Appendix 1
Supported Algorithms for PGP and OpenSSL

GPG Version 1.6 supported algorithms:

Public key	RSA, RSA-E, RSA-S, ELG-E, DSA
Symmetric ciphers	3DES, CAST5, BLOWFISH, AES, AES192, AES256, TWOFISH, CAMELLIA128, CAMELLIA192, CAMELLIA256
Hash function (MDC)	MD5, SHA1, RIPEMD160, SHA256, SHA384, SHA512, SHA224

There are OpenPGP extensions for elliptic curve methods that offer much faster public key methods while retaining excellent security. The acceptance of elliptic curves has been moving very slowly, but GPG version 2 now supports them.

GPG Version 2.1.2 supported algorithms

Public key	RSA, ELG, DSA, ECDH, ECDSA, EdDSA
Symmetric ciphers	IDEA, 3DES, CAST5, BLOWFISH, AES, AES192, AES256, TWOFISH, CAMELLIA128, CAMELLIA192, CAMELLIA256
Hash function (MDC)	SHA1, RIPEMD160, SHA256, SHA384, SHA512, SHA224

OpenSSL also has a wide range of ciphers. These are arranged into "cipher suites" in which the three essential algorithms, public key, symmetric cipher, and hash function, are specified as a group.

OpenSSL 0.9.8o 01 Jun 2010

Suite name	vr	Key exchange	Authentication, encryption, hash	Export?
DHE-RSA-AES256-SHA	3	DH	Au=RSA Enc=AES(256) Mac=SHA1	
DHE-DSS-AES256-SHA	3	DH	Au=DSS Enc=AES(256) Mac=SHA1	

(continued)

H. Orman, *Encrypted Email*,
SpringerBriefs in Computer Science,
DOI 10.1007/978-3-319-21344-6

Suite name	vr	Key exchange	Authentication, encryption, hash	Export?
AES256-SHA	3	RSA	Au=RSA Enc=AES(256) Mac=SHA1	
EDH-RSA-DES-CBC3-SHA	3	DH	Au=RSA Enc=3DES (168) Mac=SHA1	
EDH-DSS-DES-CBC3-SHA	3	DH	Au=DSS Enc=3DES (168) Mac=SHA1	
DES-CBC3-SHA	3	RSA	Au=RSA Enc=3DES (168) Mac=SHA1	
DES-CBC3-MD5	2	RSA	Au=RSA Enc=3DES (168) Mac=MD5	
DHE-RSA-AES128-SHA	3	DH	Au=RSA Enc=AES(128) Mac=SHA1	
DHE-DSS-AES128-SHA	3	DH	Au=DSS Enc=AES(128) Mac=SHA1	
AES128-SHA	3	RSA	Au=RSA Enc=AES(128) Mac=SHA1	
RC2-CBC-MD5	2	RSA	Au=RSA Enc=RC2(128) Mac=MD5	
RC4-SHA	3	RSA	Au=RSA Enc=RC4(128) Mac=SHA1	
RC4-MD5	3	RSA	Au=RSA Enc=RC4(128) Mac=MD5	
RC4-MD5	2	RSA	Au=RSA Enc=RC4(128) Mac=MD5	
EDH-RSA-DES-CBC-SHA	3	DH	Au=RSA Enc=DES(56) Mac=SHA1	
EDH-DSS-DES-CBC-SHA	3	DH	Au=DSS Enc=DES(56) Mac=SHA1	
DES-CBC-SHA	3	RSA	Au=RSA Enc=DES(56) Mac=SHA1	
DES-CBC-MD5	2	RSA	Au=RSA Enc=DES(56) Mac=MD5	
EXP-EDH-RSA-DES-CBC-SHA	3	DH(512)	Au=RSA Enc=DES(40) Mac=SHA1	Yes
EXP-EDH-DSS-DES-CBC-SHA	3	DH(512)	Au=DSS Enc=DES(40) Mac=SHA1	Yes
EXP-DES-CBC-SHA	3	RSA (512)	Au=RSA Enc=DES(40) Mac=SHA1	Yes
EXP-RC2-CBC-MD5	3	RSA (512)	Au=RSA Enc=RC2(40) Mac=MD5	Yes
EXP-RC2-CBC-MD5	2	RSA (512)	Au=RSA Enc=RC2(40) Mac=MD5	Yes
EXP-RC4-MD5	3	RSA (512)	Au=RSA Enc=RC4(40) Mac=MD5	Yes
EXP-RC4-MD5	2	RSA (512)	Au=RSA Enc=RC4(40) Mac=MD5	Yes

