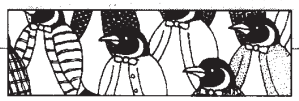

A Survey of Encryption Standards

Numerous encryption standards dot the microcomputer landscape, seemingly covering every application. One nevertheless finds much common ground underlying the many standards. This survey discusses the standards and their algorithms, how they compare, how they differ, and where they're headed.

Burt Kaliski

RSA Laboratories

Cryptography is the science, or some would say the art, of secret codes. In its broadest sense cryptography addresses a number of practical problems:

- *confidentiality*, keeping messages secret;
- *origin authentication*, verifying a message's source;
- *integrity*, assuring that a message has not been modified; and
- *key management*, distributing the secret "keys" for cryptographic algorithms.

This survey focuses on encryption algorithms, the low-level, step-by-step transformations on messages that address these problems, as well as applications that involve encryption. It covers both approved standards and work in progress; the modifiers *draft* and *proposed* should help with the distinction.

Since descriptions here are at a summary level, readers seeking greater depth may refer to the standards documents or to encryption surveys such as those by Diffie,[1] Simmons,[2] which includes a reprint of Diffie's article, and Fahn,[3] which is available from RSA Laboratories or via anonymous ftp to rsa.com. Patel gives an earlier survey on security standards for the Open Systems Interconnection (OSI) reference model.[4]

Much of the encryption standards work fits into one or more security "models." The models do not specify algorithms; rather, they define services and give structures for encryption protocols. The OSI Security Architecture standard[5] is one helpful reference. Also on the road to international standardization is the Generic Upper Layers Security (GULS) standard.[6] GULS forms the basis for IEEE P802.10, a local-area network security project, and the draft ANSI X9.41,[7] a standards effort for electronic data interchange.

Many ways other than encryption exist to protect data, from access control to tamper-resistant coatings, but they are outside the scope of this article. Even in systems based on cryptography, other issues than just the codes come into play, such as random number sources and password selection guidelines. The US Department of Defense's "Orange Book" is one of many helpful references for these topics.[8]

Remember, draft standards and other works in progress are subject to change. Furthermore, with the large number of standards efforts, I may not have covered some relevant efforts. An effort's absence from this article in no way minimizes its importance.

Algorithms

An encryption algorithm is a method of transforming a message to add some cryptographic protection, such as confidentiality or integrity. Most encryption algorithms involve one or more keys, which are cryptographic variables, often

0272-1732/93/1200-0074$03.00 © 1993 IEEE

unique to one user, that control the algorithm and provide security against attackers.

Cryptographers often classify encryption algorithms according to the type of transformation and keys. Each class solves a different set of cryptographic problems. Some classes require that parties first agree on a secret key by secure means that are separate from the normal communication protocol; others do not have this limitation. I describe the algorithms standards according to one such classification: secret-key cryptosystems, public-key cryptosystems, digital signature schemes, key-agreement algorithms, cryptographic hash functions, and authentication codes. Table 1 summarizes the classes and their properties.

Table 1. Encryption algorithm classes and their properties.

Class	C	OA	I	KM	Prior
Secret-key cryptosystems	Yes	No	No	Yes	Yes
Public-key cryptosystems	Yes	No	No	Yes	No
Digital signature schemes	No	Yes	Yes	No	No
Key-agreement algorithms	Yes	Optional	No	Yes	No
Cryptographic hash functions	No	No	Yes	No	No
Authentication codes	No	Yes	Yes	No	Yes

C indicates confidentiality; OA, origin authentication; I, integrity; KM, key management.
Prior requires that parties first agree on a secret key.

Secret-key cryptosystems. These algorithms encrypt and decrypt messages with a key in such a way that it is difficult to decrypt without the key. Because the encryption and decryption keys in a secret-key cryptosystem are the same, such systems are often called symmetric in the literature.

