What is S/MIME

S/MIME is an acronym for *Secure/Multipurpose Internet Mail Extensions*. It references a type of public encryption and signing of MIME data (a.k.a. email messages) to verify a sender's identity. With S/MIME, it is possible to send and receive encrypted emails.

- ☛ **RFC 822**, developed by IETF & first published in 1982, has defined the standard format of textual mail messages on the Internet.
- ☛ **RFC 5322** is the latest revision of the original Internet Message Format as described in RFC 822, where messages are viewed as having an envelope and contents.
- ☛ RFC 5322 provides a standard way to format internet messages, such as email, through which email systems can interoperate and exchange messages with each other.
- ☛ **Multipurpose Internet Mail Extension (MIME)** 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).

S/MIME is a complex capability that is defined in a number of documents

- **RFC 5750, S/MIME Version 3.2 Certificate Handling**: Specifies conventions for X.509 certificate usage by (S/MIME) v3.2
- **RFC 5751, S/MIME Version 3.2 Message Specification**: The principal defining document for S/MIME message creation and processing.
- **RFC 4134, Examples of S/MIME Messages**: Gives examples of message bodies formatted using S/MIME.
- **RFC 2634, Enhanced Security Services for S/MIME**: Describes four optional security service extensions for S/MIME.
- **RFC 5652, Cryptographic Message Syntax (CMS)**: Describes the CMS. This syntax is used to digitally sign, digest, authenticate, or encrypt arbitrary message content.
- **RFC 3370, CMS Algorithms:** Describes the conventions for using several cryptographic algorithms with the CMS.
- **RFC 5752, Multiple Signatures in CMS**: Describes the use of multiple, parallel signatures for a message.
- **RFC 1847, Security Multiparts for MIME**—Multipart/Signed and Multipart/Encrypted: Defines a framework within which security services may be applied to MIME body parts

S/MIME SERVICES

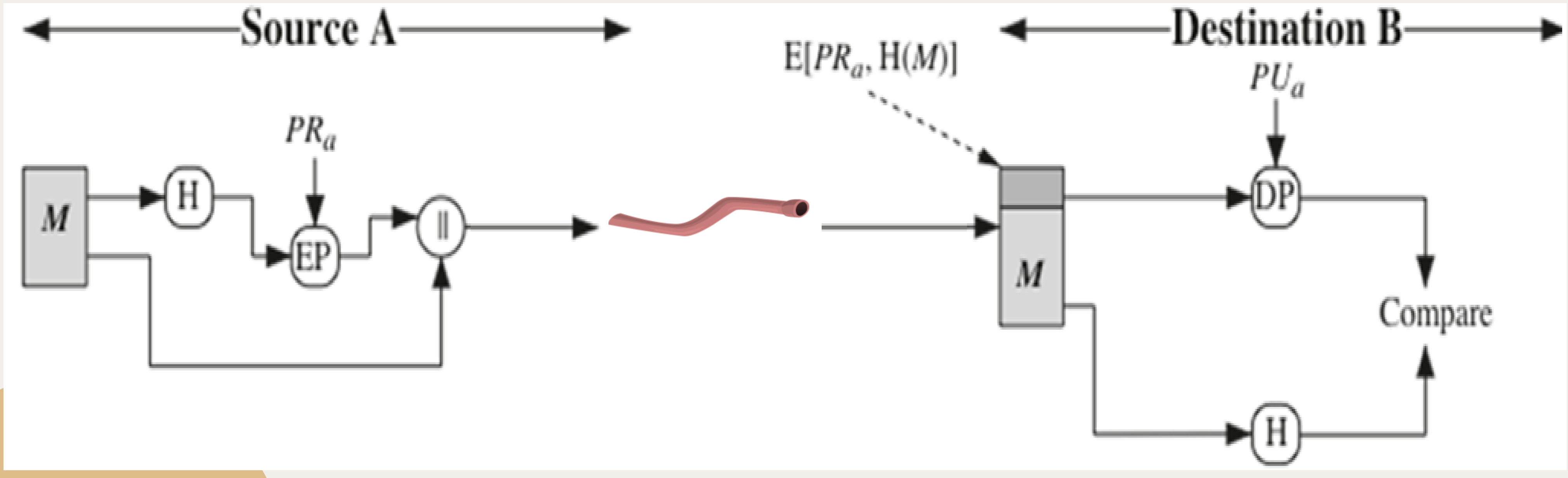
S/MIME provides for four message-related services: **authentication, confidentiality, compression, and email compatibility**.

