On the Selection of the Advanced Encryption Standard

Eli Biham

Computer Science Department
Technion, Haifa 32000, Israel

December 12, 2000

The Advanced Encryption Standard (AES)

- NIST/FIPS next encryption standard
- Successor to DES
- Security for over 30 years
- May protect sensitive information for 100 years
- Competition
- International selection process
- Public confidence
- Took 3 years

Calendar

1997	Announcement and Requirements
1998	Submission
1998–1999	Analysis
1999	Selection of 5 finalists
1999–2000	More analysis
October 2nd, 2000	Final AES selection
till mid 2001	FIPS process

There were 4 AES conferences:

1997	Requirements workshop
1998	AES1: Candidate presentation (Ventura)
1999	AES2: Analysis (Rome)
2000	AES3: More analysis (NY)

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"
- If selected, royalty free worldwide

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

Selection Criteria

- Security
- Cost/Efficiency:
  - Software, Hardware, Smartcard
  - Intellectual property
- Algorithm characteristics
  - Flexibility
  - Simplicity and elegance
- Not by: Exportability, Nationality

Optimization Target

The designers had to decide which target platform to optimize for

- Pentium? MMX? Pro?
- Pentium II?
- 64-bit processors?
- 16-bit processors?
- 8-bit processors?
- Smartcards?
- Hardware?

The decision may crucially affect the design.

Security/Speed Tradeoffs

Small margins: adding a few rounds:

Cipher	Assumed Attackable Rounds	Proposed Rounds
RC6	16	20
DFC	5	8
Deal	6	6

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

Cipher	Assumed Attackable Rounds	Proposed Rounds
Serpent	15	32
Twofish	5 (10)	16

(*) The figures are as were known/predicted/assumed at design time.

Speed Comparisons

Cipher	Encrypt (cycles)	Decrypt (cycles)
Twofish	1254	1162
Rijndael	1276	1276
Crypton	1282	1286
RC6	1436	1406
Mars	1600	1580
Serpent	1800	2102
E2	1808	1854
— DES with NIST API —		
CAST-256	2088	2080
Frog	2182	2668
HPC	2602	2962
Safer+	4424	4620
DFC	5874	5586
LOKI97	6376	6118
Deal	8950	8910
Magenta	23186	23230

Smartcard Implementations

RAM and code size are the main criteria. RAM:

- RC6: 176 bytes are required to keep the subkeys. About 200 in total. Cannot use less.
- Mars: Similar. Can reduce the RAM requirement but at a considerable cost in speed (7 times slower?)
- DFC: 160 bytes (268 data bytes).
- Serpent: less than 64 bytes in total.

Gemplus predicts that 70% of the smartcards sold in 2003 will have 128 bytes or less of RAM.

EEPROM: several ciphers require 4K for the tables.

The Finalists

1. Mars
2. RC6
3. Rijndael
4. Serpent
5. Twofish

Mars

1. Extended Feistel structure
2. Has two types of rounds: unkeyed mixing to protect the core, core
3. Uses multiplications and variable rotations
4. Hardly fits in smartcards
5. A complex round function
6. Attacks up to 21 rounds out of 32

RC6

1. Fast
2. Compact code
3. Elegant, easy to remember
4. Based on RC5
5. Relies on multiplications and variable rotations
6. Hardly fits in smartcards
7. Attacks up to 15 rounds out of 20 (small security margins)

Serpent

1. Has the largest security margins
2. In software: the slowest of the finalists, still faster than DES
3. The fastest in hardware
4. SP network with bitslice optimization
5. Many speed improvements
6. Attacks up to 9 rounds out of 32

Serpent (cont.)

The cipher structure:

- an initial permutation IP;
- 32 rounds, each consisting of:
  - A key mixing operation
  - 32 same (round-dependent) 4x4 S-boxes
  - A linear transformation (in all but the last round)
  - In the last round, the linear transformation is replaced by an additional key mixing operation
- a final permutation FP.

Twofish

1. Fast
2. Feistel
3. Highly optimized for Pentium
4. Smartcard friendly
5. Key-dependent S boxes
6. Attacks up to 8 rounds out of 16

Rijndael

1. Very fast and efficient in software and hardware
2. Based on Square
3. SP network
4. Key size dependent number of rounds $Nr \in \{10, 12, 14\}$
5. Attacks up to 8 rounds out of 10

Rijndael: Encryption

Encryption is performed by

1. First key mixing (using subkey K_0)
2. Nr rounds consisting of
   (a) Byte substitution (a fixed 8x8 S-box)
   (b) Shift row
   (c) Mix column (except for the last round)
   (d) Key mixing (XOR with K_i)

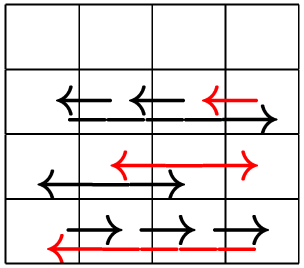
Rijndael: Encryption (cont.)