OpenSSL v3 1.0.1f 6 Jan 2014

Suite name	Key exchange	Authentication, encryption, hash
ECDHE-RSA-AES256-SHA	ECDH	Au=RSA Enc=AES(256) Mac=SHA1
ECDHE-ECDSA-AES256-SHA	ECDH	Au=ECDSA Enc=AES(256) Mac=SHA1
SRP-DSS-AES-256-CBC-SHA	SRP	Au=DSS Enc=AES(256) Mac=SHA1
SRP-RSA-AES-256-CBC-SHA	SRP	Au=RSA Enc=AES(256) Mac=SHA1
SRP-AES-256-CBC-SHA	SRP	Au=SRP Enc=AES(256) Mac=SHA1
DHE-RSA-AES256-SHA	DH	RSA Enc=AES(256) Mac=SHA1
DHE-DSS-AES256-SHA	DH	DSS Enc=AES(256) Mac=SHA1
DHE-RSA-CAMELLIA256-SHA	DH	RSA Enc=Camellia(256) Mac=SHA1
DHE-DSS-CAMELLIA256-SHA	DH	DSS Enc=Camellia(256) Mac=SHA1
ECDH-RSA-AES256-SHA	ECDH/RSA	Au=ECDH Enc=AES(256) Mac=SHA1
ECDH-ECDSA-AES256-SHA	ECDH/ECDSA	Au=ECDH Enc=AES(256) Mac=SHA1
AES256-SHA	RSA	RSA Enc=AES(256) Mac=SHA1
CAMELLIA256-SHA	RSA	RSA Enc=Camellia(256) Mac=SHA1
PSK-AES256-CBC-SHA	PSK	Au=PSK Enc=AES(256) Mac=SHA1
ECDHE-RSA-DES-CBC3-SHA	ECDH	Au=RSA Enc=3DES(168) Mac=SHA1
ECDHE-ECDSA-DES-CBC3-SHA	ECDH	Au=ECDSA Enc=3DES(168) Mac=SHA1
SRP-DSS-3DES-EDE-CBC-SHA	SRP	Au=DSS Enc=3DES(168) Mac=SHA1
SRP-RSA-3DES-EDE-CBC-SHA	SRP	Au=RSA Enc=3DES(168) Mac=SHA1
SRP-3DES-EDE-CBC-SHA	SRP	Au=SRP Enc=3DES(168) Mac=SHA1
EDH-RSA-DES-CBC3-SHA	DH	Au=RSA Enc=3DES(168) Mac=SHA1
EDH-DSS-DES-CBC3-SHA	DH	Au=DSS Enc=3DES(168) Mac=SHA1
ECDH-RSA-DES-CBC3-SHA	ECDH/RSA	Au=ECDH Enc=3DES(168) Mac=SHA1
ECDH-ECDSA-DES-CBC3-SHA	ECDH/ECDSA	Au=ECDH Enc=3DES(168) Mac=SHA1

(continued)

