From: biham@cs.Technion.AC.IL
Date: Fri, 16 Apr 1999 06:01:19 +0300 (IDT)
To: aesfirstround@nist.gov

Dear aesfirstround,

In the next three email I send a comment, along with revised version
of my paper and slides "A Note on Comparing the AES Candidates".

Eli

Eli Biham Tel: +972-4-8294308
Computer Science Department Fax: +972-4-8221128
Technion, Haifa 32000, Israel email: biham@cs.technion.ac.il
WWW: http://www.cs.technion.ac.il/~biham/

A Note on Comparing the AES Candidates

Eli Biham

Computer Science Department
Technion, Haifa 32000, Israel

March 22, 1999

Revised Version

AES Requirements

- Blockcipher
- 128-bit blocks
- 128/192/256-bit keys
- "with a strength equal to or better than that of Triple-DES and significantly improved efficiency"

The 15 Submissions

Cipher	Submitted by	Country
CAST-256	Entrust	Canada
Crypton	Future Systems	Korea‡
Deal	Outerbridge	Canada†
DFC	ENS–CNRS	France
E2	NTT	Japan
Frog*	TecApro	Costa Rica
HPC*	Schroeppel	USA
LOKI97*	Brown, Pieprzyk, Seberry	Australia
Magenta	Deutsche Telekom	Germany
Mars	IBM	USA†
RC6	RSA	USA†
Rijndael*	Daemen, Rijmen	Belgium‡
Safer+*	Cylink	USA†
Serpent*	Anderson, Biham, Knudsen	UK, Israel, Norway
Twofish*	Counterpane	USA†

* Placed in the public domain; † and foreign designers; ‡ foreign influence

General Structure

Cipher	Type	Rounds	Using
CAST-256	Ext. Feistel	48	
Crypton	Square	12	
Deal	Feistel	6, 8, 8	DES
DFC	Feistel	8	Decorrelation modules, mult.
E2	Feistel	12	
Frog	Special	8	BombPermu
HPC	Omni	8	Hasty Pudding
LOKI97	Feistel	16	
Magenta	Feistel	6, 6, 8	
Mars	Ext. Feistel	32	Var. rot., mult., non-crypt. round
RC6	Feistel	20	Var. rot., mult.
Rijndael	Square	10, 12, 14	
Safer+	SP network	8, 12, 16	PHT
Serpent	SP network	32	Bitslice
Twofish	Feistel	16	

Var. rot.=Variable rotation. Mult.=Multiplication.

Security/Speed Tradeoffs

Small margins: adding a few rounds:

- RC6: Rivest assumes that there is an attack on 16-round RC6 with complexity 2^{119}. Proposes 20 rounds.
- DFC: An attack on 5 rounds. 8 rounds are proposed.
- Deal: An attack on 6 rounds. 6 are proposed.

Large margins: Doubling the number of rounds in the expense of speed:

- Serpent: 16 rounds are secure. 32 are proposed.
- Twofish: The best known attacks are on 6 rounds (9 or 10 rounds of the 256-bit key variant can be attacked using very strong assumptions of related keys slightly faster than exhaustive search). 16 are proposed.

Security/Speed Tradeoffs (cont.)

Result of distribution:

Each designer had his own view of the required relation between strength and speed

The main purpose of this talk is to point out that

- the number of rounds of a cipher is usually the last parameter the designer chooses,
- the relation between strength and speed should have been given as a requirement in the beginning of the AES process,
- NIST should decide on a minimal strength criterion before the second AES round, allowing the cipher designers to increase the number of rounds if necessary to fit this criterion

Speed Comparisons

The following table show the speed of the optimized implementations on Linux/GCC-2.7.2.2/Pentium MMX.

Only 128-bit keys are considered.

Speed Comparisons (cont.)

Cipher	Encrypt (cycles)	Decrypt (cycles)	Key Setup* encrypt	Key Setup* decrypt	Init	
Twofish	**1254**	**1162**	**18846**	**18634**	**20**	95.4% 92pf+0w
Rijndael	**1276**	**1276**	**17742**	**18886**	**28**	99.5% 98pf+0w
Crypton	**1282**	**1286**	**758***	**824***	**24**	99.7% 66pf+0w
RC6	**1436**	**1406**	**5186**	**5148**	**30**	94.0% 92pf+0w
Mars	**1600**	**1580**	**4708**	**5548**	**18**	96.7% 92pf+0w
Serpent	**1800**	**2102**	**13154**	**12648**	**14**	94.7% 98pf+0w
E2	**1808**	**1854**	**7980**	**7780**	**24**	96.0% 76pf+0w
	— DES with NIST API —					
CAST-256	**2088**	**2080**	**11412**	**11478**	**34**	99.9% 67pf+0w
Frog	**2182**	**2668**	**3857000**	**3817100**	**22**	95.6% 64pf+0w
HPC	**2602**	**2962**	**234346**	**248444**	**20**	64.1% 142pf+5557w
Safer+	**4424**	**4620**	**4708**	**4668**	**38**	95.7% 88pf+0w
DFC	**5874**	**5586**	**23914**	**25616**	**534**	98.6% 65pf+0w
LOKI97	**6376**	**6118**	**22756**	**22490**	**148**	96.7% 108pf+0w
Deal	**8950**	**8910**	**108396**	**107996**	**36**	97.3% 68pf+0w
Magenta	**23186**	**23230**	**1490**	**1622**	**24**	99.2% 89pf+0w

Strength Measures

The complexity of each attack is the minimal number between the time of analysis, the number of required plaintext/ciphertext blocks, and the required size of memory.

The strength of a cipher is the minimal complexity of all possible attacks.

Fair Speed/Security Comparisons

Consider the speed of the reduced- or increased-round variants with the same strength.

As most ciphers claim that exhaustive search is the fastest attack, we adopt the complexity of exhaustive search as the strength parameter.

We consider only 128-bit keys, i.e., the strength parameter is 2^{128}.

Fair Speed/Security Comparisons (cont.)

We base the minimal secure variants on the shortest reduced- or increased-round variants whose strength is at least 2^{128}:

I.e., the minimal secure variants have at least one pass over the longest "insecure" variant (whose strength is smaller than 2^{128}).

To be slightly more conservative we consider the minimal secure variants to have margins of two extra passes.

The following minimal number of rounds are based either that described by the designers or other cryptographers, or my best guess.

Fair Speed/Security Comparisons (cont.)

Cipher	Original (cycles)	Rounds	Minimal Rounds	Time (cycles)
Twofish	1254	16	$6+4=10$	784
Serpent	1800	32	$15+2=17$	956
Mars	1600	32	$12+8=20$	1000
Rijndael	1276	10	$6+2=8$	1021
Crypton	1282	12	$9+2=11$	1175
RC6	1436	20	$17+4=21$	1508
E2	1808	12	$8+3=11$	1657
CAST-256	2088	48	$32+8=40$	1740
	— DES with NIST API —			
Safer+	4424	8	$5+2=7$	3871
DFC	5874	8	$5+4=9$	6608
Deal	8950	6	$6+4=10$	14917
LOKI97	6376	16	$\geq 34+4=38$	≥ 15143
Magenta	23186	6	$\geq 7+4=11$	≥ 42508
Frog	2182	8	?	
HPC	2602	8	?	