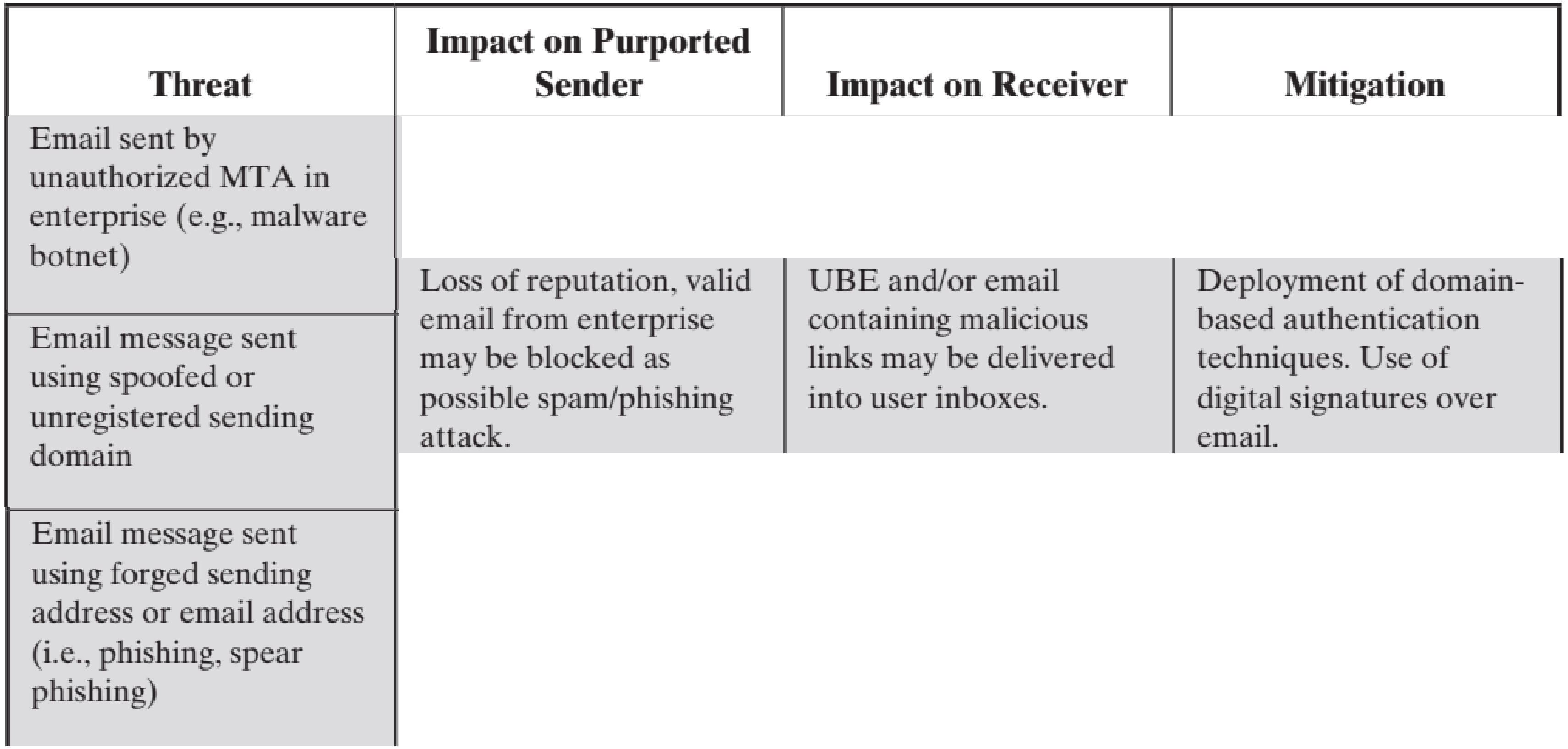
thus standardizing representations that support multimedia electronic mail

Email Security Threats

Classified as follows:

- Authenticity-related threats
  - ✓Could result in unauthorized access to an enterprise’s email system
- Confidentiality-related threats
  - ✓Could result in unauthorized disclosure of sensitive information
- Integrity-related threats
  - ✓Could result in unauthorized modification of email content
- Availability-related threats
  - ✓Could prevent end users from being able to send or receive mail

