Electronic Mail Security

S/MIME

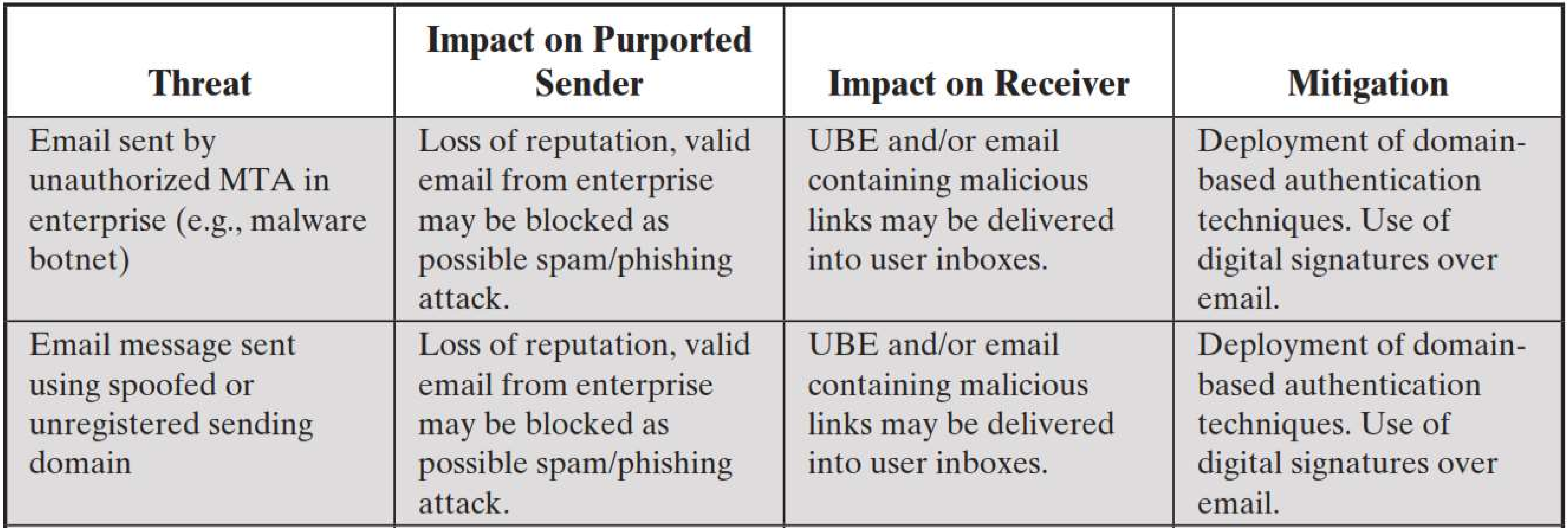
MIME

- Multipurpose Internet Mail Extension (MIME) is a standard used to expand the limited capabilities of email.
- MIME is an extension to the Internet email protocol.
- Email can only send messages in NVT 7-bit ASCII format using SMTP, where as MIME allows users to exchange different non ASCII data through email like audio, video, images etc.
- Email messages with MIME formatting are typically transmitted using standard protocols like SMTP.
- It is an extension to the RFC 5322 framework that is intended to address some of the problems and limitations of the use of Simple Mail Transfer Protocol (SMTP) or some other mail transfer protocol and RFC 5322 for electronic mail.