Most secret-key cryptosystems operate on messages one block at a time; a block may be 64 bits long, and the keys are usually short, say, 56 bits long. Ideally, an attacker's only approach is trial and error, which amounts, for example, to 2^{56} trials for 56-bit keys. Secret-key algorithms are generally quite fast.

Secret-key cryptosystems provide confidentiality and key management to parties who have previously agreed on a secret key. The Data Encryption Standard (DES)[9] is the primary standard. Published in 1977 and recently affirmed for a fourth five-year period, DES defines the Data Encryption Algorithm (DEA). It also specifies how to implement DEA: in hardware. Technically, software implementations of DEA, which abound, do not comply. ANSI standard X3.92[10] and Australian Standard AS2805.5[11] specify DEA.

Despite much controversy about the nature of DEA—the government never revealed its design criteria—the algorithm seems to be quite secure, as far as 56-bit algorithms go. It resists powerful attacks that have broken other systems.[12,13]

Along with DES come some standard modes of operation, including electronic codebook, cipher block chaining, cipher feedback, and output feedback.[14] These modes apply to any block cipher, not just DEA. ANSI X9.17[15] introduces the encrypt-decrypt-encrypt (EDE) mode of encryption involving two DEA keys.

Two password-based encryption algorithms defined in the intervendor public-key cryptography standard (PKCS) #5[16] are also based on DEA.

A potential new standard secret-key cryptosystem is Skipjack, a classified part of the proposed escrowed encryption standard.[17] A panel of cryptography experts recently certified Skipjack, with 80-bit keys, as appearing secure,[18] but its details remain unpublished.

Secret-key cryptosystems are rarely standardized; some standards bodies explicitly omit them from their scope. One of the few other candidates is RC4, a fast secret-key cryptosystem with variable-length keys.[19] RC4 is adopted in the cellular digital packet data (CDPD) specifications.[20]

Public-key cryptosystems. These algorithms encrypt and decrypt messages with two different keys in such a way that it is difficult to decrypt without the decryption key. The encryption key can be published without compromising security, and is called the public key for this reason; the decryption key is called the private key. Because the encryption and decryption keys in a public-key cryptosystem differ, such systems are often called asymmetric in the literature. The idea comes from Diffie and Hellman.[21]

Public-key cryptosystems provide confidentiality and key management. They can be as secure or more secure than secret-key cryptosystems, but they are generally slower. Their main advantage is that, since the encryption key can be published, parties need not first agree on a secret key. They are often combined with secret-key cryptosystems to gain the benefits of both: speed without prior secrets.

Although there is no primary standard public-key cryptosystem, many consider a cryptosystem invented by Rivest, Shamir, and Adleman (RSA)[22] in 1977 a de facto standard. Public-key cryptosystems, like secret-key cryptosystems, are rarely standardized; when they are standardized, key management is a more likely purpose than confidentiality.

Efforts toward RSA standardization include the intervendor PKCS #1,[23] which gives block formats for RSA operations, and the draft ANSI X9.31 part 4,[24] which is currently based on PKCS #1. PKCS #1's block formats have been adopted by Internet privacy-enhanced mail[25] and, among other algorithms,

Glossary

The acronyms for encryption standards and the groups developing them are considered by some as a form of encryption in its own right. Following is an abridged "key" to the various acronyms and their meanings, as well as to several standards organizations.

ASC X9 Accredited Standards Committee X9 (Financial Services), a body that develops standards for the banking industry; accredited by ANSI

ANSI American National Standards Institute, an organization that accredits standards bodies

CCITT Comité Consultatif International de Télégraphique et Téléphonique, (International Telegraph and Telephone Consultative Committee), an international standards body

CFONB Comité Français d'Organisation et de Normalisation Bancaire, a French banking standards body

DAA Data Authentication Algorithm, a NIST standard authentication code defined in FIPS PUB 113

DEA Data Encryption Algorithm, the secret-key cryptosystem specified by DES

DES Data Encryption Standard, a NIST standard defined in FIPS PUB 46-1 that specifies DEA