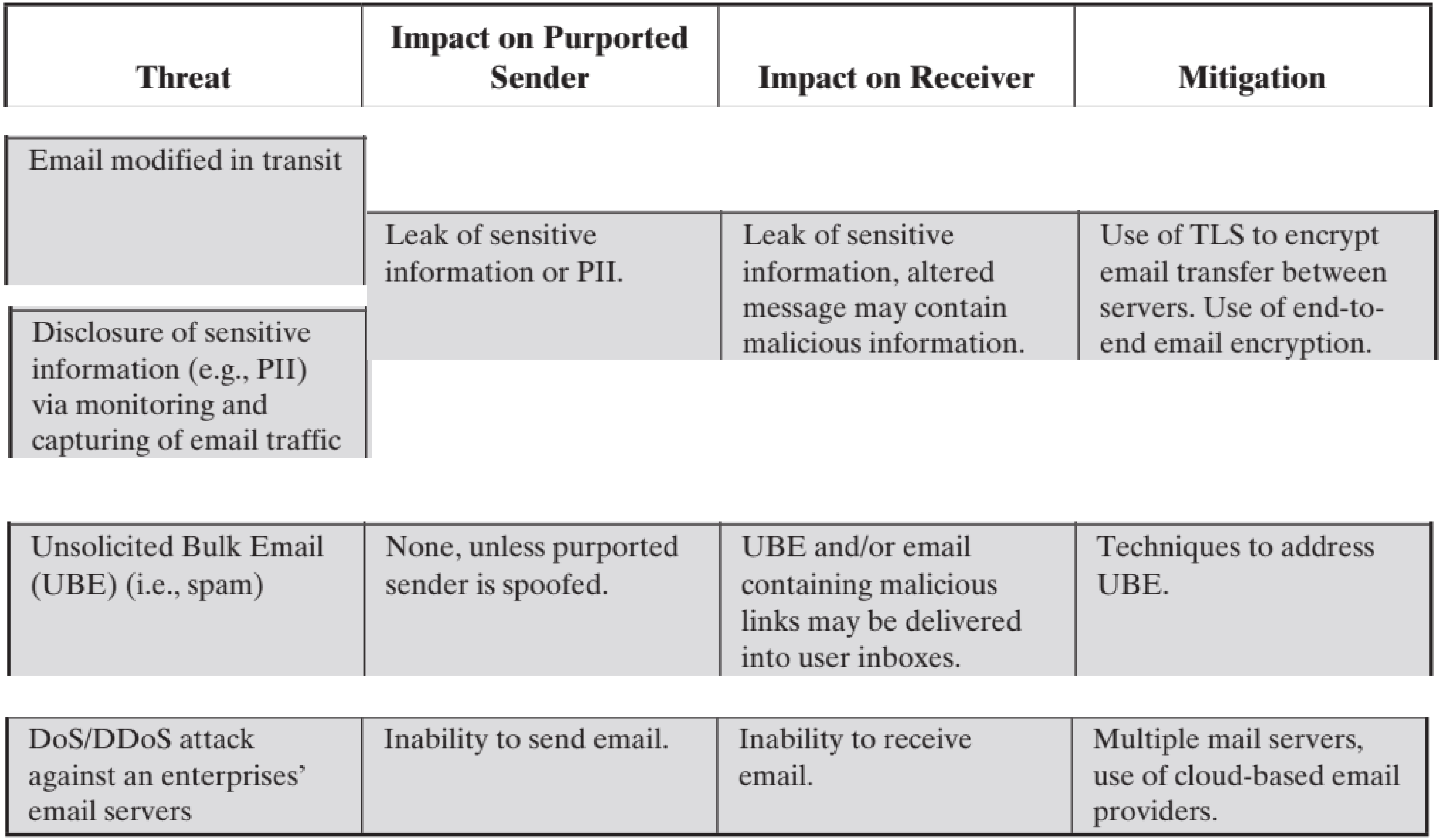
Email Threats and Mitigations



Threat	Impact on Purported Sender	Impact on Receiver	Mitigation
Email sent by unauthorized MTA in enterprise (e.g., malware botnet)	Loss of reputation, valid email from enterprise may be blocked as possible spam/phishing attack.	UBE and/or email containing malicious links may be delivered into user inboxes.	Deployment of domain-based authentication techniques. Use of digital signatures over email.
Email message sent using spoofed or unregistered sending domain			
Email message sent using forged sending address or email address (i.e., phishing, spear phishing)			

Unsolicited bulk email (UBE), Personal Identifying Information (PII)

Email Threats and Mitigations



Threat	Impact on Purported Sender	Impact on Receiver	Mitigation
Email modified in transit	Leak of sensitive information or PII.	Leak of sensitive information, altered message may contain malicious information.	Use of TLS to encrypt email transfer between servers. Use of end-to-end email encryption.
Disclosure of sensitive information (e.g., PII) via monitoring and capturing of email traffic			
Unsolicited Bulk Email (UBE) (i.e., spam)	None, unless purported sender is spoofed.	UBE and/or email containing malicious links may be delivered into user inboxes.	Techniques to address UBE.
DoS/DDoS attack against an enterprises' email servers	Inability to send email.	Inability to receive email.	Multiple mail servers, use of cloud-based email providers.