Suite name	Key exchange	Authentication, encryption, hash
DES-CBC3-SHA	RSA	Au=RSA Enc=3DES(168) Mac=SHA1
PSK-3DES-EDE-CBC-SHA	PSK	PSK Enc=3DES(168) Mac=SHA1
ECDHE-RSA-AES128-SHA	ECDH	Au=RSA Enc=AES(128) Mac=SHA1
ECDHE-ECDSA-AES128-SHA	ECDH	Au=ECDSA Enc=AES(128) Mac=SHA1
SRP-DSS-AES-128-CBC-SHA	SRP	DSS Enc=AES(128) Mac=SHA1
SRP-RSA-AES-128-CBC-SHA	SRP	RSA Enc=AES(128) Mac=SHA1
SRP-AES-128-CBC-SHA	SRP	SRP Enc=AES(128) Mac=SHA1
DHE-RSA-AES128-SHA	DH	RSA Enc=AES(128) Mac=SHA1
DHE-DSS-AES128-SHA	DH	DSS Enc=AES(128) Mac=SHA1
DHE-RSA-SEED-SHA	DH	RSA Enc=SEED(128) Mac=SHA1
DHE-DSS-SEED-SHA	DH	DSS Enc=SEED(128) Mac=SHA1
DHE-RSA-CAMELLIA128-SHA	DH	RSA Enc=Camellia(128) Mac=SHA1
DHE-DSS-CAMELLIA128-SHA	DH	DSS Enc=Camellia(128) Mac=SHA1
ECDH-RSA-AES128-SHA	ECDH/RSA	Au=ECDH Enc=AES(128) Mac=SHA1
ECDH-ECDSA-AES128-SHA	ECDH/ECDSA	Au=ECDH Enc=AES(128) Mac=SHA1
AES128-SHA	RSA	RSA Enc=AES(128) Mac=SHA1
SEED-SHA	RSA	RSA Enc=SEED(128) Mac=SHA1
CAMELLIA128-SHA	RSA	RSA Enc=Camellia(128) Mac=SHA1
PSK-AES128-CBC-SHA	PSK	PSK Enc=AES(128) Mac=SHA1
ECDHE-RSA-RC4-SHA	ECDH	Au=RSA Enc=RC4(128) Mac=SHA1
ECDHE-ECDSA-RC4-SHA	ECDH	Au=ECDSA Enc=RC4(128) Mac=SHA1
ECDH-RSA-RC4-SHA	ECDH/RSA	Au=ECDH Enc=RC4(128) Mac=SHA1
ECDH-ECDSA-RC4-SHA	ECDH/ECDSA	Au=ECDH Enc=RC4(128) Mac=SHA1
RC4-SHA	RSA	RSA Enc=RC4(128) Mac=SHA1
RC4-MD5	RSA	RSA Enc=RC4(128) Mac=MD5
PSK-RC4-SHA	PSK	PSK Enc=RC4(128) Mac=SHA1
EDH-RSA-DES-CBC-SHA	DH	RSA Enc=DES(56) Mac=SHA1
EDH-DSS-DES-CBC-SHA	DH	DSS Enc=DES(56) Mac=SHA1
DES-CBC-SHA	RSA	RSA Enc=DES(56) Mac=SHA1
EXP-EDH-RSA-DES-CBC-SHA[a]	DH(512)	Au=RSA Enc=DES(40) Mac=SHA1

(continued)

Suite name	Key exchange	Authentication, encryption, hash
EXP-EDH-DSS-DES-CBC-SHA[a]	DH(512)	Au=DSS Enc=DES(40) Mac=SHA1
EXP-DES-CBC-SHA[a]	RSA(512)	Au=RSA Enc=DES(40) Mac=SHA1
EXP-RC2-CBC-MD5[a]	RSA(512)	RSA Enc=RC2(40) Mac=MD5
EXP-RC4-MD5[a]	RSA(512)	RSA Enc=RC4(40) Mac=MD5

[a]Exportable

Appendix 2
ASN.1 Definition of an S/MIME Message Part

This gives some idea of how the Cryptographic Message Syntax is embodied in S/MIME messages. The first line shows the sequence of values that indicate that what follows is encoded for S/MIME version 3.1. From IETF RFC5911, "New ASN.1 Modules for Cryptographic Message Syntax (CMS) and S/MIME", by P. Hoffman and J. Schaad, June 2010.

```
SecureMimeMessageV3dot1
  { iso(1) member-body(2) us(840) rsadsi(113549)
         pkcs(1) pkcs-9(9) smime(16) modules(0) msg-v3dot1(21) }

DEFINITIONS IMPLICIT TAGS ::=
BEGIN

IMPORTS
-- Cryptographic Message Syntax
    SubjectKeyIdentifier, IssuerAndSerialNumber,
    RecipientKeyIdentifier
        FROM    CryptographicMessageSyntax
               { iso(1) member-body(2) us(840) rsadsi(113549)
                 pkcs(1) pkcs-9(9) smime(16) modules(0) cms-2001(14) };


--  id-aa is the arc with all new authenticated and unauthenticated
--  attributes produced the by S/MIME Working Group

id-aa OBJECT IDENTIFIER ::= {iso(1) member-body(2) usa(840)
        rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) attributes(2)}

-- S/MIME Capabilities provides a method of broadcasting the symmetric
-- capabilities understood.  Algorithms SHOULD be ordered by
-- preference and grouped by type

smimeCapabilities OBJECT IDENTIFIER ::=
   {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) 15}
```