MIME

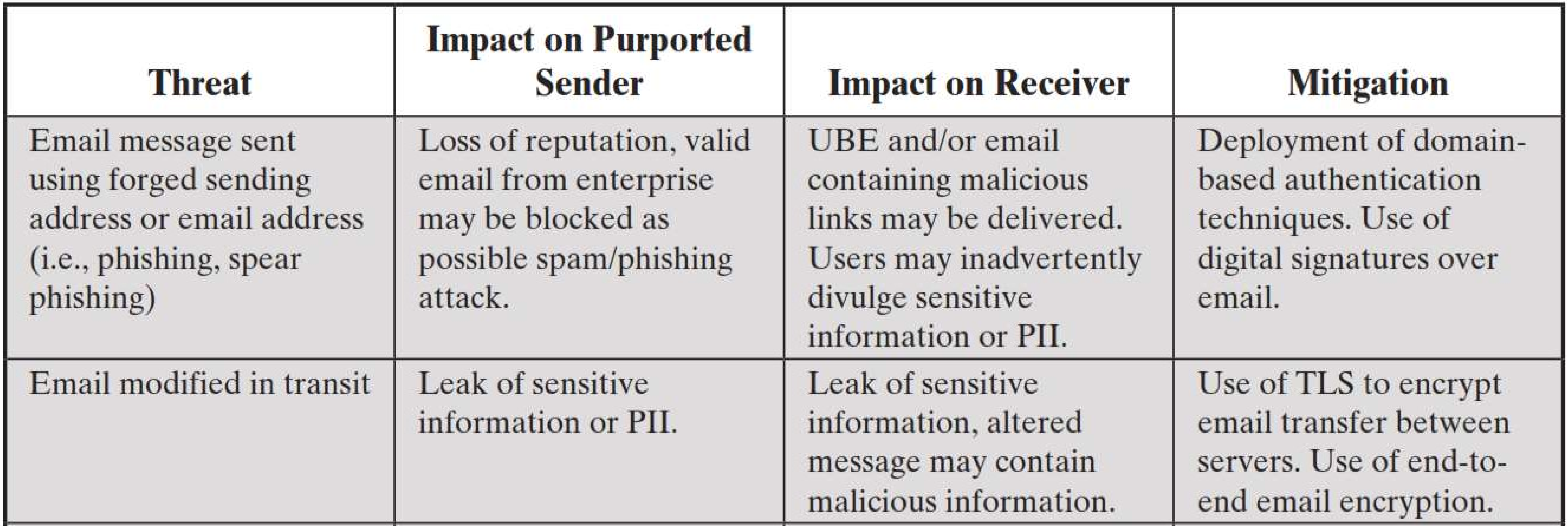
- Limitations of the SMTP/5322 scheme:
  - **SMTP cannot transmit executable files or other binary objects**. A number of schemes are in use for converting binary files into a text form that can be used by SMTP mail systems.
  - **SMTP cannot transmit text data that includes national language characters,** because these are represented by 8-bit codes with values of 128 decimal or higher, and SMTP is limited to **7-bit ASCII**.
  - **SMTP servers may reject mail message over a certain size.**
  - **SMTP gateways that translate between ASCII and the character code EBCDIC** do not use a consistent set of mappings, resulting in translation problems.
  - **SMTP gateways to X.400 electronic mail networks cannot handle nontextual** data included in X.400 messages.

Email Threats and Mitigations



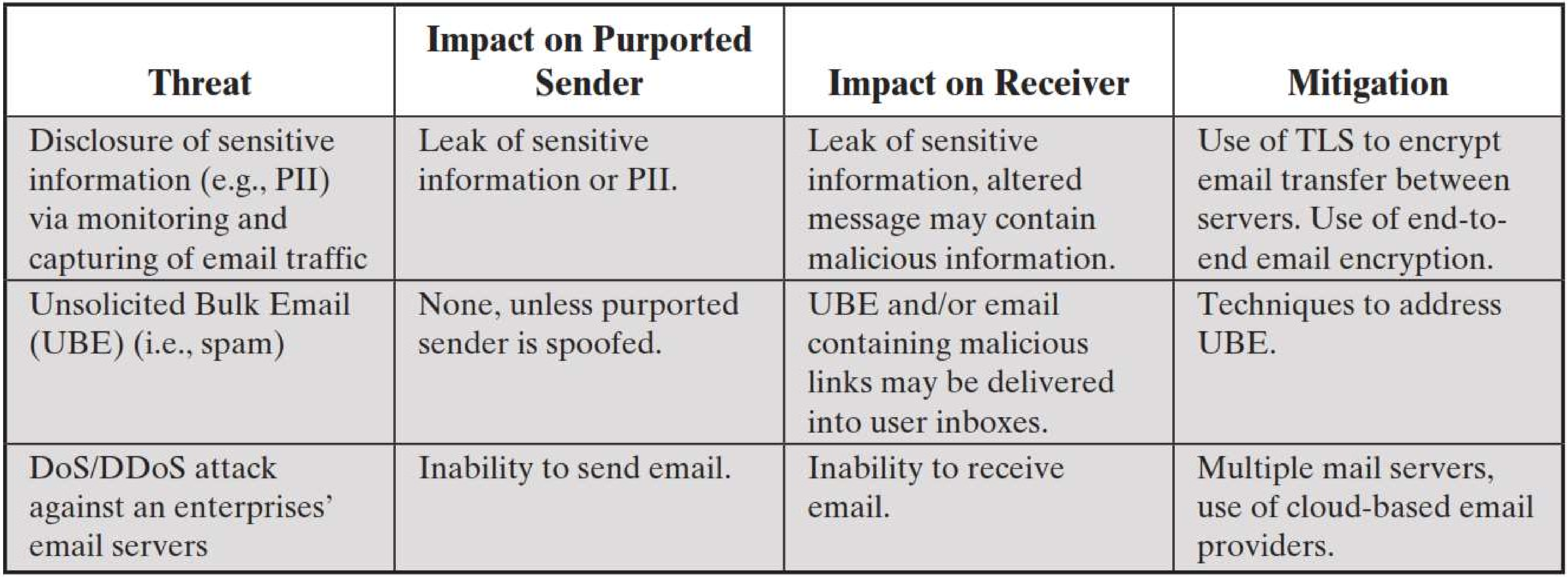
Threat	Impact on Purported Sender	Impact on Receiver	Mitigation
Email sent by unauthorized MTA in enterprise (e.g., malware botnet)	Loss of reputation, valid email from enterprise may be blocked as possible spam/phishing attack.	UBE and/or email containing malicious links may be delivered into user inboxes.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



