From: "Brian Gladman" <brian.gladman@btinternet.com>
To: <AESround2@nist.gov>
Subject: AES Comments
Date: Mon, 15 May 2000 12:42:40 +0100
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 5.00.2919.6700
X-MimeOLE: Produced By Microsoft MimeOLE V5.00.2919.6700

The enclosed Microsoft Word document provides second round comments on the AES selection process.

Brian Gladman

AES Second Round Comments

By Brian Gladman, Worcester, UK.

1. Performance Results

In final AES algorithm selection I would be grateful if you could consider the results presented at:

http://www.brian.gladman.btinternet.co.uk/cryptography_technology/aes2/

for all AES finalist algorithms and those at:

http://www.brian.gladman.btinternet.co.uk/cryptography_technology/serpent/

for the Serpent algorithm.

Please note, in particular, the recent result for Serpent bulk encryption running on Pentium family machines with MMX. This provides a throughput equivalent to 45 Mbits/second at the 200 MHz speed of the reference platform.

2. Information Security Requirements

On information security grounds I favour an AES standard comprising a primary and a secondary algorithm. I envisage only two information security requirements for which the secondary algorithm should be implemented:

(a) as a backup to guard against the failure of the primary algorithm ('hot spare');

(b) to provide for long lifetime information protection by encrypting with the secondary and the primary algorithms in sequence ('super-encryption').

I do not believe that the secondary algorithm should be a performance alternative for the primary algorithm. Accordingly I envisage the following provisions within the AES standard:

1. a decision to implement the secondary algorithm should be based only on an information security requirement and not on performance considerations;
2. in all applications where the information security requirement can be met with a single algorithm only the primary algorithm should be implemented;
3. when both algorithms are implemented, but only one is used, the algorithm used should be the primary algorithm unless this is known have a cryptographic weakness while the secondary algorithm is believed to remain sound (the secondary algorithm as a 'hot spare');
4. when the information security requirement dictates that both algorithms should be used in sequence, encryption should be undertaken by the secondary algorithm and then by the primary algorithm (the secondary algorithm used for 'super-encryption').

To meet such requirements the primary and secondary algorithms should be chosen to be as structurally diverse as possible in order to minimise the probability that any weakness discovered in one of them will not also be discovered in the other.

It has been postulated that the requirement for multiple algorithms is unnecessary because a future attack that 'breaks' the primary algorithm will also be likely to break the secondary one. It is possible to envisage two sets of future attacks:

(a) those that will 'break' both the primary and the secondary algorithm;

(b) those that will 'break' the primary but not the secondary algorithm.

If set (a) is much larger than set (b) this would make the adoption of a primary and a secondary algorithm within the AES standard ineffective. I would hence agree that this requirement should be dropped if an analysis of historical data for past encryption algorithms can be provided that suggests that this is most likely to be the case.