Protocols to Counter Email Threats

- **STARTTLS**
  - An SMTP security extension that provides authentication, integrity, non-repudiation and confidentiality for the entire SMTP message by running SMTP over TLS
- **S/MIME**
  - Provides authentication, integrity, non-repudiation and confidentiality of the message body carried in SMTP messages
- **DNS Security Extensions (DNSSEC)**
  - Provides authentication and integrity protection of DNS data, and is an underlying tool used by various email security protocols
- **DNS-based Authentication of Named Entities (DANE)**
  - Is designed to overcome problems in the certificate authority (CA) system by providing an alternative channel for authenticating public keys based on DNSSEC

Cont…

- **Sender Policy Framework (SPF)**
  - Uses the DNS to allow domain owners to create records that associate the domain name with a specific IP address range of authorized message senders.

- **DomainKeys Identified Mail (DKIM)**
  - Enables an MTA to sign selected headers and the body of a message. This validates the source domain of the mail and provides message body integrity

- **Domain-based Message Authentication, Reporting, and Conformance (DMARC)**
  - Lets senders know the proportionate effectiveness of their SPF and DKIM policies, and
  - signals to receivers what action should be taken in various individual and bulk attack scenarios

STARTTLS

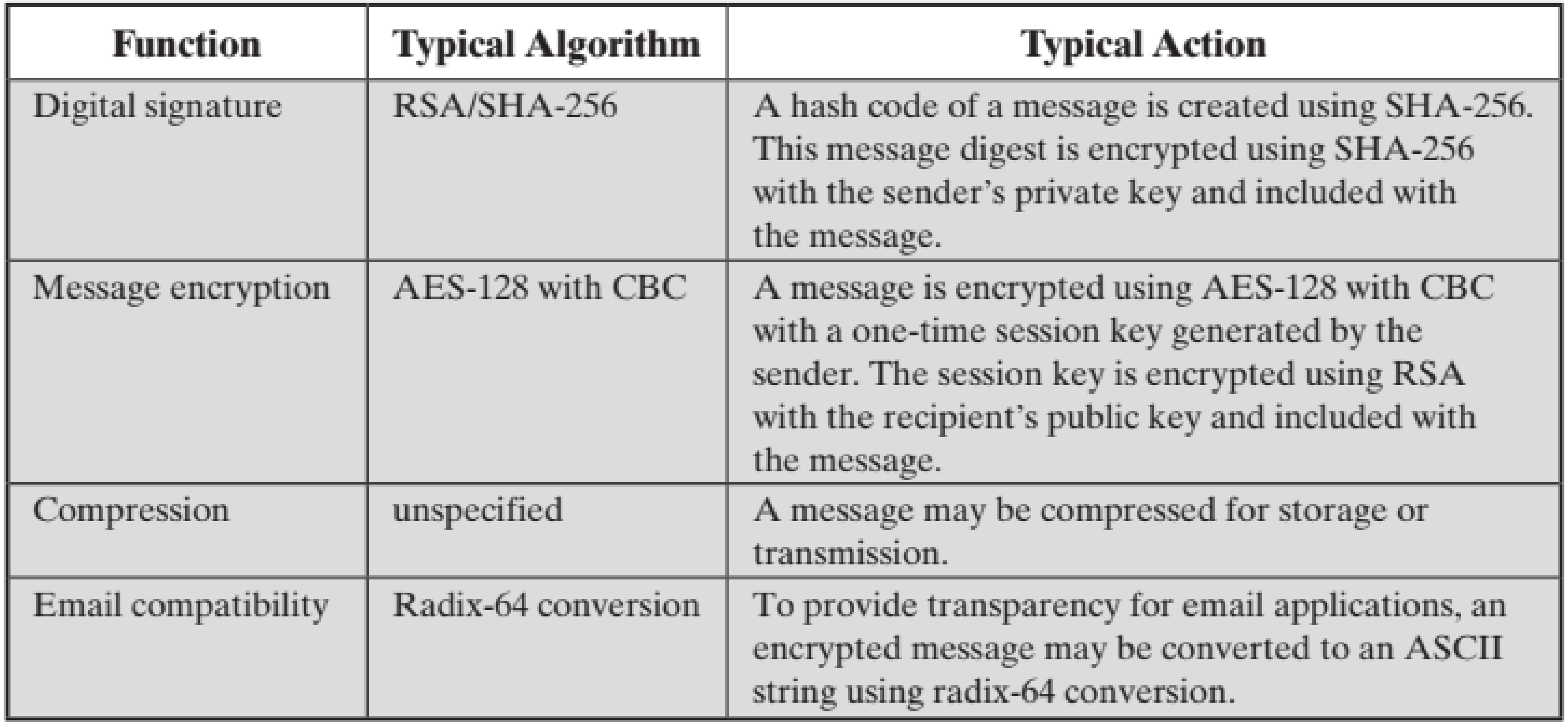
- STARTTLS is security-related extension for SMTP
  - ✓ RFC 3207 (SMTP Service Extension for Secure SMTP over Transport Layer Security, February 2002)

- Enables below features in the exchange between SMTP agents
  - ➢ confidentiality
  - ➢ authentication

- Advantage of using STARTTLS is that-
  - ➢ the server can offer secured SMTP service on a single port, rather than requiring separate port numbers for secure and clear-text operations