Threat	Impact on Purported Sender	Impact on Receiver	Mitigation
Email message sent using forged sending address or email address (i.e., phishing, spear phishing)	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. Users may inadvertently divulge sensitive information or PII.	Deployment of domain-based authentication techniques. Use of digital signatures over email.
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.

Email Threats and Mitigations



Threat	Impact on Purported Sender	Impact on Receiver	Mitigation
Disclosure of sensitive information (e.g., PII) via monitoring and capturing of email traffic	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.
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.

S/MIME

- Secure/Multipurpose Internet Mail Extension (S/MIME) is a security enhancement to the MIME Internet email format standard based on technology from RSA Data Security.
- S/MIME provides security for commercial emails by encrypting mails.
- It is an extension of MIME protocol.
- It is a widely accepted Method (or more precisely a protocol) for sending digitally signed and encrypted messages.
- It allow us to digitally sign our email to verify ourselves as the legitimate sender and also encryption and decryption of mails
- It is based on Asymmetric key encryption.
- In short, S/MIME is a protocol used to encrypt emails and digitally sign them.

- S/MIME provides
  - authentication,
  - message integrity,
  - non repudiation of origin using digital signature,
  - privacy and
  - data security using encryption.
- S/MIME provides for four message-related services: authentication, confidentiality, compression, and email compatibility.