Authentication

Authentication is provided by means of a digital signature

- Sender creates a message M
- Uses SHA-256 to generate 256-bit hash of message
- Signed hash is generated with RSA using sender's private key, and is attached to message. In addition, identifying information of the signer which enables receiver to retrieve the senders public key is appended.
- Receiver uses RSA with sender's public key to decrypt and recover hash code
- Receiver generates a new hash for the received message and compares it with the decrypted hash code. If it’s a match, then the message is authentic

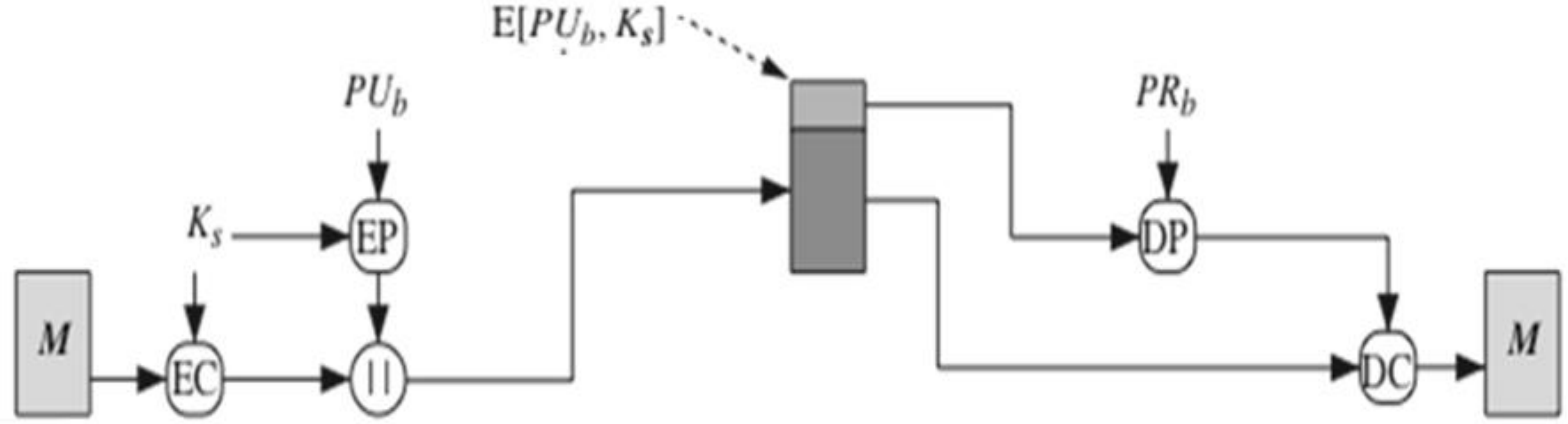
- The combination of SHA-256 and RSA provides an effective digital signature scheme. A recipient can be assured that the message was sent by the person or organization who claims to have sent the message.
- Also, the recipient is assured that the email message that is received is, in fact, the same message that was signed and sent, and has not been altered while in transit.



Confidentiality

- S/MIME provides confidentiality by encrypting messages. Most commonly AES with a 128-bit key is used, with the cipher block chaining (CBC) mode. The key itself is also encrypted with RSA.
- In S/MIME, each symmetric key, referred to as a content-encryption key, is used only once. A new key is generated as a random number for each message and is bound to the message and transmitted along with it. To protect the key, it is encrypted with the receiver's public key.