S/MIME

- S/MIME is a security enhancement to the MIME Internet email format standard
- It provides four message-related services:
  - authentication, confidentiality, compression, and email compatibility

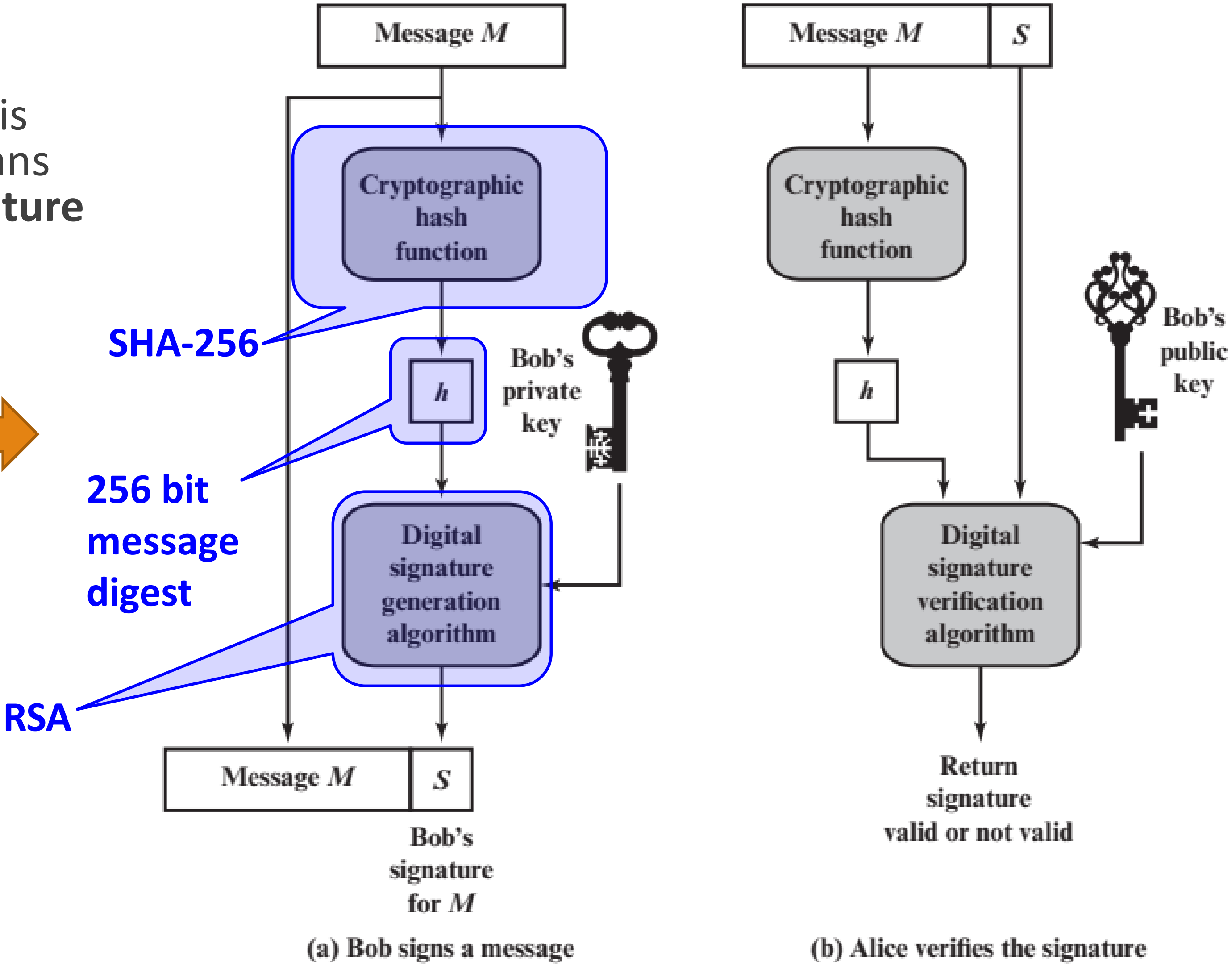


Function	Typical Algorithm	Typical Action
Digital signature	RSA/SHA-256	A hash code of a message is created using SHA-256. This message digest is encrypted using SHA-256 with the sender's private key and included with the message.
Message encryption	AES-128 with CBC	A message is encrypted using AES-128 with CBC with a one-time session key generated by the sender. The session key is encrypted using RSA with the recipient's public key and included with the message.
Compression	unspecified	A message may be compressed for storage or transmission.
Email compatibility	Radix-64 conversion	To provide transparency for email applications, an encrypted message may be converted to an ASCII string using radix-64 conversion.