Diffie-Hellman A key-agreement algorithm invented by Whitfield Diffie and Martin Hellman

DSA Digital Signature Algorithm, the digital signature scheme specified by DSS

DSS Digital Signature Standard, a proposed NIST standard that specifies DSA

EDE Encrypt-decrypt-encrypt, a mode of DEA involving two keys and three DEA operations that is defined in ANSI X9.17

EES Escrowed Encryption Standard, a proposed NIST standard that specifies Skipjack

FIPS PUB Federal Information Processing Standard publication, one of a series of standards published by NIST

GULS Generic Upper Layers Security, an OSI security architecture effort

IEC International Electrotechnical Commission, an international standards body

IEEE Institute of Electrical and Electronics Engineers, an organization that develops transnational standards; that is, the standards are the consensus of individuals rather than national representatives

Internet A transnational body that develops standards for computer networking and publishes RFCs; also, the network of computers that implements those standards

ISO International Standards Organization, an international standards body

MD2 Message Digest Algorithm 2, a hash function developed by Ron Rivest that is defined in Internet RFC 1319

MD5 Message Digest Algorithm 5, another hash function developed by Ron Rivest and defined in Internet RFC 1321

MDC-2 Manipulation Detection Code 2, the hash function specified in draft ANSI X9.31 part 2

NBS National Bureau of Standards; see NIST

NIST National Institute of Standards and Technology (formerly NBS), a US government agency that develops standards and publishes FIPS PUBs

OIW Open Systems Environment (formerly OSI) Implementors' Workshop, a group of developers that agrees on implementation issues such as algorithms

OSI Open Systems Interconnection, a standard networking model

are cited in the OIW implementors' agreements.[26] (As this article was going to press, I received a copy of Australian Standard AS28095.5.3, which specifies RSA.[27])

Digital signature schemes. These schemes "sign" messages and verify the resulting signature with two different keys in such a way that it is difficult to sign without the signing key. Similar to public-key cryptosystems, the verification key can be published without compromising security, and is called the public key; the signing key is called the private key.

Digital signature schemes provide integrity and origin authentication. Like public-key cryptosystems, they do not require that parties first agree on a secret key, and they are generally somewhat slower than, for instance, secret-key cryptosystems and cryptographic hash functions. They are often combined with hash functions to gain the benefits of both.

Public-key cryptosystems and digital signature schemes are

Glossary (continued)

PEM	Privacy-enhanced mail, a proposed Internet standard for encrypting and authenticating electronic mail; defined in Internet RFCs 1421-1424
PKCS	Public-key cryptography standards, informal standards developed by RSA Laboratories with representatives of Apple, Digital, Lotus, Microsoft, MIT, Northern Telecom, Novell, and Sun; available from RSA Laboratories or via electronic mail to pkcs@rsa.com
RC4	Rivest Cipher 4, a fast secret-key cryptosystem developed by Ron Rivest and proprietary to RSA Data Security
RFC	"Request for Comments," an Internet publication
RSA	Rivest-Shamir-Adleman algorithm, a public-key cryptosystem and digital signature scheme invented by Ron Rivest, Adi Shamir, and Len Adleman
SC6	Subcommittee 6 (Telecommunications and Information Exchange Between Systems), a joint subcommittee of ISO/IEC
SC27/WG2	Subcommittee 27 (Information Technology), Working Group 2 (Security Techniques), a joint working group of ISO/IEC
SHA	Secure Hash Algorithm, the hash function specified by SHS
SHS	Secure Hash Standard, a NIST standard defined in FIPS PUB 180 that specifies SHA
SILS	Secure Interoperable Local Area Network Security, an IEEE project; also called P802.10
Skipjack	The classified secret-key cryptosystem specified by EES
SNMP	Simple Network Management Protocol, an Internet standard defined in Internet RFC 1157
Standards	
Australia	An Australian standards body
X9	See ASC X9

closely related. In so-called reversible cryptography, signing in a digital signature scheme is the same as decryption in a public-key cryptosystem, while verification is the same as encryption. In irreversible cryptography, the relationships do not hold, although a given public/private-key pair may work in both a digital signature scheme and a public-key cryptosystem.