H. Orman, *Encrypted Email*,
SpringerBriefs in Computer Science,
DOI 10.1007/978-3-319-21344-6

```
SMIMECapability ::= SEQUENCE {
   capabilityID OBJECT IDENTIFIER,
   parameters ANY DEFINED BY capabilityID OPTIONAL }

SMIMECapabilities ::= SEQUENCE OF SMIMECapability

-- Encryption Key Preference provides a method of broadcasting the
-- preferred encryption certificate.

id-aa-encrypKeyPref OBJECT IDENTIFIER ::= {id-aa 11}

SMIMEEncryptionKeyPreference ::= CHOICE {
   issuerAndSerialNumber   [0] IssuerAndSerialNumber,
   receipentKeyId          [1] RecipientKeyIdentifier,
   subjectAltKeyIdentifier [2] SubjectKeyIdentifier
}
```

Appendix 3
IETF Documents for S/MIME Mail Security

This information is from the IETF website in the section for the smime working group. It shows the complete history of documents produced by the group. Note that some documents have several versions, and some have been rendered obsolete.

Document	Date	Status
RFC 2630 Cryptographic Message Syntax	1999-06 60 pages	Proposed Standard RFC Obsoleted by RFC3369, RFC3370 IETF RFC stream
RFC 2631 Diffie-Hellman Key Agreement Method	1999-06 13 pages	Proposed Standard RFC IETF RFC stream
RFC 2632 S/MIME Version 3 Certificate Handling	1999-06 13 pages	Proposed Standard RFC Obsoleted by RFC3850 IETF RFC stream
RFC 2633 S/MIME Version 3 Message Specification	1999-06 32 pages	Proposed Standard RFC Obsoleted by RFC3851 IETF RFC stream
RFC 2634 Enhanced Security Services for S/MIME	1999-06 58 pages	Proposed Standard RFC Updated by RFC5035 IETF RFC stream
RFC 2785 Methods for Avoiding the “Small-Subgroup” Attacks on the Diffie-Hellman Key Agreement Method for S/MIME	2000-03 11 pages	Informational RFC IETF RFC stream
RFC 2876 Use of the KEA and SKIPJACK Algorithms in CMS	2000-07 13 pages	Informational RFC IETF RFC stream

(continued)

H. Orman, *Encrypted Email*,
SpringerBriefs in Computer Science,
DOI 10.1007/978-3-319-21344-6

Document	Date	Status
RFC 2984 Use of the CAST-128 Encryption Algorithm in CMS	2000-10 6 pages	Proposed Standard RFC IETF RFC stream
RFC 3058 Use of the IDEA Encryption Algorithm in CMS	2001-02 8 pages	Informational RFC IETF RFC stream
RFC 3114 Implementing Company Classification Policy with the S/MIME Security Label	2002-05 14 pages	Informational RFC IETF RFC stream
RFC 3125 Electronic Signature Policies	2001-09 44 pages	Experimental RFC WG Document
RFC 3126 Electronic Signature Formats for long term electronic signatures	2001-09 84 pages	Informational RFC Obsoleted by RFC5126 WG Document
RFC 3183 Domain Security Services using S/MIME	2001-10 24 pages	Experimental RFC IETF RFC stream
RFC 3185 Reuse of CMS Content Encryption Keys	2001-10 10 pages	Proposed Standard RFC IETF RFC stream
RFC 3211 Password-based Encryption for CMS	2001-12 17 pages	Proposed Standard RFC Obsoleted by RFC3369, RFC3370 IETF RFC stream
RFC 3217 Triple-DES and RC2 Key Wrapping	2001-12 9 pages	Informational RFC IETF RFC stream
RFC 3218 Preventing the Million Message Attack on Cryptographic Message Syntax	2002-01 7 pages	Informational RFC IETF RFC stream
RFC 3274 Compressed Data Content Type for Cryptographic Message Syntax (CMS)	2002-06 6 pages	Proposed Standard RFC IETF RFC stream
RFC 3278 Use of Elliptic Curve Cryptography (ECC) Algorithms in Cryptographic Message Syntax (CMS)	2002-05 16 pages	Informational RFC Obsoleted by RFC5753 IETF RFC stream
RFC 3369 Cryptographic Message Syntax (CMS)	2002-09 52 pages	Proposed Standard RFC Obsoleted by RFC3852 IETF RFC stream
RFC 3370 Cryptographic Message Syntax (CMS) Algorithms Errata	2002-09 24 pages	Proposed Standard RFC Updated by RFC5754 IETF RFC stream