Authentication

- Authentication is provided by means of a **digital signature**

Digital Signature


Message *M*
SHA-256
Cryptographic hash function
h
256 bit message digest
Bob's private key
Digital signature generation algorithm
RSA
Message *M*
S
Bob's signature for *M*
(a) Bob signs a message
Message *M*
S
Cryptographic hash function
h
Bob's public key
Digital signature verification algorithm
Return signature valid or not valid
(b) Alice verifies the signature

Authentication

- **Who is the sender?**

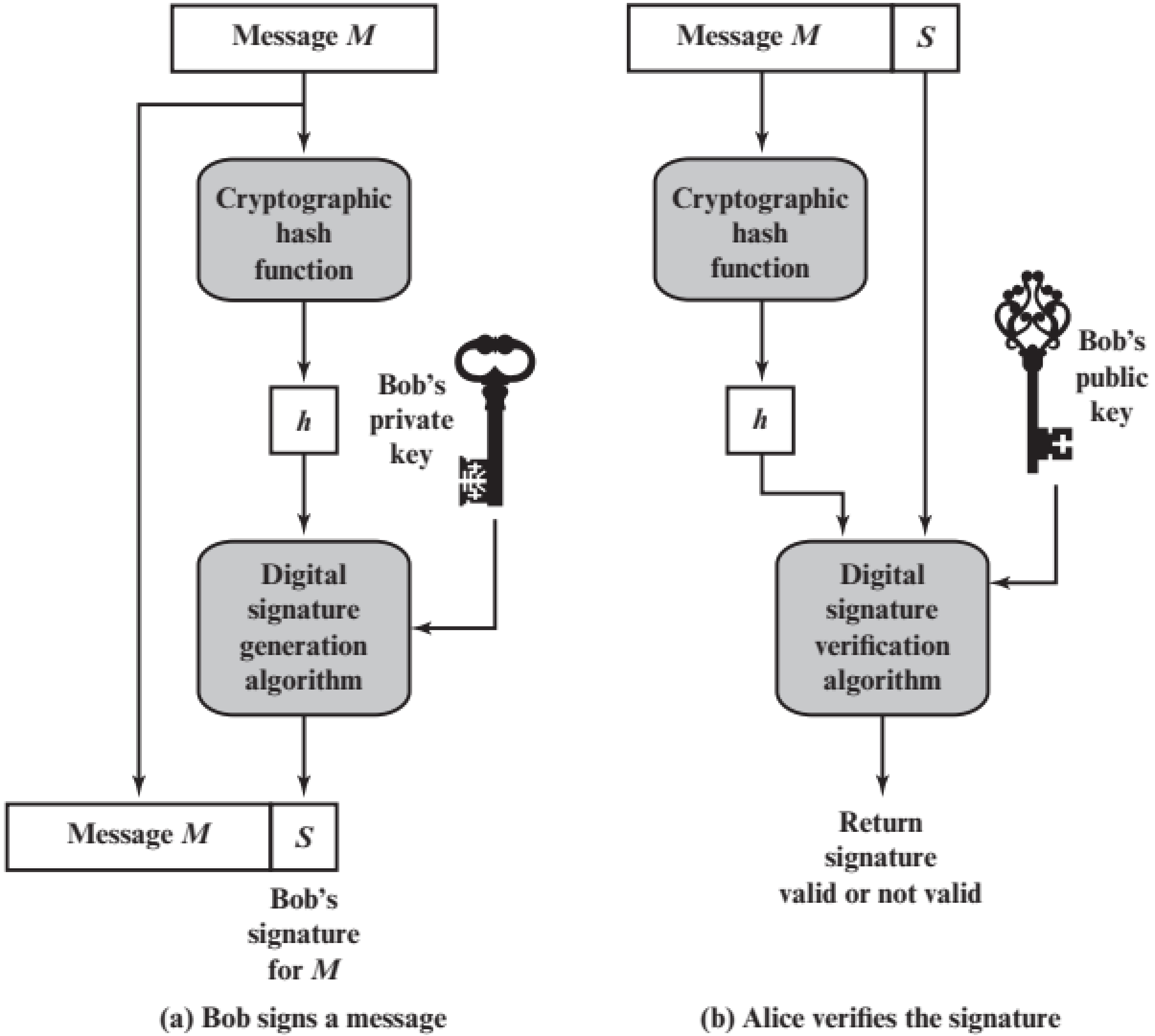
  Because of RSA: the recipient is assured that only the possessor of the matching private key can generate the signature

- **Any duplicate hash code?**

  Because of SHA-256: the recipient is assured that no one else could generate a new message that matches the hash code

- **S&M should be together?**

  Detached signatures are supported. It may be stored and transmitted separately from the message it signs.
  - e.g. legal contract



Message *M*
Cryptographic hash function
h
Bob's private key
Digital signature generation algorithm
Message *M*
S
Bob's signature for *M*
Message *M*
S
Cryptographic hash function
h
Bob's public key
Digital signature verification algorithm
Return signature valid or not valid

(a) Bob signs a message

(b) Alice verifies the signature

Confidentiality

- Confidentiality is provided by encrypting messages.
  - AES with a 128-bit key in cipher block chaining (CBC) mode is commonly used
  - The key itself is also encrypted, typically with RSA

