From: Bright Michael-CMB002 <cmb002@lmpsil02.comm.mot.com>
To: "'AESround2@nist.gov'" <AESround2@nist.gov>
Subject: AES comments
Date: Mon, 15 May 2000 18:06:07 -0500
X-Mailer: Internet Mail Service (5.5.2650.21)

<<SDC comments on AES 051500.pdf>>

Attached and listed below are Motorola Secure Design Center's comments on AES.

Please direct inquires to:

Mike Bright
Principle Staff Engineer
Secure Design Center
email: CMB002@email.mot.com
(847) 576-8059

Thanks,
Mike.

[See attached file]

May 15, 2000

Information Technology Laboratory
ATTN: AES Finalist Comments (Bldg. 820, Room 423)
National Institute of Standards and Technology
100 Bureau Drive, STOP 8970
Gaithersburg, MD 20899-8970
Email: AESround2@nist.gov

Motorola actively supports the National Institute of Standards and Technology (NIST) in its efforts to develop an Advanced Encryption Standard (AES) to replace the Data Encryption Standard (DES). The Secure Design Center (SDC) is a product development group within the Commercial Government Industrial Solutions Sector (CGISS) of Motorola responsible for providing encryption and security services into two-way land mobile radio products and systems. The SDC develops embedded cryptographic modules for subscriber radios and infrastructure devices within a private two-way radio system. The embedded module provides encryption and decryption services for voice and data traffic, authentication services, key management services and other security services. The SDC currently produces products that use the DES algorithm and several Motorola proprietary algorithms. The US government and public safety markets are large users of our DES equipped secure products and it is expected that they will demand AES equipped products as soon as the standard is announced.

Scope

Each of the five AES finalists differs from one another in various categories and properties. The SDC evaluated each of the five finalists based on two-way land mobile applications and products. The comments that follow convey which properties of the algorithm that are the most important for land mobile applications and in particular for portable (battery powered) operation. At the end we have some general comments that are not specific to any one algorithm.

For portable applications it is important to minimize the power consumption, the processor resources (RAM and ROM) or the size of the hardware circuitry, and the cost due to the high volume of products produced. These same properties are also important for infrastructure applications.

The SDC implementation of the AES algorithm in portable and mobile products will be in software (ANSI C/C++). The software will be executed on an embedded 32-bit microprocessor that will have a multiply instruction. For infrastructure equipment, such as an operator console, the AES algorithm may be implemented in a programmable hardware cryptographic engine that does not have a multiply instruction and will require high data throughput.

Differentiation Categories

Performance

All of the finalists are more than sufficient in terms of speed performance for land mobile applications. In portable products it is desirable to clock the embedded processors just fast enough to perform the required tasks including encryption. This saves on power consumption, and thus, extends battery life. An algorithm that executes in the fewest machine cycles on an embedded microprocessor can run with a slower clock and will use less power. The SDC recommends selecting an algorithm that requires very little or no multiplication operations, since multiplication is difficult to implement on some processors. Performance is a highly important property of the algorithm as it relates to power consumption.

Code Space

The size of the algorithm encryption or decryption application code is of some importance. Some secure processors have the capability to page encrypted code from external memory and then execute that code from on-chip RAM. If the algorithm code becomes too large, then the extra overhead of paging in separate parts of the algorithm would be required. Again this affects the performance of the system. An algorithm whose encrypt only or decrypt only code size is less than 2K bytes would be preferred. It is also desirable to select an algorithm that does not contain a large S-box table.

RAM Usage

RAM use in subscriber products is important. For portable and mobile products, it is typically not an option to add additional memory devices due to power and space limitations. The selected algorithm should minimize the RAM requirement for both program execution and key schedule storage.

Ease of Implementation

The ease to implement the algorithm is not an important consideration in the selection of the algorithm since the algorithm is typically implemented once and then ported to other products that use the same embedded hardware.

Key Agility

Key agility is of mild importance. The subscribers typically have a limited number of encryption services being executed simultaneously. However, when multiple encryption services are executed simultaneously, it is desirable that the storage requirement for the key schedule and state of the algorithm be kept at a minimum. An acceptable alternative is to minimize the time required to re-create the key schedule in order to conserve RAM. In fixed equipment, such as an operator console, multiple encryption services will be executed simultaneously as the rule.

Security

Security is extremely important to our customers. The SDC believes that all five finalists are sufficiently secure based upon the current evaluations by the encryption community. Therefore, the SDC has no recommendation for the selection of one algorithm over another based on algorithm security.

One Algorithm vs. Multiple Algorithms

The SDC recommends that NIST choose just one algorithm for AES. It is felt that selecting multiple algorithms will lead to confusion by the customer in the market place and will cause interoperability issues unless all of the selected algorithms are implemented. The customer will question which algorithm should be used and which algorithm is more secure than the other. Just as DES is not universally used today, it will be up to the other standard bodies to determine if the AES algorithm or another algorithm should be used for their application.

Modes of Operation

The SDC recommends that NIST continue to support the four modes of operation defined for DES along with the counter addressing mode for the AES algorithm. Most established systems today use one or more of these modes and this would allow an easy transition from DES to AES. For output feedback (OFB), the only approved mode of operation should be n-bit OFB, where n is the block size of the algorithm.

Douglas Hanson
Director, US Federal and World Wide Secure
Secure Design Center
Commercial Government Industrial Solutions Sector
Motorola
1301 E. Algonquin Rd.
Schaumburg, IL 60196