More About

RSA Algorithm

Recent results on OAEP security

RSAES-OAEP Dictionary

RSA-based Cryptographic Schemes

The RSA algorithm was invented by Ronald L. Rivest, Adi Shamir, and Leonard Adleman in 1977. This page has a collection of links to RSA-related documents on this web site. There are a variety of different cryptographic schemes and protocols based on the RSA algorithm in products all over the world; RSA Laboratories recommends the RSAES-OAEP encryption scheme and the RSASSA-PSS signature scheme with appendix for new applications.

RSAES-OAEP (***RSA*** ***E****ncryption* ***S****cheme - **O**ptimal* ***A****symmetric* ***E****ncryption* ***P****adding*) is a public-key encryption scheme combining the RSA algorithm with the OAEP method. The inventors of OAEP are Mihir Bellare and Phillip Rogaway, with enhancements by Don B. Johnson and Stephen M. Matyas.

RSASSA-PSS (***RSA*** ***S****ignature* ***S****cheme with* ***A****ppendix -* ***P****robabilistic* ***S****ignature* ***S****cheme*) is an asymmetric signature scheme with appendix combining the RSA algorithm with the PSS encoding method. The inventors of the PSS encoding method are Mihir Bellare and Phillip Rogaway. During efforts to adopt RSASSA-PSS into the P1363a standards effort, certain adaptations to the original version of RSA-PSS were made by Bellare and Rogaway and also by Burt Kaliski (the editor of IEEE P1363a) to facilitate implementation and integration into existing protocols.

Documents

Recent results on OAEP security (HTML page)
This document outlines the security of the OAEP encoding method and the RSAES-OAEP encryption scheme. To summarize, RSAES-OAEP is secure against what is termed adaptive chosen ciphertext attacks. However, OAEP combined with other public-key algorithms different from RSA may not achieve provable security in this strongest sense.

RSAES-OAEP dictionary (HTML page)
In this dictionary, we give brief descriptions of words and phrases related to the RSAES-OAEP encryption scheme (as well as public-key encryption schemes in general).

RSA Labs submissions (HTML page)
RSA Laboratories has submitted RSAES-OAEP and RSASSA-PSS to the NESSIE project and the Japanese IPA CRYPTREC project. RSAES-OAEP is also submitted to ISO/IEC NP 18033 via the U.S. and Swedish ISO/IEC JTC 1/SC 27 member bodies.

RELATED LINKS

- > RSA Labs algorithms submissions
- > PKCS #1
- > RSA-OAEP algorithm specification and supporting documentation (.PDF)
- > RSA-PSS algorithm specification and supporting documentation (to be added)
- > RSA-OAEP and RSA-PSS test vectors (.zip file)
- > RSA Factoring Challenge
- > IEEE P1363 (standard specifications for public-key cryptography)
- > NESSIE project
- > ISO/IEC 18033 project
- > Japanese IPA CRYPTREC project
- > The history of Non-Secret Encryption at the British Communications-Electronics Security Group (CESG)

PKCS #1 (HTML page)
The Public Key Cryptography Standard (PKCS) #1 provides recommendations for the implementation of public-key cryptography based on the RSA algorithm. RSAES-OAEP is included in PKCS #1 v2.0 and in the draft PKCS #1 v2.1. RSASSA-PSS is included in PKCS #1 v2.1 d2 (note however that the specification of RSASSA-PSS in v2.1 d1 is obsolete).

RSAES-OAEP algorithm specification and supporting documentation (PDF document)
This document is a revised version of the algorithm specification submitted to the NESSIE project (see previous link), containing the latest updates on the security of OAEP.

RSASSA-PSS algorithm specification and supporting documentation
To be added. In the meantime, download the RSASSA-PSS submission to NESSIE from our submissions page.

External link

The history of Non-Secret Encryption at the British Communications-Electronics Security Group (CESG) (HTML page)
In 1973, a few years before RSA was invented at M.I.T., the U.K. cryptographer Clifford Cocks invented an RSA variant (using CRT for decryption!). Unfortunately, his discovery was classified, as were James Ellis' survey about the possibility of non-secret encryption from 1970 and Malcolm Williamson's invention of a Diffie-Hellman analog from 1974 (with improvements in 1976). Recently, the results were released; PDF documents can be downloaded from the CESG web site.

© Copyright 2002 RSA Security Inc - all rights reserved. Reproduction of this Web Site, in whole or in part, in any form or medium without express written permission from RSA Security is prohibited.