Network Working Group
Request for Comments: 2313
Category: Informational

B. Kaliski
RSA Laboratories East

March 1998

PKCS #1: RSA Encryption
Version 1.5

Status of this Memo

This memo provides information for the Internet community. It does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

Copyright Notice

Overview

This document describes a method for encrypting data using the RSA public-key cryptosystem.

1. Scope

This document describes a method for encrypting data using the RSA public-key cryptosystem. Its intended use is in the construction of digital signatures and digital envelopes, as described in PKCS #7:

- For digital signatures, the content to be signed is first reduced to a message digest with a message-digest algorithm (such as MD5), and then an octet string containing the message digest is encrypted with the RSA private key of the signer of the content. The content and the encrypted message digest are represented together according to the syntax in PKCS #7 to yield a digital signature. This application is compatible with Privacy-Enhanced Mail (PEM) methods.

- For digital envelopes, the content to be enveloped is first encrypted under a content-encryption key with a content-encryption algorithm (such as DES), and then the content-encryption key is encrypted with the RSA public keys of the recipients of the content. The encrypted content and the encrypted content-encryption key are represented together according to the syntax in PKCS #7 to yield a digital envelope. This application is also compatible with PEM methods.

The document also describes a syntax for RSA public keys and private keys. The public-key syntax would be used in certificates; the private-key syntax would be used typically in PKCS #8 private-key information. The public-key syntax is identical to that in both X.509 and Privacy-Enhanced Mail. Thus X.509/PEM RSA keys can be used in this document.

The document also defines three signature algorithms for use in signing X.509/PEM certificates and certificate-revocation lists, PKCS #6 extended certificates, and other objects employing digital signatures such as X.401 message tokens.

Details on message-digest and content-encryption algorithms are outside the scope of this document, as are details on sources of the pseudorandom bits required by certain methods in this document.

2. References

FIPS PUB 46-1 National Bureau of Standards. FIPS PUB 46-1: Data Encryption Standard. January 1988.

PKCS #6 RSA Laboratories. PKCS #6: Extended-Certificate Syntax. Version 1.5, November 1993.

PKCS #7 RSA Laboratories. PKCS #7: Cryptographic Message Syntax. Version 1.5, November 1993.

PKCS #8 RSA Laboratories. PKCS #8: Private-Key Information Syntax. Version 1.2, November 1993.

RFC 1319 Kaliski, B., "The MD2 Message-Digest Algorithm," RFC 1319, April 1992.

RFC 1320 Rivest, R., "The MD4 Message-Digest Algorithm," RFC 1320, April 1992.

RFC 1321 Rivest, R., "The MD5 Message-Digest Algorithm," RFC 1321, April 1992.

RFC 1423 Balenson, D., "Privacy Enhancement for Internet Electronic Mail: Part III: Algorithms, Modes, and Identifiers," RFC 1423, February 1993.

X.208 CCITT. Recommendation X.208: Specification of Abstract Syntax Notation One (ASN.1). 1988.

X.209 CCITT. Recommendation X.209: Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1). 1988.

X.411 CCITT. Recommendation X.411: Message Handling Systems: Message Transfer System: Abstract Service Definition and Procedures.1988.

X.509 CCITT. Recommendation X.509: The Directory--Authentication Framework. 1988.

[dBB92] B. den Boer and A. Bosselaers. An attack on the last two rounds of MD4. In J. Feigenbaum, editor, Advances in Cryptology---CRYPTO ’91 Proceedings, volume 576 of Lecture Notes in Computer Science, pages 194-203. Springer-Verlag, New York, 1992.

[dBB93] B. den Boer and A. Bosselaers. Collisions for the compression function of MD5. Presented at EUROCRYPT ’93 (Lofthus, Norway, May 24-27, 1993).

[DO86] Y. Desmedt and A.M. Odlyzko. A chosen text attack on the RSA cryptosystem and some discrete logarithm schemes. In H.C. Williams, editor, Advances in Cryptology---CRYPTO ’85 Proceedings, volume 218 of Lecture Notes in Computer Science, pages 516-521. Springer-Verlag, New York, 1986.

[Has88] Johan Hastad. Solving simultaneous modular equations. SIAM Journal on Computing, 17(2):336-341, April 1988.

[IM90] Colin I’Anson and Chris Mitchell. Security defects in CCITT Recommendation X.509--The directory authentication framework. Computer Communications Review, :30-34, April 1990.

[Mer90] R.C. Merkle. Note on MD4. Unpublished manuscript, 1990.

[Mil76] G.L. Miller. Riemann’s hypothesis and tests for primality. Journal of Computer and Systems Sciences, 13(3):300-307, 1976.

[QC82] J.-J. Quisquater and C. Couvreur. Fast decipherment algorithm for RSA public-key cryptosystem. Electronics Letters, 18(21):905-907, October 1982.

[RSA78] R.L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21(2):120-126, February 1978.

3. Definitions

For the purposes of this document, the following definitions apply.

AlgorithmIdentifier: A type that identifies an algorithm (by object identifier) and associated parameters. This type is defined in X.509.

ASN.1: Abstract Syntax Notation One, as defined in X.208.

BER: Basic Encoding Rules, as defined in X.209.

DES: Data Encryption Standard, as defined in FIPS PUB 46-1.

MD2: RSA Data Security, Inc.'s MD2 message-digest algorithm, as defined in RFC 1319.

MD4: RSA Data Security, Inc.'s MD4 message-digest algorithm, as defined in RFC 1320.

MD5: RSA Data Security, Inc.'s MD5 message-digest algorithm, as defined in RFC 1321.

modulus: Integer constructed as the product of two primes.

PEM: Internet Privacy-Enhanced Mail, as defined in RFC 1423 and related documents.

RSA: The RSA public-key cryptosystem, as defined in [RSA78].

private key: Modulus and private exponent.

public key: Modulus and public exponent.

4. Symbols and abbreviations

Upper-case symbols (e.g., BT) denote octet strings and bit strings (in the case of the signature S); lower-case symbols (e.g., c) denote integers.

ab	hexadecimal octet value	c	exponent
BT	block type	d	private exponent
D	data	e	public exponent
EB	encryption block	k	length of modulus in octets
ED	encrypted data	n	modulus
M	message	p, q	prime factors of modulus
MD	message digest	x	integer encryption block
MD'	comparative message digest	y	integer encrypted data
PS	padding string	mod n	modulo n
S	signature	X || Y	concatenation of X, Y
		||X||	length in octets of X

5. General overview

The next six sections specify key generation, key syntax, the encryption process, the decryption process, signature algorithms, and object identifiers.

Each entity shall generate a pair of keys: a public key and a private key. The encryption process shall be performed with one of the keys and the decryption process shall be performed with the other key. Thus the encryption process can be either a public-key operation or a private-key operation, and so can the decryption process. Both processes transform an octet string to another octet string. The processes are inverses of each other if one process uses an entity's public key and the other process uses the same entity's private key.

The encryption and decryption processes can implement either the classic RSA transformations, or variations with padding.

6. Key generation

This section describes RSA key generation.

Each entity shall select a positive integer e as its public exponent.

Each entity shall privately and randomly select two distinct odd primes p and q such that (p-1) and e have no common divisors, and (q-1) and e have no common divisors.

The public modulus n shall be the product of the private prime factors p and q:

$$n = pq .$$

The private exponent shall be a positive integer d such that de-1 is divisible by both p-1 and q-1.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.

WHAT WILL YOU BUILD? | **sales@docketalarm.com** | **1-866-77-FASTCASE**

fastcase®
Smarter legal research.