There is no primary standard digital signature scheme, but two main efforts are in progress. One involves RSA, which is reversible, and the other involves an irreversible algorithm proposed by the US National Institute of Standards and Technology (NIST).

ISO/IEC 9796[28] almost creates a standard for RSA, but not quite. It defines a signature block format; RSA is in an informative (but nonstandard) annex. The block format prevents certain mathematical relationships among possible RSA signatures.[29] The draft ANSI X9.31 part 1,[30] which is expected to become a standard late this year, is based on ISO/IEC 9796 and specifies RSA. The intervendor PKCS #1[23] gives alternate block formats for RSA signatures. ISO/IEC's joint working group SC27/WG2 is developing other digital signature standards.

NIST's proposed Digital Signature Standard (DSS),[31] which defines the Digital Signature Algorithm (DSA), has been the center of recent controversy.[32] DSA, an irreversible algorithm, is a variant of signature schemes due to Elgamal[33] and Schnorr.[34] It is intended to be combined with the Secure Hash Algorithm (SHA).[35] Mainly due to objections from industry, DSS has not yet been approved. The draft ANSI X9.30 part 1[36] specifies DSA.

Key-agreement algorithms. These algorithms manage keys through an exchange of messages derived from private values that are not shared. The result of the exchange is that parties agree on a secret key. It is difficult to determine the secret key from the exchanged messages without the private values from which they are derived. Key-agreement algorithms are sometimes called key exchange algorithms in the literature.

Key-agreement algorithms provide confidentiality and key management, and in some cases origin authentication. They do not require that parties first agree on a secret key. As with public-key cryptosystems, no primary standard key-agreement algorithm exists. Many consider an algorithm invented by Diffie and Hellman,[21] usually called Diffie-Hellman, the de facto standard here.

Efforts toward Diffie-Hellman standardization include the intervendor PKCS #3[37] and the draft ANSI X9.30 part 4,[38] which is based on a variant of Diffie-Hellman having origin authentication. The cellular digital packet data (CDPD) specifications[20] adopt Diffie-Hellman key agreement. ISO/IEC's joint working group SC6 is developing standards for key agreement in the network and transport layers of the OSI reference model,[39,40] with Diffie-Hellman as a possible algorithm.

Cryptographic hash functions. These functions reduce a message of arbitrary length to a short code so that it is difficult to find a message with a given hash code, and in some cases also to find two messages with the same hash code. There is no key. Hash functions are also called message digests and modification detection codes in the literature.

A hash code is typically 128 or 160 bits long. Ideally, an attacker's only approach is trial and error, which amounts to 2^{128} trials to find a message with a given hash code (for a 128-bit hash), and 2^{64} trials to find two messages with the same hash code. (This is akin to the "birthday paradox": You need

365 people in a room to be likely to find one with a given birthday, but only 23 to be likely to find two with the same birthday.) Hash functions are generally quite fast. They provide message integrity to parties knowing a message's hash code. They are often combined with digital signature schemes, as noted earlier.

The Secure Hash Standard (SHS),[35] which defines SHA, is the primary standard. SHA produces a 160-bit hash from a message of arbitrary length; it is intended to be combined with DSA.[31] ANSI X9.30 part 2[41] specifies SHA.

Other hash algorithms suitable for standardization include MD2 and MD5, developed by Ron Rivest for RSA Data Security[42,42] and adopted by Internet privacy-enhanced mail,[25] and MDC-2, which is specified in draft ANSI X9.31 part 2.[44] SC27/WG2 is also developing standards for hash functions.

