Cryptography FAQ (07/10: Digital Signatures)

Message-ID: <cryptography-faq/part07 1040202968@rtfm.mit.edu>
Supersedes: <cryptography-faq/part07 1038303482@rtfm.mit.edu>
Expires: 22 Jan 2003 09:16:08 GMT
References: <cryptography-faq/part01 1040202968@rtfm.mit.edu>
X-Last-Updated: 1994/07/05
Newsgroups:
sci.crypt,talk.politics.crypto,sci.answers,news.answers,talk.answers
Subject: Cryptography FAQ (07/10: Digital Signatures)
Followup-To: poster
From: crypt-comments@math.ncsu.edu
Organization: The Crypt Cabal
Reply-To: crypt-comments@math.ncsu.edu
Date: 18 Dec 2002 09:16:17 GMT
X-Trace: 1040202977 senator-bedfellow.mit.edu 3936 18.181.0.29

Archive-name: cryptography-faq/part07
Last-modified: 93/10/10

This is the seventh of ten parts of the sci.crypt FAQ. The parts are mostly independent, but you should read the first part before the rest. We don't have the time to send out missing parts by mail, so don't ask. Notes such as ``[KAH67]'' refer to the reference list in the last part.

The sections of this FAQ are available via anonymous FTP to rtfm.mit.edu as /pub/usenet/news.answers/cryptography-faq/part[xx]. The Cryptography FAQ is posted to the newsgroups sci.crypt, talk.politics.crypto, sci.answers, and news.answers every 21 days.

Contents:

7.1. What is a one-way hash function?

A typical one-way hash function takes a variable-length message and produces a fixed-length hash. Given the hash it is computationally impossible to find a message with that hash; in fact one can't determine any usable information about a message with that hash, not even a single bit. For some one-way hash functions it's also computationally impossible to determine two messages which produce the same hash.

A one-way hash function can be private or public, just like an encryption function. Here's one application of a public one-way hash function, like MD5 or Snefru. Most public-key signature systems are relatively slow. To sign a long message may take longer than the user is willing to wait. Solution: Compute the one-way hash of the message, and sign the hash, which is short. Now anyone who wants to verify the signature can do the same thing.

Another name for one-way hash function is message digest function.

7.2. What is the difference between public, private, secret, shared, etc.?

There is a horrendous mishmash of terminology in the literature for a very small set of concepts. Here are the concepts: (1) When an algorithm depends on a key which isn't published, we call it a private algorithm; otherwise we call it a public algorithm. (2) We have encryption functions E and decryption functions D, so that D(E(M)) = M for any message M. (3) We also have hashing functions H and verification functions V, such that V(M,X) = 1 if and only if X = H(M).

A public-key cryptosystem has public encryption and private decryption. Checksums, such as the application mentioned in the previous question, have public hashing and public verification. Digital signature functions have private hashing and public verification: only one person can produce the hash for a message, but everyone can verify that the hash is correct.

Obviously, when an algorithm depends on a private key, it's meant to be unusable by anyone who doesn't have the key. There's no real difference between a ``shared'' key and a private key: a shared key isn't published, so it's private. If you encrypt data for a friend rather than ``for your eyes only'', are you suddenly doing ``shared-key encryption'' rather than private-key encryption? No.

7.3. What are MD4 and MD5?

MD4 and MD5 are message digest functions developed by Ron Rivest. Definitions appear in RFC 1320 and RFC 1321 (see part 10). Code is available from [FTPMD].

Note that a transcription error was found in the original MD5 draft RFC. The corrected algorithm should be called MD5a, though some people refer to it as MD5.

7.4. What is Snefru?

Snefru is a family of message digest functions developed by Ralph Merkle. Snefru-8 is an 8-round function, the newest in the family. Definitions appear in Merkle's paper [ME91a]. Code is available from [FTPSF].

Part01 - Part02 - Part03 - Part04 - Part05 - Part06 - Part07 - Part08 - Part09 - Part10

[By Archive-name | By Author | By Category | By Newsgroup]
[Home | Latest Updates | Archive Stats | Search | Usenet References | Help]

Send corrections/additions to the FAQ Maintainer:
crypt-comments@math.ncsu.edu

Last Update January 01 2003 @ 00:33 AM