Let the 128-bit blocks be divided into 16 bytes, and be viewed in a rectangle (square) of 4×4 bytes

0	4	8	12
1	5	9	13
2	6	10	14
3	7	11	15

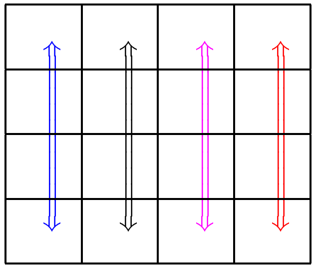
(a)Byte Substitution (S box)

(b)Shift Row



(d)Key Mixing (XOR)

(c)Mix Column ($GF(2^8)$)



A Brief Comparison

Rijndael, RC6, and Twofish are the fastest in software.

Rijndael and Serpent are the fastest in hardware.

Serpent has the largest security margins against known attacks.

Rijndael, Twofish, and Serpent fit well in smartcards.

Rijndael supports variable block sizes.

Should Several AES Ciphers be Selected?

Advantages:

1. Backup for case of a total break
2. Gain both speed and security by selecting two algorithms: a very fast cipher and a very secure (but slower) cipher
3. Backup against intellectual property attacks

Should Several AES Ciphers be Selected? (cont.)

Drawbacks:

1. Will both have to be implemented in each chip?
2. Which will be actually used?
3. If a backup, in which conditions will it be used?
4. How will the chip know which should be used?
5. If only one is implemented in each chip, better to have the same one in all chips.

Speed/Security Tradeoffs

Different tradeoffs between speed and security

- **each candidate proposes a different tradeoff**

1. **Should the fastest be selected?**
2. **Should the most secure be selected?**
3. **How to measure the tradeoff between speed and security?**

All the candidates can easily be tweaked to any decision

NIST decided to consider the ciphers as they are, e.g., if selecting security as the most important criterion, not selecting the ones optimized for speed.

Public Comments

NIST received comments (in writing and in conferences) on

- Cryptanalysis (security)
- Efficiency testing: software, hardware (speed)
- Intellectual property issues
- Fitness for applications
- Flexibility, Simplicity
- Confidence
- Comparisons of candidates
- Also on: required security margins, novel vs conservative design, importance of smartcards and other 8-bit applications, importance of hardware applications, etc.

Polls

NIST also made two polls during AES2 and AES3.

In AES2 they asked which ciphers should be selected for the 5 finalists, and which not.

The results were that

- MARS,
- RC6,
- Rijndael
- Serpent, and
- Twofish,

should be selected. E2 appeared in the 6th place.

All other ciphers had negative votes (more votes against the cipher than for it).

Polls (cont.)

In AES3 they made a poll that asked

- which finalist(s) should be selected to be the AES,
- how many should be selected,
- which combinations to consider,
- and which must not be selected.

The results showed that the audience prefers only one selected AES, and that it prefers

1. Rijndael (with some remarks on its number of rounds), and
2. Serpent in the second place.

The other three got considerably fewer votes.

The Decision: Rijndael

Rijndael was selected to be the AES.

Rijndael is certainly suitable as the AES.

The FIPS standardization process is now starting.

The Decision: Rijndael (cont.)

Rijndael might never be practically broken

- **Exhaustive search**
- **Practical shortcut attacks**

The Decision: Rijndael (cont.)

Rijndael might never be practically broken

- Exhaustive search
- Practical shortcut attacks

However, I predict that within the next few years, a theoretical attack (e.g., differential cryptanalysis) will be found

- Will require an impractical number of plaintexts
- Still will be faster than exhaustive search

My preference: Adding more rounds (16–20 in total)

The Selection Process Was

- Open
- Relied on public participation
- International
- Fair

- NIST received comments
- All comments became public
- NIST decided
- The decision is based on the comments

What Have We Learned

The second best algorithm can win

:-)

What Have We Learned

A very successful process

Collaborated well with the cryptographic community: common conferences AES/FSE

Nobody suspects existence of trapdoors

The process proves that international cryptographic standards can effectively be developed by the open research community

The process created new interactions between theoreticians and practitioners

More Information

- AES home page http://www.nist.gov/aes/
- Including: AES process information, decision documentation, descriptions and code of the algorithms, public comments, etc.

The End