Authentication codes. These codes reduce a message of arbitrary length to a short code under a secret key so that it is difficult, without the key, to compute the authentication code, or to find a new message with a given authentication code. Authentication codes provide message integrity and origin authentication to parties who have previously agreed on a secret key. The message itself need not be encrypted.

An authentication code is typically 32 or 64 bits long, and the keys are 56 bits long. Ideally, an attacker's only approach is trial and error on the keys; arbitrary message modifications have some probability of success, but the attacker cannot check for success without the help of the real user. Authentication codes, like hash functions, are generally quite fast.

The primary standard is FIPS PUB 113,[45] which defines the Data Authentication Algorithm. The algorithm is a variant of DEA; it produces a 32-bit authentication code from a message of arbitrary length and a 56-bit key. ANSI X9.9[46] and Australian standard AS2805.4[47] specify DAA.

Applications

The applications standards described next combine families of algorithms, and sometimes specify particular algorithms, to solve confidentiality, integrity, origin authentication, and key management problems. Although many of the standards specify much more than just cryptography, encryption plays an important role.

Ideally, an algorithm should work in many applications, and many algorithms should work in a given application. The design of applications and algorithms is in this sense "orthogonal," and the designers have generally done a good job at providing orthogonality.

Do not confuse these applications with the applications layer of the OSI reference model; some may well run at that layer, and others at lower layers.

Secure electronic mail. Six years in development and now a proposed standard, Internet privacy-enhanced mail (PEM) combines secret-key cryptosystems, public-key cryptosystems, hash functions, and digital signature schemes to provide security for electronic mail.[48] It is a text-based protocol compatible with most electronic-mail systems. PEM supports public-key and secret-key techniques; the former involves X.509 certificates.[49] Currently, PEM has adopted RSA, DEA, MD2, and MD5 algorithms,[25] but the protocols are flexible and other suites of algorithms are likely to be added.

Mail is not the only application of PEM, of course, although it is a primary one. The same protocol that adds encryption or authentication to a mail message can enhance any digital document, such as a contract; the document need not be mailed to someone.

The intervendor PKCS #7[50] is a binary extension of PEM; it offers the same services, but works with binary data and allows one to sign attributes such as the time of day along with the underlying message. Certain modes of PKCS #7 are cryptographically compatible with PEM, in the sense that messages can be translated between the two protocols without any cryptographic operations. PKCS #7 does not specify a particular algorithm.

Another approach to electronic-mail security is found in X.400 message-handling systems,[51] which solve the basic problems of confidentiality, authentication, and key management. X.400 also provides special encryption-based services such as proof of submission and proof of delivery. (X.411 supplies the details.[52]) X.400, like most international standards, does not specify particular algorithms. It supports both public-key and secret-key techniques. ISO 10021-1[53] is technically aligned with X.400.

X.435,[54] a standard for electronic data interchange over X.400, builds on X.411's services, defining related services such as signed receipts.

Secure communications. These standards focus on the security of local-area networks and wireless links. IEEE's P802.10 project, Secure Interoperable LAN (local area network) Security (SILS), addresses privacy and authentication of data at the data link layer. Devices following the protocol encrypt data link frames as they pass through the network; the protocol is transparent to higher layers. A proposed draft[55] specifies Diffie-Hellman key agreement. The CDPD specifications[20] define an encryption protocol for wireless links based on Diffie-Hellman key agreement and RC4.

IEEE project P802.11, focusing on wireless links, has just started.

Directory authentication and network management. X.509 directory authentication[49] applies public-key and secret-key techniques to the problem of determining the identity of a user attempting to access an X.500 global directory.[56] "Weak" authentication identifies a user by a password, while "strong" authentication involves digital signatures. The authentication protocols can also ensure that messages to and from the directory are not modified in transit.

X.509 standardizes on no particular algorithm, although RSA is in an informative annex. Two additional contributions

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.