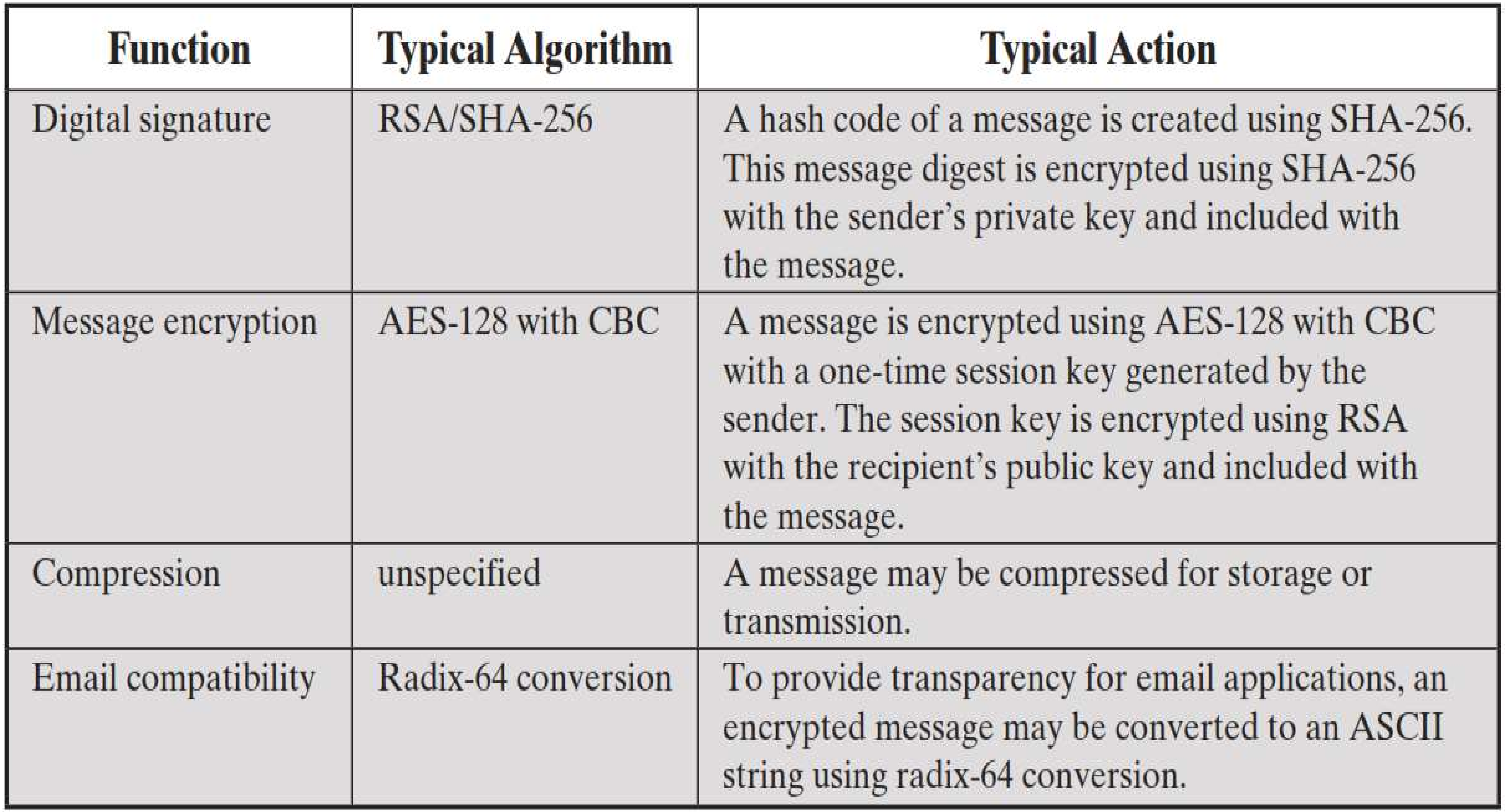
S/MIME Services

Authentication

Non-repudiation

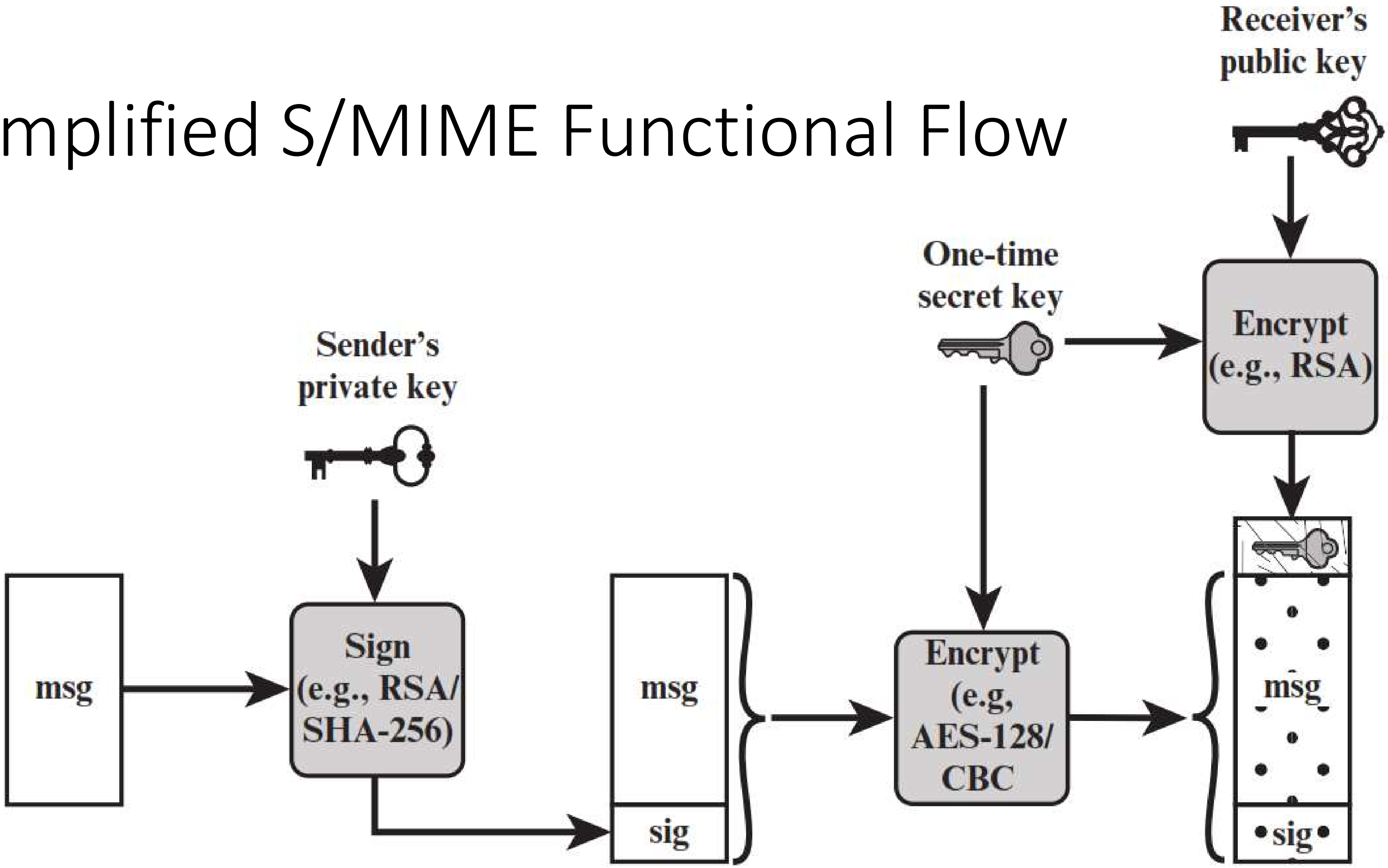
Confidentiality

Data integrity



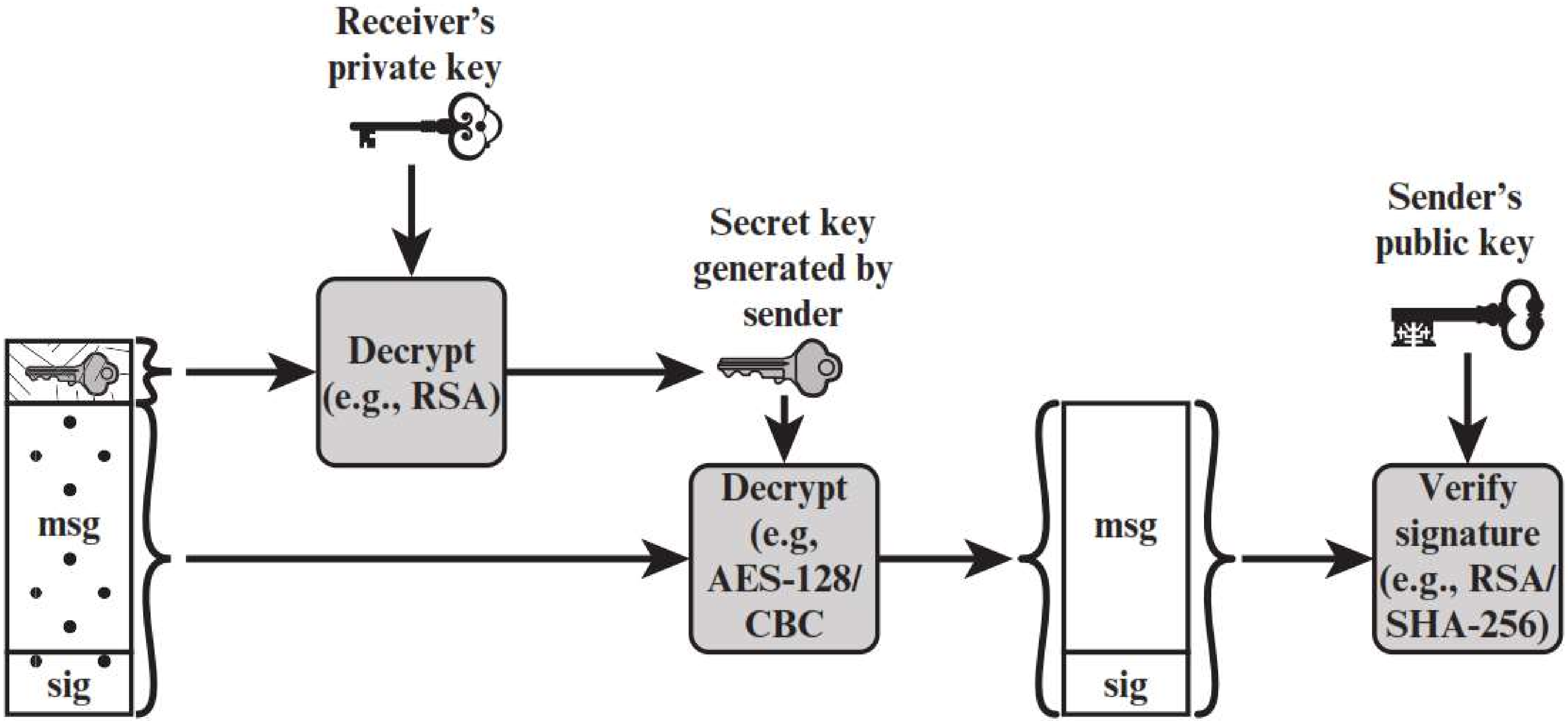
Function	Typical Algorithm	Typical Action
Digital signature	RSA/SHA-256	A hash code of a message is created using SHA-256. This message digest is encrypted using SHA-256 with the sender's private key and included with the message.
Message encryption	AES-128 with CBC	A message is encrypted using AES-128 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.

Simplified S/MIME Functional Flow



(a) Sender signs, then encrypts message

Simplified S/MIME Functional Flow


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

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

Simplified S/MIME Functional Flow

- As Figure illustrates, both confidentiality and encryption may be used for the same message. The figure shows a sequence in which a signature is generated for the plaintext message and appended to the message.
- Then the plaintext message and signature are encrypted as a single block using symmetric encryption and the symmetric encryption key is encrypted using public-key encryption.
- S/MIME allows the signing and message encryption operations to be performed in either order. If signing is done first, the identity of the signer is hidden by the encryption. Plus, it is generally more convenient to store a signature with a plaintext version of a message.
- Furthermore, for purposes of third-party verification, if the signature is performed first, a third party need not be concerned with the symmetric key when verifying the signature.