- **Assume**: key distribution is done
- each symmetric key, referred to as a content-encryption key, is used only once

Steps:

I. The sender generates a message and a random 128-bit number to be used as a content-encryption key for this message only

II. The message is encrypted using the content-encryption key

III. The content-encryption key is encrypted with RSA using the recipient's public key and is attached to the message.

IV. The receiver uses RSA with its private key to decrypt and recover the content-encryption key

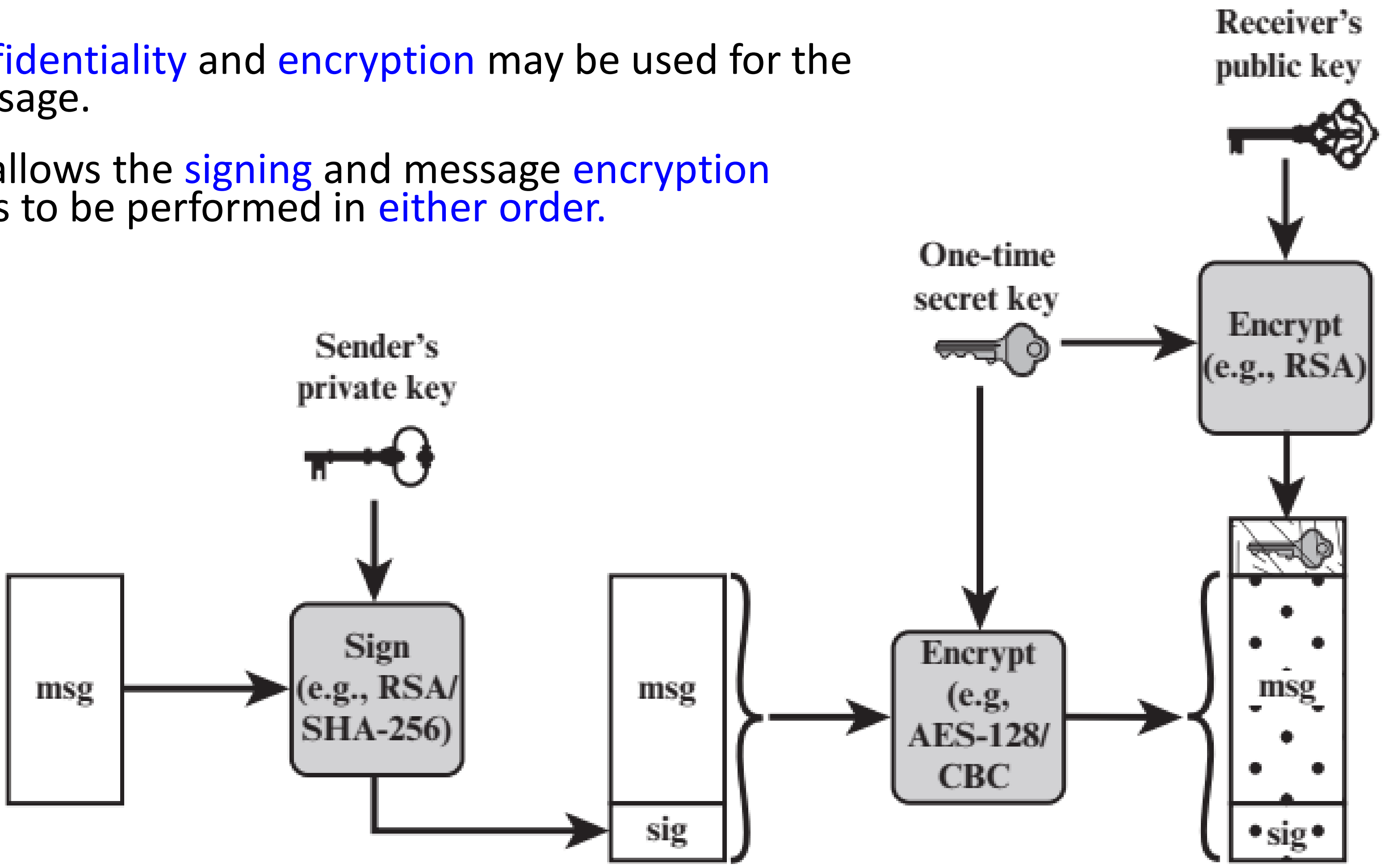
V. The content-encryption key is used to decrypt the message.

Confidentiality

- Several observations
  - First, to reduce encryption time, the combination of symmetric and public-key encryption is used
  - Second, the use of the public-key algorithm solves the session-key distribution problem
    - Furthermore, given the store-and-forward nature of electronic mail, the use of handshaking to assure that both sides have the same session key is not practical.
  - Finally, the use of onetime symmetric keys strengthens what is already a strong symmetric encryption approach.