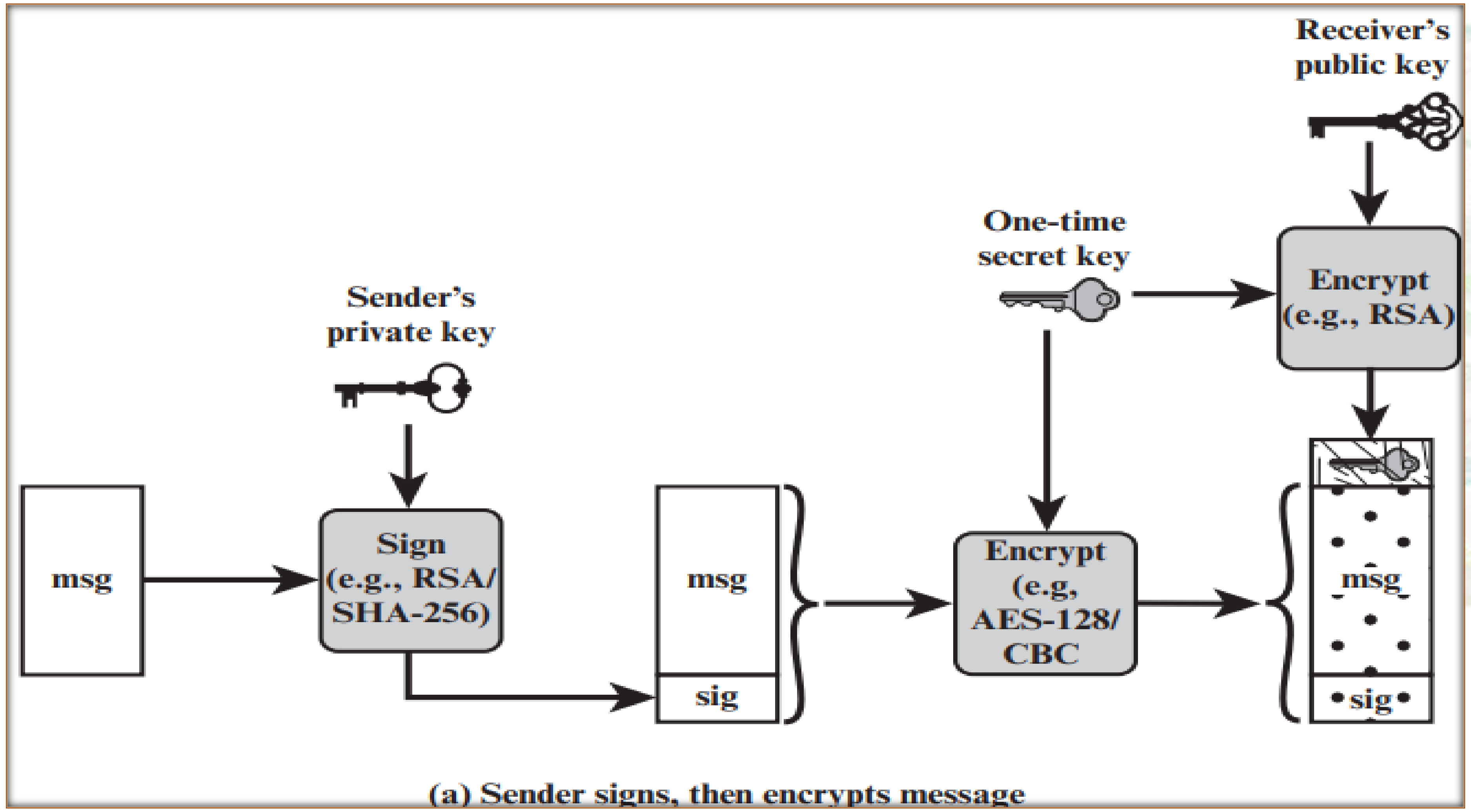
- The sender generates a message and a random 128-bit number to be used as a **content-encryption key** for this message only.
- The message is encrypted using the content-encryption key .
- This key is encrypted with RSA using the recipient's public key and is attached to the message.
- The receiver uses RSA with its private key to decrypt and recover the **content-encryption key.**
- Then the key is used to decrypt the message.



