September 2002

ITL Bulletin

ADVISING USERS ON INFORMATION TECHNOLOGY

CRYPTOGRAPHIC STANDARDS AND GUIDELINES: A STATUS REPORT

By Elaine Barker, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology

Introduction

The Computer Security Division within NIST's Information Technology Laboratory is responsible for the development of cryptographic standards and guidelines for the protection of the sensitive, unclassified information of federal government agencies. A comprehensive toolkit of cryptographic standards and associated guidance that covers a wide range of cryptographic technology is nearing completion. These standards and guidelines will enable federal government agencies to select cryptographic security components and functionality for protecting their data communications and operations.

The toolkit consists of standards for encryption, digital signatures, secure hashing, message (data) authentication codes, key management, entity authentication, password usage, and random number generation. The current standards and guidelines are available at http://csrc.nist.gov/publications/. Links to information on standards and guidelines under development are provided below.

The Computer Security Division and the Communications Security Establishment of the Government of Canada coordinate a validation program with independent accredited testing laboratories that validate conformance to Federal Information Processing Standard (FIPS) 140-2, *Security Requirements for Cryptographic Modules*. The Cryptographic Module Validation Program (CMVP) includes the validation of implementations of many of the cryptographic standards and guidelines developed by NIST. Information is available about the CMVP at http://csrc.nist.gov/cryptval/.

Encryption

Encryption provides confidentiality for data. The data to be protected is called plaintext. Encryption transforms the plaintext data into an unreadable form, called ciphertext, using an encryption key. Decryption transforms the ciphertext back into plaintext using a decryption key. Several algorithms have been approved in FIPS for the encryption of general-purpose data. Each of these algorithms is a symmetric key algorithm, where the encryption key is the same as the decryption key. In order to maintain the confidentiality of the data encrypted by a key, the key must be known only by the entities that are authorized to access the data. These symmetric key algorithms are commonly known as block cipher algorithms, because the encryption and decryption processes each operate on blocks (chunks) of data of a fixed size.

FIPS 46-3 and FIPS 197 have been approved for the encryption of general-purpose data. The protection (e.g., encryption) of keys is discussed below under Key Management.

FIPS 46-3, Data Encryption Standard (DES). FIPS 46-3 specifies the DES algorithm. It was originally adopted in 1977 as FIPS 46, and reaffirmed in 1983 and 1987 as FIPS 46-1 and FIPS 46-2 with changes to the allowed embodiment of the algorithm. In 1999, the standard was affirmed as FIPS 46-3, adopting the Triple DES algorithm (TDES) as specified in the American National Standards Institute (ANSI) X9.52 standard, and continuing to allow [single] DES for legacy systems, as specified in FIPS 46-2. ***When FIPS 46-3 comes up for review in 2004, single DES will no longer be approved for Federal Government applications***. Therefore, neither new applications nor current legacy systems, including systems using crypto-

Continued on page 2

ITL Bulletins are published by the Information Technology Laboratory (ITL) of the National Institute of Standards and Technology (NIST). Each bulletin presents an in-depth discussion of a single topic of significant interest to the information systems community. **Bulletins are issued on an as-needed basis** and are available from ITL Publications, National Institute of Standards and Technology, 100 Bureau Drive, Stop 8901, Gaithersburg, MD 20899-8901, telephone (301) 975-2832. To be placed on a mailing list to receive future bulletins, send your name, organization, and business address to this office. You will be placed on this mailing list only.

Bulletins issued since January 2001

graphic modules previously validated against FIPS 140-1 and 2, will be approved for using single DES after 2004. However, TDES and AES (the algorithm specified in FIPS 197; see below) will continue to be approved for all systems. Agencies should develop and implement a transition plan for using approved algorithms other than single DES.

