Cryptography Trends: A US-Based Perspective

Burt Kaliski, RSA Laboratories

IPA/TAO Cryptography Symposium

October 20, 2000

RSA LABORATORIES

Outline

- Advanced Encryption Standard
- Dominant design
- Thoughts on key size

Advanced Encryption Standard

- New symmetric encryption algorithm for US federal agencies
- Replaces Data Encryption Standard (DES), first published in 1977, providing stronger security:
  - 128-bit minimum key size — vs. 56 for DES
  - 128-bit block size — vs. 64 for DES
- Open, public evaluation process
- Likely to become a new worldwide de facto symmetric algorithm

Timetable

1997	Jan.: First announcement Sept.: Call for algorithms	
1998	June: Submission deadline August: First AES Conference	ROUND 1 ↓
1999	March: Second AES Conference August: Finalists announced	ROUND 2 ↓
2000	April: Third AES Conference May: Comments deadline Oct.: Winner announced	

Evaluation Criteria

Security (primary)	general security attacks on implementations
Cost and algorithm characteristics (secondary)	software implementations restricted-space environments hardware implementations encryption vs. decryption key agility other versatility and flexibility instruction-level parallelism intellectual property issues

AES Finalists

- **Twofish (Bruce Schneier, John Kelsey *et al.*)**
- **MARS (IBM)**
- **RC6 (RSA Laboratories)**
- **Rijndael (Joan Daemen and Vincent Rijmen)**
- **Serpent (Ross Anderson, Eli Biham and Lars Knudsen)**

RSA LABORATORIES

And the Winner ...

- **NIST announced on October 2, 2000:**

  Rijndael will be the AES

- **Draft standard to be published in November; final standard expected in April-June 2001**

RSA LABORATORIES

About Rijndael

- Design based on byte substitutions and permutations
- Adequate security margin with significant analysis during AES evaluation
  - though some criticism of mathematical structure
- Consistently good performance across a wide range of environments
- Royalty-free for all purposes
- Pronunciation: “Rain Doll” or “Rhine Dahl”

RSA LABORATORIES

What about the Other Finalists?

- **NIST prefers Rijndael's security, efficiency and other attributes, taken together, but other finalists have their own advantages**
- **NIST's remarks:**

"Each of the finalist algorithms appears to offer adequate security, and each offers a considerable number of advantages. Any of the finalists could serve admirably as the AES. However, each algorithm has one or more areas where is does not fare quite as well as some other algorithm; none of the finalists is outstandingly superior to the rest." (NIST Report, p. 91)

RSA LABORATORIES

Dominant Design

- **As security has become more widely deployed in recent years, a "dominant design" has emerged that governs mainstream implementation**
  - **[Abernathy & Utterback, *Technol. Rev.*, 1978]**
- **This dominant design is a challenge in moving toward stronger or more efficient cryptographic techniques**
  - **… until the next design emerges**

Why It's a Challenge

- For interoperability, many elements must typically be updated together to support a new technique:
  - applications
  - services (e.g., certificate authorities)
  - protocol standards
- Changes that affect only one element are often an easier "investment"
  - e.g., local performance improvements
- Multi-element changes must therefore be relatively simple

RSA LABORATORIES

Some Dominant Security Choices

- X.509 v3 certificates
- SSL protocol
- PKCS #1 v1.5 RSA, DES, RC4, SHA-1 algorithms

- All have become embedded in today's security infrastructure, and improvements must "fit"

RSA LABORATORIES

Toward New Algorithms

- Despite the challenges, new techniques are needed
- DES key size, block size are too short
- PKCS #1 v1.5 RSA, though adequate in practice, lacks provable security
- SHA-1 hash size may not be enough
- Other hard problems besides integer factorization should be considered

How Hard to Update?

- Introducing AES is (relatively) simple: just the underlying block cipher
  - though larger block size may add some complexity
- RSA-OAEP, RSA-PSS are also simple: just how a hash value is processed, not the keys
  - deliberate design feature of “standard” RSA-PSS
- SHA-2 is simple
- ECC is more complex: keys, processing, possibly protocols (e.g., for EC key agreement)
  - less “constrained” environments are easier targets

Towards the Next Design

- **Wireless security may provide a "next" design**
  - **"lightweight" certificates, WTLS, ECC, etc., optimized for constrained environment**
- **But even WAP and IETF protocols are converging, and it's not clear yet how "next" wireless will be in terms of security design**
- **New *functionality* is perhaps a better catalyst for new design**
  - **e.g., multi-party secure computation, vs. signatures & encryption**

RSA LABORATORIES

US-Based Crypto Standards Efforts

- ASC X9.F.1 (Financial Services Industry)
  - X9.30, .31, .62: Digital signatures
  - X9.42, .44, .63: Key establishment
  - three families: discrete log, factoring (RSA), ECC
- NIST (US Federal Government)
  - FIPS 186-2: Digital signatures via three families
  - AES
  - SHA-2
  - key management FIPS
- Significant US company involvement in worldwide standards efforts, e.g., IEEE P1363, IETF, ISO/IEC, WAP

RSA LABORATORIES

Thoughts on Key Size

- Operations vs. cost
- Key size comparisons
- A quiz question

Operations vs. Cost

- **The security of a algorithm is often considered in terms of the number of operations to break it**
- **Other elements must also be considered**
- ***Memory cost* is a significant factor**
- **Availability of *general-purpose workstations* vs. development of custom machines, can affect analysis as well**

Key Size Comparisons

- Various efforts to compare key sizes:
  - Certicom Research
  - cryptosavvy.com
  - IEEE 1363
  - RSA Laboratories (see Bulletin #13)
- Comparison of key sizes depends significantly on assumptions and what is compared
- Moreover, at very large sizes, comparison is theoretical only: if “cost” were invested in research, situation could change dramatically

RSA LABORATORIES

Example Key Size Equivalences

(for purposes of discussion …)

Symmetric	ECC	RSA (cost)	RSA (operations)
80	161	760	1024
96	192	1020	~1500
112	225	~1500	2048
128	257	2060	3072

RSA LABORATORIES

A Quiz Question

An asymmetric key size for use with a 128-bit AES key should …

a) take 2^{128} operations to break

b) *cost* the same to break as 128-bit AES

c) provide the security level an application needs

Conclusions

- Dominant design is a challenge for supporting new techniques
- When better techniques are needed, changes should be simple
  - or part of a new design
- In the long term, new functionality is a catalyst
- Key size comparison is a challenge as well
- AES winner: Rijndael

RSA LABORATORIES

For More Information

- Burt Kaliski
  RSA Laboratories
  bkaliski@rsasecurity.com
  www.rsasecurity.com/rsalabs
- AES Web page: www.nist.gov/aes

RSA LABORATORIES