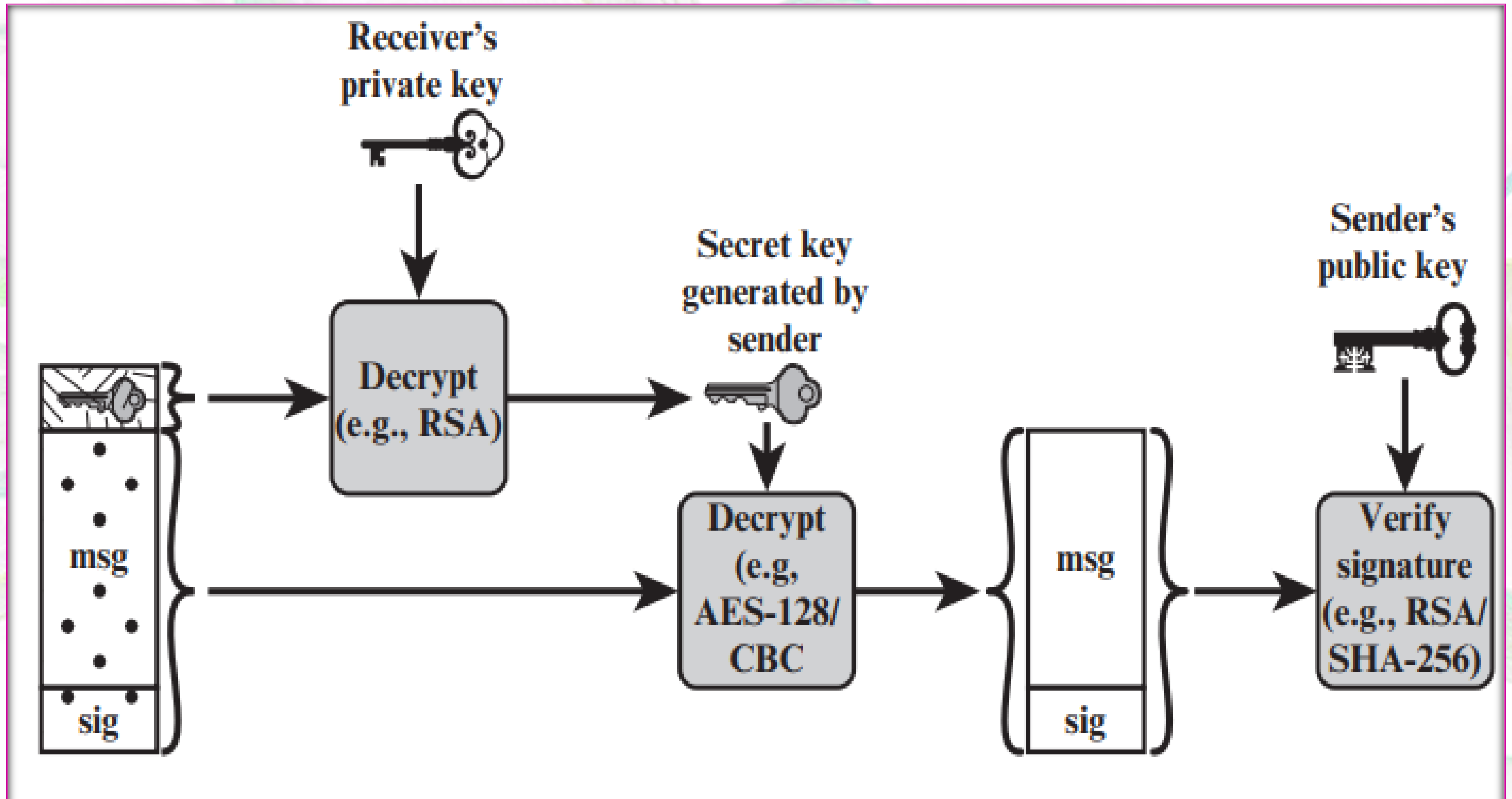
- The combination of symmetric and public-key encryption is used to reduce encryption time.
- Usage of the public-key algorithm solves the session-key distribution problem
- The use of onetime symmetric keys strengthens what is already a strong symmetric encryption approach

Authentication & Confidentiality

- In S/MIME, both confidentiality and authentication can be provided to the same message.
- First, 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.