(continued)

Document	Date	Status
RFC 3394 Advanced Encryption Standard (AES) [2] Key Wrap Algorithm Errata	2002-10 41 pages	Informational RFC IETF RFC stream
RFC 3537 Wrapping a Hashed Message Authentication Code (HMAC) key with a Triple-Data Encryption Standard (DES) [5] Key or an Advanced Encryption Standard (AES) Key	2003-05 9 pages	Proposed Standard RFC IETF RFC stream
RFC 3560 Use of the RSAES-OAEP Key Transport Algorithm in Cryptographic Message Syntax (CMS)	2003-07 18 pages	Proposed Standard RFC IETF RFC stream
RFC 3565 Use of the Advanced Encryption Standard (AES) Encryption Algorithm in Cryptographic Message Syntax (CMS)	2003-07 14 pages	Proposed Standard RFC IETF RFC stream
RFC 3657 Use of the Camellia Encryption Algorithm in Cryptographic Message Syntax (CMS)	2004-01 14 pages	Proposed Standard RFC IETF RFC stream
RFC 3850 (was draft-ietf-smime-rfc2632bis) Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Certificate Handling	2004-07 16 pages	Proposed Standard RFC Obsoleted by RFC5750 IETF RFC stream
RFC 3851 Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification	2004-07 36 pages	Proposed Standard RFC Obsoleted by RFC5751 IETF RFC stream
RFC 3852 Cryptographic Message Syntax (CMS)	2004-07 56 pages	Proposed Standard RFC Obsoleted by RFC5652 Updated by RFC4853, RFC5083 IETF RFC stream
RFC 3854 Securing X.400 Content with Secure/Multipurpose Internet Mail Extensions (S/MIME)	2004-07 15 pages	Proposed Standard RFC IETF RFC stream
RFC 3855 Transporting Secure/Multipurpose Internet Mail Extensions (S/MIME) Objects in X.400	2004-07 12 pages	Proposed Standard RFC IETF RFC stream
RFC 4010 Use of the SEED Encryption Algorithm in Cryptographic Message Syntax (CMS)	2005-02 13 pages	Proposed Standard RFC IETF RFC stream
RFC 4056 Use of the RSASSA-PSS Signature Algorithm in Cryptographic Message Syntax (CMS)	2005-06 6 pages	Proposed Standard RFC WG Document

(continued)

Document	Date	Status
RFC 4134 Examples of S/MIME Messages	2005-07 136 pages	Informational RFC IETF RFC stream
RFC 4262 X.509 Certificate Extension for Secure/Multipurpose Internet Mail Extensions (S/MIME) Capabilities	2005-12 5 pages	Proposed Standard RFC IETF RFC stream
RFC 4490 Using the GOST 28147-89, GOST R 34.11-94, GOST R 34.10-94, and GOST R 34.10-2001 Algorithms with Cryptographic Message Syntax (CMS)	2006-05 29 pages	Proposed Standard RFC IETF RFC stream
RFC 4853 Cryptographic Message Syntax (CMS) Multiple Signer Clarification	2007-04 5 pages	Proposed Standard RFC IETF RFC stream
RFC 5035 Enhanced Security Services (ESS) Update: Adding CertID Algorithm Agility	2007-08 17 pages	Proposed Standard RFC IETF RFC stream
RFC 5083 Cryptographic Message Syntax (CMS) Authenticated-Enveloped-Data Content Type	2007-11 10 pages	Proposed Standard RFC IETF RFC stream
RFC 5084 Using AES-CCM and AES-GCM Authenticated Encryption in the Cryptographic Message Syntax (CMS)	2007-11 11 pages	Proposed Standard RFC IETF RFC stream
RFC 5126 CMS Advanced Electronic Signatures (CAdES)	2008-03 141 pages	Informational RFC WG Document
RFC 5275 CMS Symmetric Key Management and Distribution	2008-06 89 pages	Proposed Standard RFC IETF RFC stream
RFC 5408 Identity-Based Encryption Architecture and Supporting Data Structures	2009-01 30 pages	Informational RFC IETF RFC stream
RFC 5409 Using the Boneh-Franklin and Boneh-Boyen Identity-Based Encryption Algorithms with the Cryptographic Message Syntax (CMS)	2009-01 13 pages	Informational RFC IETF RFC stream
RFC 562 Cryptographic Message Syntax (CMS)	2009-09 56 pages	Internet Standard RFC IETF RFC stream
RFC 5750 Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Certificate Handling	2010-01 21 pages	Proposed Standard RFC IETF RFC stream
RFC 5751 Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification	2010-01 45 pages	Proposed Standard RFC IETF RFC stream
RFC 5752 Multiple Signatures in Cryptographic Message Syntax (CMS) Errata	2010-01 17 pages	Proposed Standard RFC WG Document