TDES is a method for encrypting data in 64-bit blocks using three 56-bit keys by combining three successive invocations of the DES algorithm. ANSI X9.52 specifies seven modes of operation for TDES and three keying options: 1) the three keys may be identical (one key TDES), 2) the first and third key may be the same but different from the second key (two key TDES), or 3) all three keys may be different (three key TDES). One key TDES is equivalent to DES under the same key; therefore, one key TDES, like DES, is currently allowed only for legacy systems, but will not be approved after 2004. Two key TDES provides more security than one key TDES (or DES), and three key TDES achieves the highest level of security for TDES. ***NIST recommends the use of three different 56-bit keys in Triple DES for Federal Government sensitive/unclassified applications.***

FIPS 197, Advanced Encryption Standard (AES). The encryption algorithm specified in FIPS 197 is the result of a multiyear, worldwide competition to develop a replacement algorithm for DES. The winning algorithm (originally known as Rijndael, but hereafter referred to as the AES algorithm) was announced in 2000 and adopted in FIPS 197 in 2001. The AES algorithm encrypts and decrypts data in 128-bit blocks, with three possible key sizes: 128, 192, or 256 bits. The nomenclature for the AES algorithm for the different key sizes is AES-x, where x is the size of the AES key. NIST considers all three AES key sizes adequate for Federal Government sensitive/unclassified applications. Information on the AES development effort is available at http://csrc.nist.gov/encryption/aes/.

Comparison of the TDES and AES Algorithms. Both algorithms are considered to be secure for the foreseeable future. The following is a comparison of the algorithms.

1. TDES builds on DES implementations and is readily available in many cryptographic products and protocols. The AES algorithm is new; although many implementers are quickly adding the algorithm to their products, and protocols are being modified to incorporate the algorithm, it may be several years before the AES algorithm is as pervasive as TDES.
2. The AES algorithm was designed to provide better performance (e.g., faster speed) than TDES. Some performance metrics are available at http://csrc.nist.gov/encryption/aes/.
3. Although the security of block cipher algorithms is difficult to quantify, the AES algorithm, at any of the key sizes, appears to provide greater security than TDES. In particular, the best attack known against AES-128 is to try every possible 128-bit key (i.e., perform an exhaustive key search). By contrast, although three key TDES has a 168-bit key, there is a "shortcut" attack on TDES that is comparable, in the number of required operations, to performing an exhaustive key search on 112-bit keys. However, unlike exhaustive key search, this shortcut attack requires a lot of memory. Assuming that such shortcut attacks are not discovered for the AES algorithm, the uses of the AES algorithm may be more appropriate for the protection of high-risk or long-term data.
4. The smallest AES key size is 128 bits; the recommended key size for TDES is 168 bits. The smaller key size means that fewer resources are needed for the generation, exchange, and storage of key bits.
5. The AES block size is 128 bits; the TDES block size is 64 bits. For some constrained environments, the smaller block size may be preferred; however, the larger AES block size is more suitable for cryptographic applications, especially those requiring data authentication on large amounts of data.

Modes of Operation. With a block cipher algorithm, the same plaintext block will always encrypt to the same ciphertext block whenever the same key is used. If the multiple blocks in a typical message were to be encrypted separately, an adversary could easily substitute individual blocks, possibly without detection. Furthermore, data patterns in the plaintext would be apparent in the ciphertext. Cryptographic modes of operation have been defined to alleviate these problems by combining the basic cryptographic algorithm with a feedback of the information derived from the cryptographic operation.

FIPS 81, *DES Modes of Operation*, defines four confidentiality (encryption) modes for the DES algorithm specified in FIPS 46-3: the Electronic Codebook (ECB) mode, the Cipher Block Chaining (CBC) mode, the Cipher Feedback (CFB) mode, and the Output Feedback (OFB) mode.

NIST Special Publication 800-38A (NIST SP 800-38A), *Recommendation for Block Cipher Modes of Operation-Methods and Techniques*, defines modes of operation for the encryption and decryption of data using approved block cipher algorithms such as the AES and TDES algorithms. Analogues of the four confidentiality modes defined in FIPS 81 are included: ECB, CBC, CFB, and OFB. A fifth mode is also defined: the Counter (CTR) mode.

ITL Bulletins Via E-Mail

We now offer the option of delivering your ITL Bulletins in ASCII format directly to your e-mail address. To subscribe to this service, send an e-mail message from your business e-mail account to listproc@nist.gov with the message **subscribe itl-bulletin**, and your name, e.g., John Doe. For instructions on using listproc, send a message to listproc@nist.gov with the message **HELP**. To have the bulletin sent to an e-mail address other than the From address, contact the ITL editor at 301-975-2832 or elizabeth.lennon@nist.gov.