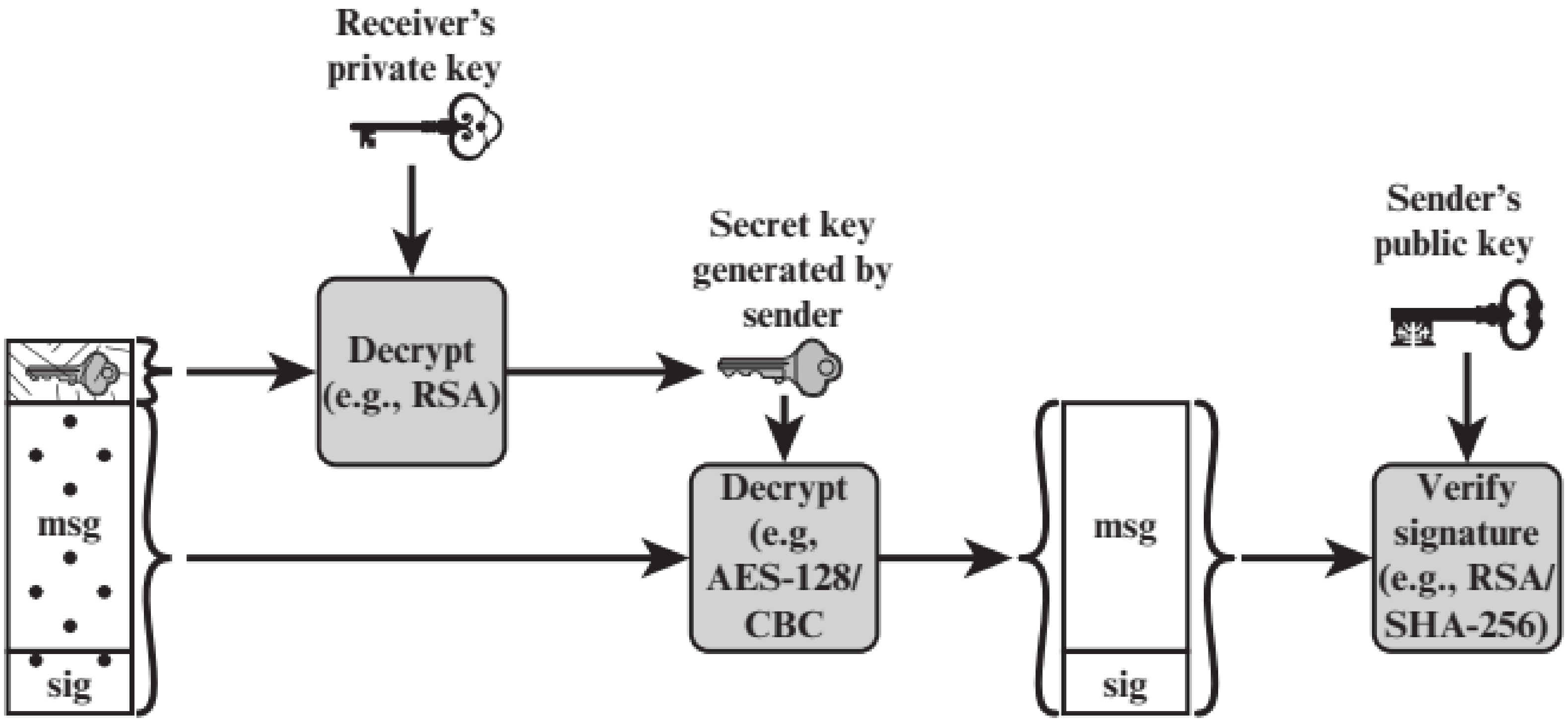
Confidentiality & Authentication

- both confidentiality and encryption may be used for the same message.
- S/MIME allows the signing and message encryption operations to be performed in either order.



(a) Sender signs, then encrypts message

Cont…


Receiver's private key
Secret key generated by sender
Sender's public key
Decrypt (e.g., RSA)
Decrypt (e.g, AES-128/ CBC
Verify signature (e.g., RSA/ SHA-256)
msg
sig
msg
sig