(continued)

Document	Date	Status
RFC 5753 Use of Elliptic Curve Cryptography (ECC) Algorithms in Cryptographic Message Syntax (CMS)	2010-01 61 pages	Informational RFC IETF RFC stream
RFC 5754 Using SHA2 Algorithms with Cryptographic Message Syntax Errata	2010-01 10 pages	Proposed Standard RFC IETF RFC stream
RFC 5911 New ASN.1 Modules for Cryptographic Message Syntax (CMS) and S/MIME Errata	2010-06 59 pages	Informational RFC Updated by RFC6268 IETF RFC stream
RFC 5990 Use of the RSA-KEM Key Transport Algorithm in the Cryptographic Message Syntax (CMS)	2010-09 27 pages	Proposed Standard RFC IETF RFC stream
Related documents		
draft-melnikov-smime-header-signing-02 Considerations for protecting Email header with S/MIME	2015-04-03 6 pages	I-D Exists
draft-melnikov-smime-msa-to-mda-04 Domain-based signing and encryption using S/MIME	2014-03-05 26 pages	Waiting for Writeup for 414 days Proposed Standard Submitted to IESG for Publication

Appendix: OpenPGP, Internet RFCs

Document	Date	Status
RFC 2440 OpenPGP Message Format	1998-11 65 pages	Proposed Standard RFC Obsoleted by RFC4880 IETF RFC stream
RFC 3156 MIME Security with OpenPGP	2001-08 15 pages	Proposed Standard RFC IETF RFC stream
RFC 4880 OpenPGP Message Format	2007-11 90 pages	Proposed Standard RFC Updated by RFC5581 IETF RFC stream
Related documents		
draft-atkins-openpgp-algebraic-eraser-04 Using Algebraic Eraser (AEDH) in OpenPGP	2015-01-14 12 pages	
draft-atkins-openpgp-device-certificates-02 OpenPGP Extensions for Device Certificates	2014-12-08 9 pages	
draft-vb-openpgp-linked-ids-00 Linked Identites for OpenPGP	2015-04-15 New 9 pages	
draft-vb-openpgp-uri-attribute-00 URI Attributes for OpenPGP	2015-04-11 New 4 pages	

