The Effect of Multiple Algorithms in the Advanced Encryption Standard

Ian Harvey
Chief Scientist, nCipher Corporation
AES3, April 13-14 2000

The Problem

• Five finalist candidates
• No significant security results (yet)
• Different performance trade-offs
• Choice of one appears arbitrary
• Can we do better?
  – List factors in algorithm choice
  – Suggest multiple algorithm approaches
  – Analyse benefits & disadvantages
Factors in algorithm choice

- Security (theoretical and practical)
- Performance (speed, resource requirement)
- Cost of implementation
- Architectural implications
- Legal / IP issues

In a given situation, some factors may be almost totally unimportant

Security

- Theoretical security
  - Reputation of authors
  - Reputation of analysts
  - Absence of results over time
- Implementation security (emissions, fault induction)
  - Depends on platform
  - Difficult to evaluate in advance
- Individuals don’t want to / shouldn’t decide
  - ‘Brand names’ are useful
Performance

• Trade-off between speed and security
• Trade-off between speed and resource requirement
• One-dimensional ‘figure of merit’ impossible
• Always depends on platform
• Can identify typical categories...

Performance (2)

• Best ideal-case speed
  – chosen platform
  – e.g. hand-coded assembler, big ASIC
• Best worst-case speed
  – mixed-platform deployment
  – portable code, possibly fewer optimisations
• Minimum resource requirement
  – Speed less important
  – Mass production, may relax interoperability
Cost of Implementation

- Hardware complexity
- Software availability & portability
- Existence of reference design for given platform
- Design for test
  - vectors for complete coverage
  - vectors for debugging

Architectural Issues

- What ‘shape’ is interface to algorithm?
- Fundamental: block size and key size
- Additional parameters & nonstandard features
- Source of frustration to developers
  - often badly specified ⇒ compatibility problems
  - may require extra protocol ⇒ security holes?
Legal Issues

- License cost often commercially prohibitive
- ‘Free Software’ increasingly important
- International deployment a major headache
- “Circumvention is better than cure”
  - inconvenience to users

Multiple Algorithm AES

- More than one algorithm is presented
- Algorithms can be made optional
- Interoperability questions
  - End users need interoperability
  - AES could guarantee it
  - AES could present alternatives but no recommendations
AES with free algorithm choice

- **End users decide:**
  - only if components available
  - not qualified to make security judgments
- **Protocol designers decide:**
  - often, don’t know platform ⇒ same problems as us
- **Hardware vendors & toolkit suppliers**
  - don’t know application ⇒ need to compromise
- **Confusion in the marketplace**
  - what does “AES Compatible” mean?
  - ‘brand name’ effect diluted

Multiple Algorithm Models

- **A:** All implementations include all N algorithms
- **B:** One primary algorithm, 0..N-1 optional extras
- **C:** Any (N/2)+1 from N chosen
  - More generally M (≤N) chosen, argue about compatibility
  - Will become norm if AES makes no specific rules
Security properties

- Need continued operation if one algorithm is broken
- Approach A gives significant benefit
  - Simply discontinue broken algorithm
- Approach B gives some benefit
  - Most problematic if primary algorithm is broken
- Approach C has disadvantages
  - Any break might render systems inoperable
  - Leaves implementers to judge security
  - Negotiation open to attack

Performance

- Best ideal-case
  - All multiple-algorithm approaches score well
- Best worst-case
  - Overall benefits
  - Approach A: select mutually fastest algorithm
  - Approach B: add secondary algorithms if faster
  - Approach C: choose M best algorithms on each platform
**Performance - minimum size**

- Resource requirements:
  - Approach A has major disadvantages
  - Approach B good if primary algorithm is small
  - Approach C can choose M ‘smallest’ algorithms

- Some natural pairing of candidates
  - RC6 can reuse MARS’ resources
  - Rijndael, Twofish use similar primitives

- In future, security will be more important
  - Moore's law - 1% per week!

**Implementation-cost issues**

- Multiple algorithms increase implementation cost
  - Approach A is worst of all
  - Approach B as good as single-algorithm case if important
  - Approach C is worse than single-algorithm case

- Mitigated by good standard
  - Portable reference C code
  - Comprehensive test vectors (including ‘simple’ cases)
  - Intermediate values aid debugging
Architectural Implications

- Most significant disadvantage of multi-algorithm AES
- Need for negotiation?
  - extra security design required
  - approaches A, B can hardwire choice
- Need to restrict non-standard options
  - no two candidates agree on what ‘odd’ key lengths allowed
  - block size, # of rounds variations
  - don’t allow explicit choice of # of rounds!

Legal Issues

- Ideal: all final algorithms free of IP problems
- Necessary: enough final algorithms freely available
- Work required by NIST
  - Approach B easiest, C and A progressively harder
- ‘Patent hijack’ resilience
  - Similar properties to security resilience; A is best
Summary

• Generally increases security, but be careful!
  – Approach C has notable problems
• All approaches increase speed
• All approaches create architectural issues
• Approaches A, C increase costs
• Approach B need not increase costs

Approach B Strategy

• Primary algorithm criteria
  – security is #1 factor
  – speed not important
  – small size an advantage
  – lack of legal issues
  ⇒ conservative, traditional design?
• Secondary algorithm criteria
  – can take more risks for added performance
Contact

• mailto: ih@ncipher.com
• http://www.ncipher.com/

• © nCipher Corporation Ltd., 2000
  this version dated 2000.04.04