(a) Sender signs, then encrypts message


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)

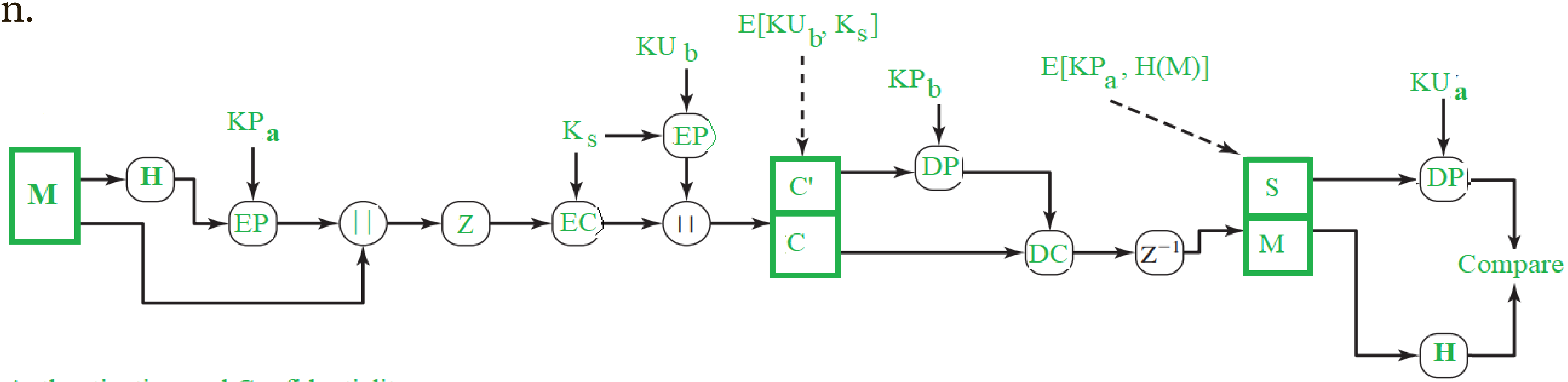
(b) Receiver decrypts message, then verifies sender's signature

EMAIL COMPATIBILITY

- In S/MIME, atleast part of the message is encrypted either the signature part or the message itself.
- Hence, the resultant block to be transmitted always contains a stream of arbitrary octets.
- But, many electronic 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 ASCII characters, a process referred to as 7-bit encoding.
- Base64 conversion, which is used for this process converts each group of three octets of binary data into four ASCII characters.
- Common to all binary-to-text encoding schemes, Base64 is designed to carry data stored in binary formats across channels that only reliably support text content.
- Base64 is also widely used for sending e-mail attachments. This is required because SMTP – in its original form – was designed to transport 7-bit ASCII characters only.