Three additional modes for TDES have been defined in ANSI X9.52 (adopted by FIPS 46-3) to pipeline and interleave the data during the encryption and decryption to attain better performance with TDES: a pipeline mode for CFB, and interleave modes for CBC and OFB.

Message Authentication Codes

Message authentication codes (MACs) (also known as data authentication codes) are cryptographic checksums on data that are used to provide assurance to a message receiver of the authenticity and integrity of the data. The computation of a MAC requires the use of a MAC algorithm and a secret key.

Two types of MAC algorithms have been approved: MAC algorithms that are based on block cipher algorithms and MAC algorithms that are based on hash functions.

FIPS 113, *Computer Data Authentication*, specifies an algorithm, which is based on DES, for generating and verifying a MAC. FIPS 113 specifies the generation of a MAC of 24, 32, 40, 48, or 56 bits.

FIPS 198, *Keyed-Hash Message Authentication Code (HMAC)*, specifies the computation of a MAC using an approved hash function (see below) and a key. The lengths of the MAC in bits depend on the length of the output of the hash function. If the hash function produces an output of L bits (e.g., L = 160 for SHA-1), then FIPS 198 specifies that the MAC should be between $L/2$ and L bits in length; however, FIPS 198 allows a smaller MAC (e.g., 32 bits) under certain conditions.

NIST SP 800-38B, which is under development, will specify algorithms for the computation of MACs using approved block cipher algorithms, such as the AES and TDES algorithms. Information on this project is available at http://www.nist.gov/modes.

Digital Signatures

Digital signatures are used to provide data authentication, data integrity detection, and non-repudiation. Data authentication and data integrity were discussed under Message Authentication Codes. Non-repudiation is the property whereby data authentication and data integrity can be verified not only by a receiving entity, but by a third party as well.

Digital signatures are generated and verified using asymmetric key algorithms, commonly known as public key algorithms. Asymmetric key algorithms use a pair of keys: a public key that may be known by anyone, and a private key that must be known only by the owner of the key pair. The key pair owner generates a digital signature on the information to be signed using the private key. The signed information and the digital signature are then provided to the intended receiver. The receiver uses the public key to verify the digital signature. If the digital signature is verified as correct, the receiver 1) is assured of the identity of the signing entity (because only that entity knows the private key), 2) is assured that the signed information was received correctly, and 3) can prove the identity of the message signer to an independent third party, if necessary.

FIPS 186-2, *Digital Signature Standard*, specifies the Digital Signature Algorithm (DSA) and adopts the algorithms specified in two ANSI standards: ANSI X9.31 (RSA and Rabin-Williams signature algorithms) and ANSI X9.62 (The Elliptic Curve Digital Signature Algorithm [ECDSA]). FIPS 186-2 also includes recommended elliptic curves for ECDSA; note that these are the only curves validated by the CMVP during an ANSI X9.62 validation. Each of the Digital Signature algorithms specifies a number of allowable key sizes in order to provide varying levels of strength.

Cryptographic algorithms provide different levels of security against currently known attacks, depending on the algorithm and the size of the key or other parameters. ***NIST recommends that all algorithms used for Digital Signatures be used with key sizes that are comparable to key sizes of at least 80 bits that are used for symmetric encryption algorithms.*** Guidance on acceptable key sizes is being developed as part of the key management effort described below. In the case of the RSA signature algorithm, a minimum key size of 1024 bits is required; for DSA, a modulus of 1024 bits and a key size of 160 bits are required; for ECDSA, a 160-bit key is required.

FIPS 186-2 also includes specifications for random number generators to be used for the generation of DSA keys and digital signatures.

A change notice for FIPS 186-2 was recently published. This change notice updated the specified random number generators to protect against an attack that was recently proposed. The change notice for FIPS 186-2 is available at http://csrc.nist.gov/publications/fips/.

NIST is in the process of revising FIPS 186-2, to be proposed as FIPS 186-3. This revision will include a specification of larger key sizes for DSA that will provide more security, and a specification for a random number generator that will be based on the complete set of hash functions specified in FIPS 180-2 and discussed below. NIST is also considering the inclusion of the RSA signature algorithm as specified in Public Key Cryptographic Standard (PKCS) #1, the *RSA Encryption Standard*.