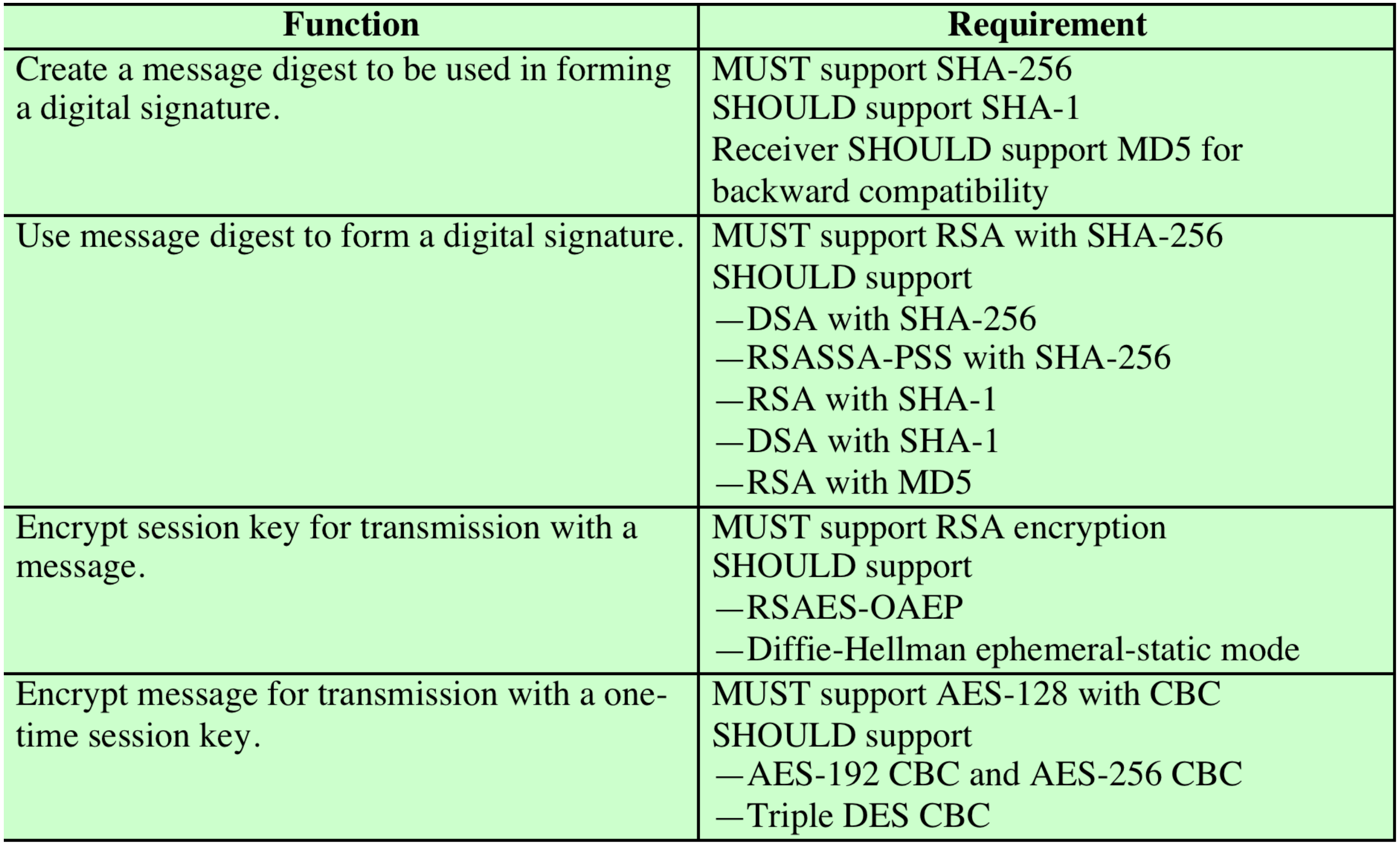
(b) Receiver decrypts message, then verifies sender's signature

E-mail Compatibility

- Many e-mail systems only permit the use of blocks consisting of ASCII text
  - To accommodate this restriction, S/MIME provides the service of converting the raw 8-bit binary stream to a stream of printable 7-bit ASCII characters
  - The scheme used for this purpose is Base-64 conversion
    - ✓ Each group of three octets of binary data is mapped into four ASCII characters
    - ✓ The Base64 algorithm blindly converts the input stream to Base64 format regardless of content, even if the input happens to be ASCII text
- If only the signature service is used, then the message digest is encrypted (with the sender's private key).
- If the confidentiality service is used, the message plus signature (if present) are encrypted (with a one-time symmetric key)

Approved Cryptographic Algorithms

- Cryptographic Algorithms Used in S/MIME



Function	Requirement
Create a message digest to be used in forming a digital signature.	MUST support SHA-256 SHOULD support SHA-1 Receiver SHOULD support MD5 for backward compatibility
Use message digest to form a digital signature.	MUST support RSA with SHA-256 SHOULD support —DSA with SHA-256 —RSASSA-PSS with SHA-256 —RSA with SHA-1 —DSA with SHA-1 —RSA with MD5
Encrypt session key for transmission with a message.	MUST support RSA encryption SHOULD support —RSAES-OAEP —Diffie-Hellman ephemeral-static mode
Encrypt message for transmission with a one-time session key.	MUST support AES-128 with CBC SHOULD support —AES-192 CBC and AES-256 CBC —Triple DES CBC

S/MIME Certificate Processing

- S/MIME uses public-key certificates that conform to version 3 of X.509
- S/MIME managers and/or users must configure each client with a list of trusted keys and with certificate revocation lists, i.e. the responsibility is local.
- The certificates are signed by certification authorities (CA)

- A user's public key must be registered with a CA in order to receive an X.509 public-key certificate.
- A user requires access to a local list of certificates in order to verify incoming signatures and to encrypt outgoing messages

Thank you

Questions and Discussion