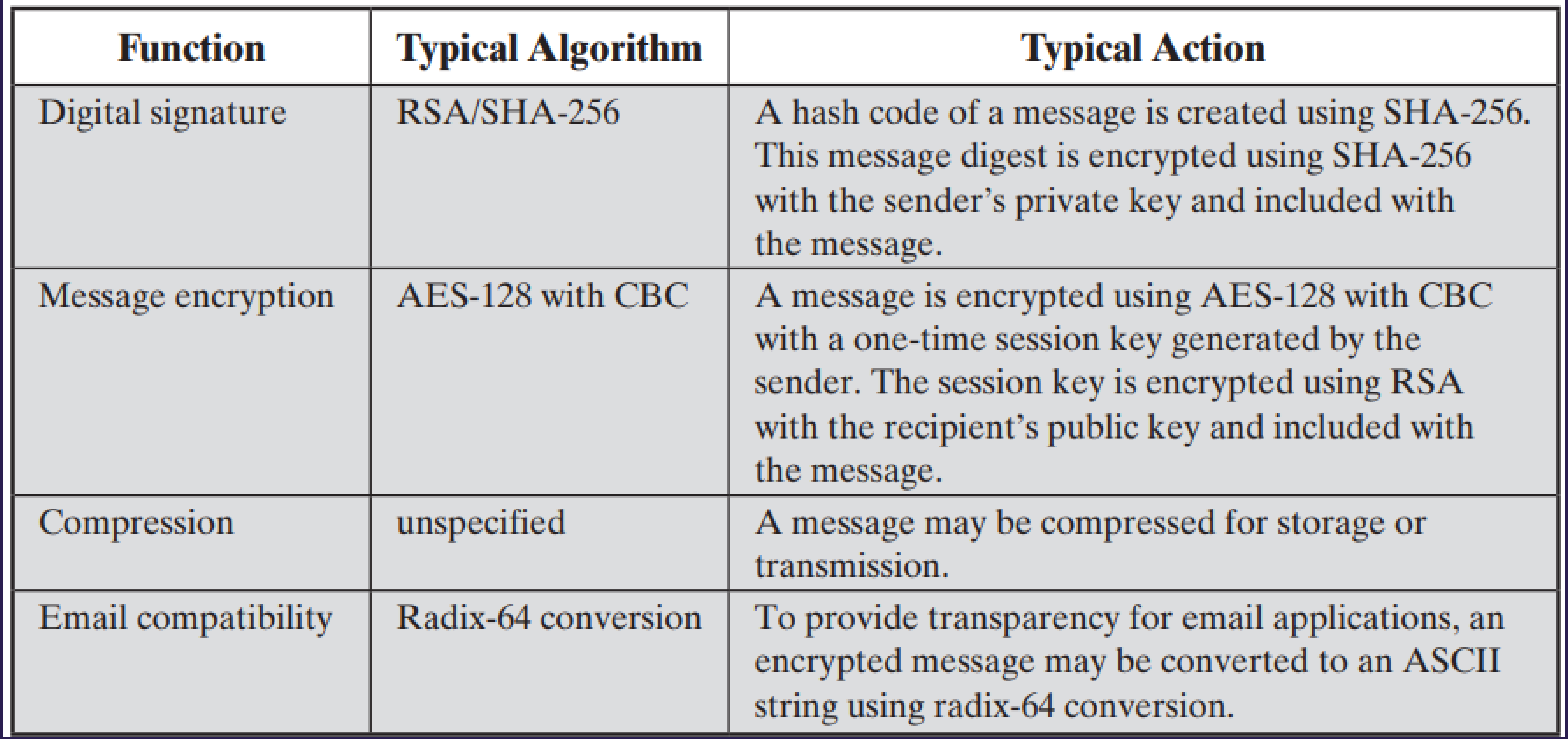
COMPRESSION

- S/MIME also offers the ability to compress a message. This has the benefit of saving space both for email transmission and for file storage.
- Compression can be applied in any order with respect to the signing and message encryption operations.
- RFC 5751 provides the following guidelines:
  - Compression of binary encoded encrypted data is discouraged, since it will not yield significant compression.
  - If a lossy compression algorithm is used with signing, you will need to compress first, then sign.



Authentication and Confidentiality

Summary of S/MIME Services



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.

S/MIME

Message Content Types

S/MIME adds some new content types to include security services to the MIME standard. All these new types include the parameter "application/pkcs7-mime", in which 'pkcs' defines "Public Key Cryptography Specification".