Bibliography

1. Adams C, Lloyd S (1999) Understanding public-key infrastructure: concepts, standards, and deployment considerations. New Riders Publishing. ISBN 1-57870-166-x
2. Advanced Encryption Standard (2001) Federal information processing standards publication 197, November 26
3. Bell DE, LaPadula LJ (1974) Secure Computer Systems. Mathematical foundations and model M74–244, MITRE Corp., Bedford, Mass
4. Boneh D, Franklin M (2003) Identity based encryption from the Weil pairing. SIAM J Comput 32(3):586–615. Extended abstract in proc. of Crypto '2001, LNCS 2139:213–229. Springer-Verlag. 2001
5. Data Encryption Standard (1977) NIST, FIPS-46
6. Deutsch DP, Dodds DW (1979) Hermes system overview, BBN report No. 4115
7. Diffie W, Hellman ME (1977) Special feature exhaustive cryptanalysis of the NBS data encryption standard. Computer 10(6):74–84
8. Diffie W, Hellman ME (1976) New directions in cryptography. IEEE transactions on information theory, vol IT-22, No. 6
9. Dingledine R, Mathewson N, Syverson P (2004) Tor: the second-generation onion router. In: Proceedings of the 13th conference on USENIX security symposium, vol 13. USENIX Association, San Diego, CA, pp 21
10. FIPS (2009) Digital signature standard, NIST, FIPS publication 186–3. [This has been superseded by FIPS 186-4]
11. FIPS (2014) NIST, Draft FIPS 202, SHA-3 standard: permutation-based hash and extendable-output functions
12. Foer J (2012) Moonwalking with Einstein: the art and science of remembering everything. Penguin Books, Reprint edition, Paperback: 320 pages. ISBN-10: 9780143120537, ISBN-13: 978-0143120537, ASIN: 0143120530
13. Heninger N, Durumeric Z, Wustrow E, Halderman JA (2012) Mining your {p}s and {q}s: {d}etection of widespread weak keys in network devices. In: Proceedings of the 21st {USENIX} security symposium
14. Hoffman P (2002) IETF RFC 3207, SMTP service extension for secure SMTP over transport layer security
15. Housley R (2009) IETF RFC5652, cryptographic message syntax
16. Kahn D (1967) The code breakers. MacMillan Publishing Company. ISBN 0-020560460-0
17. Kallander JW, Goodwin NC, Hosmer S, Smith C, Fralick D (1979) Military message experiment, mid experiment report. Memorandum rept. Nov 78-Mar 79, DTIC (Defense Techical Information Center) Accession Number: ADA079889
18. Kent ST (1995) Internet Privacy Enhanced Mail. In: Marshall D, Abrams SJ, Podell HJ (eds) Information security: an integrated collection of essay's. IEEE Computer Society Press, Los Alamitos, California, USA. ISBN 0-8186-3662-9, LoC CIP: 94-20899, DDN: QA76.9. A25I5415

H. Orman, *Encrypted Email*,
SpringerBriefs in Computer Science,
DOI 10.1007/978-3-319-21344-6

19. Kohnfelder L (1978) Towards a practical public key system, MIT. B.S. Thesis
20. Kurtz A. What apple missed to fix in iOS 7.1.1. http://www.andreas-kurtz.de/2014/04/what-apple-missed-to-fix-in-ios-711.html
21. Linde RL, Chaney PE (1966) Operational management of time-sharing systems in ACM '66: Proceedings of the 1966 21st National Conference, pp 149–159. ACM, New York, NY. doi:10.1145/800256. 810691
22. Linn J (1993) IETF RFC 1421, privacy enhancement for internet electronic mail: part i: message encryption and authentication procedures
23. Matsui M, Nakajima J, Moriai S (2004) IETF RFC 3713, a description of the Camellia Encryption Algorithm
24. Merkle R, Hellman M (1978) Hiding information and signatures in trapdoor knapsacks. Inf Theory, IEEE Trans 24(5):525–530
25. Nelson R, Heimann J (1990) Advances in cryptology—CRYPTO' 89 proceedings. In: Brassard G (eds) Lecture notes in computer science, SDNS architecture and end-to-end encryption, vol 435. Springer, New York, pp 356–366
26. Ramsdell B, Turner S (2010) IETF RFC 5751, secure/multipurpose internet mail extensions (S/MIME) version 3.2, message specification
27. Rivest RL, Shamir A, Adleman L (1978) A method for obtaining digital signatures and public-key cryptosystems. Commun ACM 21(2):120–126
28. Schneier B (1996) Applied cryptography, 2nd edn. John Wiley and Sons. ISBN 0-471-12845-7
29. Short history of study group 17 (2013) http://www.itu.int/en/ITU-T/studygroups/com17/Pages/history.aspx
30. Sibert WO, Baldwin RW (2007) The multics encipher_Algorithm. Cryptologia, Taylor and Francis Group, LLC 31(4):292–304. ISSN: 0161-1194; doi: 10.1080/01611190701506105
31. Turner S (2008) IETF RFC 5275, CMS symmetric key management and distribution
32. Whitten A, Tygar JD (1999) Why Johnny can't encrypt: a usability evaluation of PGP 5.0. In: Proceedings of the 8th conference on USENIX security symposium, vol 8. USENIX Association, Washington, DC, pp 14