Hash Functions

Hash functions generate a hash value (message digest) from a message or file. The input to the hash function is of arbitrary length (e.g., a large message or file); the output is a fixed size value (the hash value), which is often smaller than the input. A hash function

Who we are

The Information Technology Laboratory (ITL) is a major research component of the National Institute of Standards and Technology (NIST) of the Technology Administration, U.S. Department of Commerce. We develop tests and measurement methods, reference data, proof-of-concept implementations, and technical analyses that help to advance the development and use of new information technology. We seek to overcome barriers to the efficient use of information technology, and to make systems more interoperable, easily usable, scalable, and secure than they are today. Our web site is http://www.itl.nist.gov/.

is usually used as a component in other cryptographic processes, such as the computation of a digital signature, the generation of a Message Authentication Code, the establishment of cryptographic keying material, or the generation of a random number.

FIPS 180-2, *Secure Hash Standard*, specifies four approved hash functions: SHA-1, SHA-256, SHA-384, and SHA-512. Each function provides a different length hash value and a different cryptographic strength. FIPS 180-2 is available at http://csrc.nist.gov/publications/fips/.

Key Management

Key management includes the rules and protocols for generating and establishing keys, and the subsequent handling of those keys. The security and reliability of any process using a cryptographic key depends on the protection afforded to that key. Two documents for key management are in development for sensitive, unclassified applications: a key establishment schemes document and a key management guideline.

The key establishment schemes document will include schemes to establish keys between communicating entities, based on standards developed by the American National Standards Institute (ANSI). A specification for a key wrapping technique will also be included, whereby a symmetric key is encrypted using another symmetric key (e.g., an AES key is encrypted by an AES key).

The key management guideline will provide guidance to federal agencies for the life cycle management of cryptographic keys, including the generation, establishment, storage, cryptoperiod, recovery, and destruction of those keys. In addition, the guideline will provide guidance on the selection of cryptographic algorithms and key sizes, will aid managers in setting up their key management infrastructure, and will assist users and system administrators of currently available infrastructures, protocols, and applications to configure and use their products more securely.

Information about this project and drafts of the key management documents are available at http://www.nist.gov/kms.

Entity Authentication

FIPS 196, *Entity Authentication Using Public Key Cryptography*, specifies two protocols for entity authentication that use a public key cryptographic algorithm for generating and verifying digital signatures. One entity can prove its identity to another entity by using a private key to generate a digital signature on a random challenge. The use of public key cryptography provides strong authentication, without the requirement for authenticating entities to share secret information.

Passwords and PINS

FIPS 112, *Password Usage*, provides guidance on the generation and management of passwords that are used to authenticate the identity of a system user and, in some instances, to grant or deny access to private or shared data. This standard recognizes that passwords are widely used in computer systems and networks for these purposes, although passwords are not the only method of personal authentication, and the standard does not endorse the use of passwords as the best method.

FIPS 112 was adopted in 1985. An effort is currently in progress to update this guidance.

Random Number Generation

Random numbers are used within many cryptographic applications, such as the generation of keys and other cryptographic values, the generation of digital signatures, and challenge-response protocols. Some approved algorithms to produce random numbers have been specified in FIPS 186-2, *Digital Signature Standard*. An effort is in progress by the Financial Services Committee of ANSI to develop a random number generation standard, and representatives from NIST participate in the development of this standard. It is anticipated that the eventual ANSI standard will be adopted as a FIPS.

Guest Research Internship Opportunities

Opportunities are available at NIST for 6-to24-month-long internships in the security program. Qualified individuals should contact the Computer Security Division, providing a statement of qualifications and indicating the area of work that is of interest. Contact: Elaine Barker, (301) 975-2911, ebarker@nist.gov.

Summary and Future Plans

The toolkit of cryptographic standards and guidance is nearing completion. NIST is planning to develop additional guidance for using its approved algorithms and combining them with other functions in a secure manner. NIST will continue to monitor the security of its approved algorithms and revise the standards, as appropriate. As cryptographic technologies emerge, NIST will investigate their security and applicability for the federal government and develop new standards and guidance when necessary.

Disclaimer: Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST nor does it imply that the products mentioned are necessarily the best available for the purpose.

U.S. DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
100 Bureau Drive, Stop 8900
Gaithersburg, MD 20899-8900