S/MIME provides several content types that can be used to exchange secure email messages. The message content types, defined in RFC 5652, Cryptographic Message Syntax are:

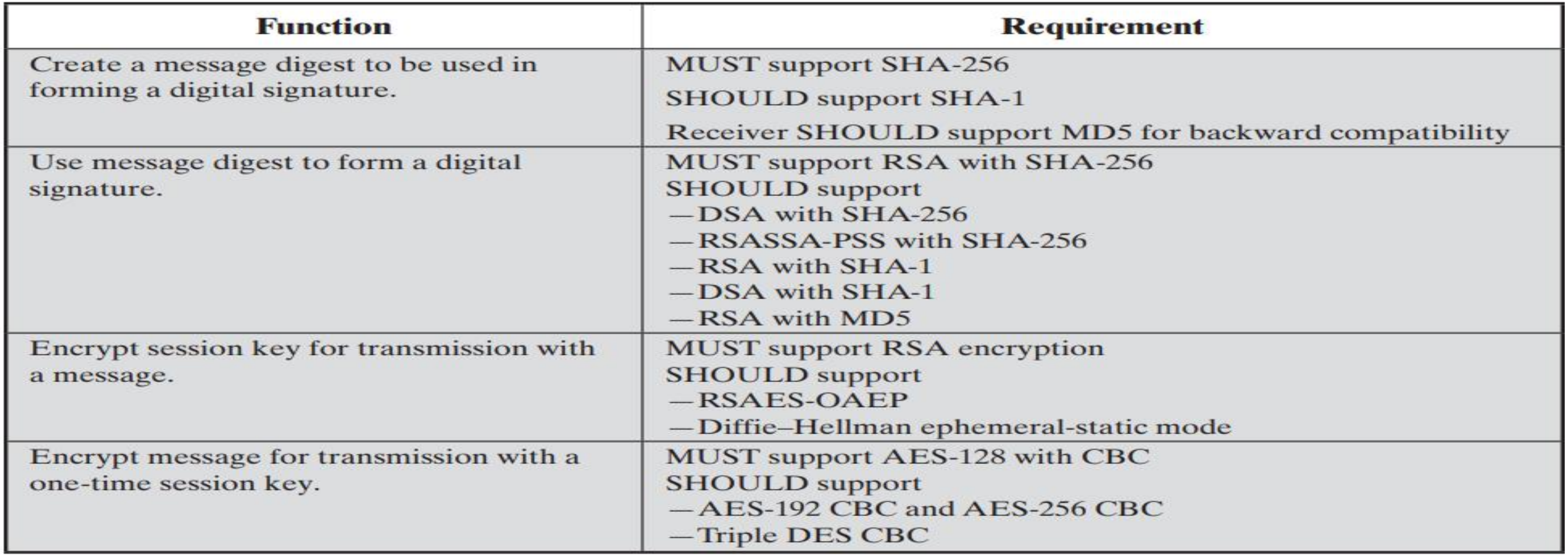
- **Data**
- **SignedData**
- **EnvelopedData**
- **CompressedData**

- **Signed Data:** This content type is used for message authentication and integrity. This consists of a series of blocks, including a message digest algorithm identifier, the message being signed, and SignerInfo.
- **Enveloped Data**: This content type is used for encryption and decryption of email messages. It contains the encrypted message and the encrypted-content encryption keys for one or more recipients.
- **Clear-Signed Data**: This content type is used to sign the message body and header separately. It allows the recipient to verify the authenticity and integrity of the message body without the need for decryption.
- **Compressed Data**: This content type is used for compressing the email message before sending it. It reduces the size of the message, making it faster to transmit.
- **Signed and Enveloped Data**: This content type combines the functionalities of Signed Data and Enveloped Data. It provides both confidentiality and message integrity in one package.

S/MIME - Approved Cryptographic Algorithms

S/MIME uses the following terminology taken from RFC 2119 (Key Words for use in RFCs to Indicate Requirement Levels, March 1997) to specify the requirement level:

- MUST: The definition is an absolute requirement of the specification. An implementation must include this feature or function to be in conformance with the specification.
- SHOULD: There may exist valid reasons in particular circumstances to ignore this feature or function, but it is recommended that an implementation include the feature or function.



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

According to S/MIME specification, a sending agent has two decisions to make. First, the sending agent must determine if the receiving agent is capable of decrypting using a given encryption algorithm. Second, if the receiving agent is only capable of accepting weakly encrypted content, the sending agent must decide if it is acceptable to send using weak encryption. To support this decision process, a sending agent may announce its decrypting capabilities in order of preference for any message that it sends out. A receiving agent may store that information for future use.