Simplified S/MIME Functional Flow

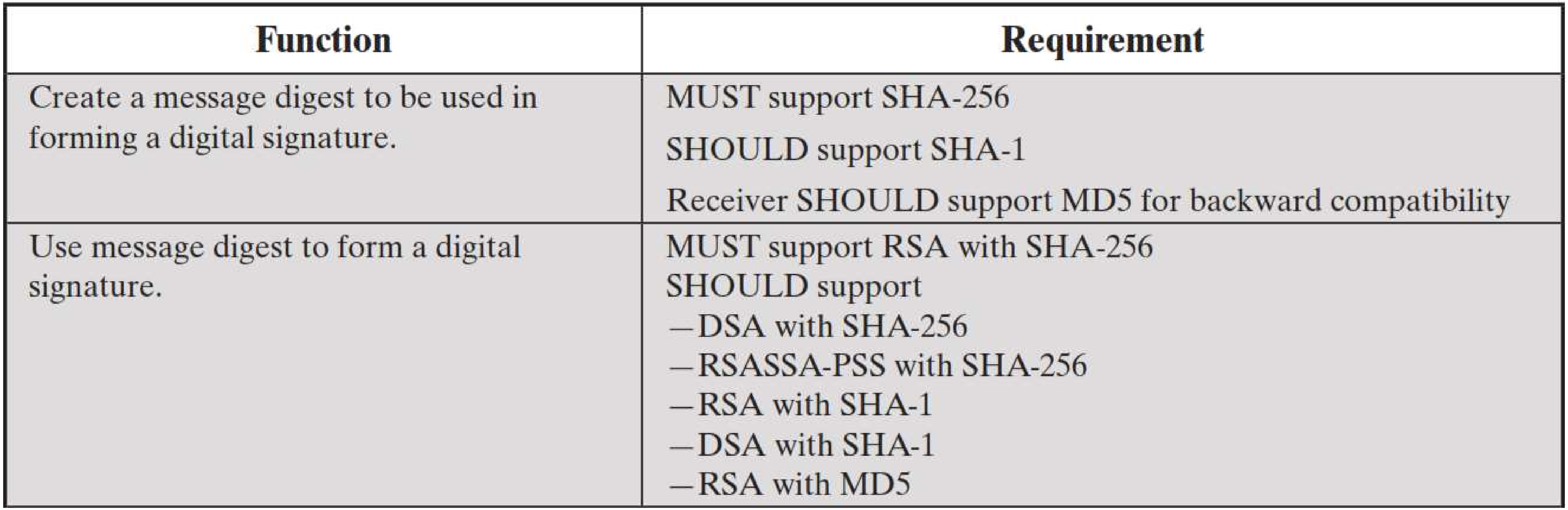
- If encryption is done first, it is possible to verify a signature without exposing the message content. This can be useful in a context in which automatic signature verification is desired, as no private key material is required to verify a signature.
- However, in this case the recipient cannot determine any relationship between the signer and the unencrypted content of the message.

S/MIME Message Content Types

S/MIME uses the following message content types,

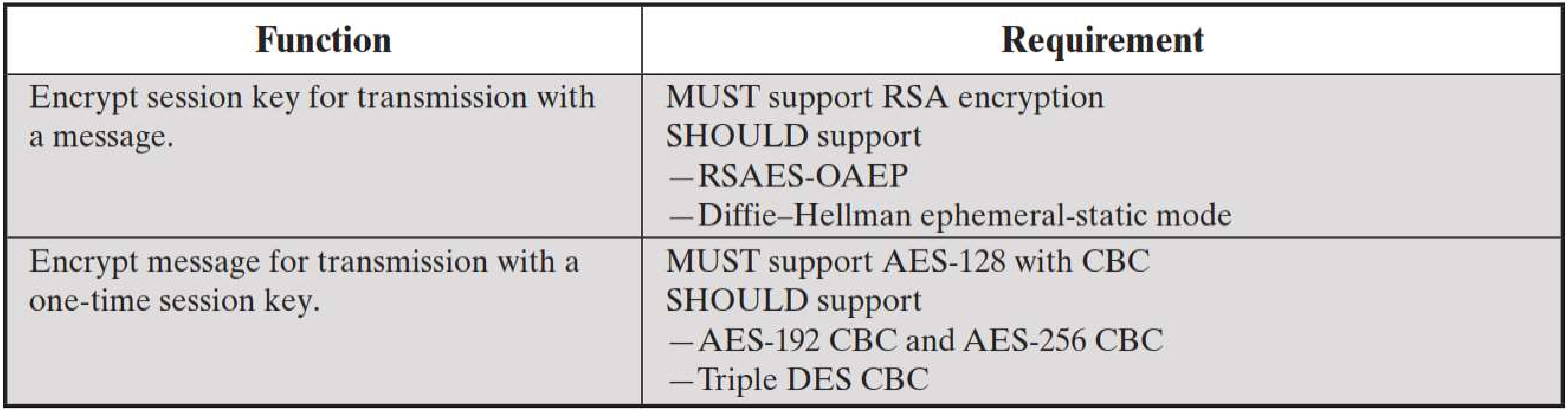
- **Data:** Refers to the inner MIME-encoded message content, which may then be encapsulated in a SignedData, EnvelopedData, or CompressedData content type.
- **SignedData:** Used to apply a digital signature to a message.
- **EnvelopedData:** This consists of encrypted content of any type and encryptedcontent encryption keys for one or more recipients.
- **CompressedData:** Used to apply data compression to a message.

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

Cryptographic Algorithms Used in S/MIME



Function	Requirement
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