NAUTILUS INSTITUTE
FOR SECURITY AND SUSTAINABILITY

THE AES PROJECT: ANY LESSONS FOR NC3?

Recommended Citation

Thomas Berson, "THE AES PROJECT: ANY LESSONS FOR NC3?", NAPSNet Special Reports, June 23, 2020, https://nautilus.org/napsnet/napsnet-special-reports/the-aes-project-any-lessons-for-nc3/

THOMAS A. BERSON
JUNE 23, 2020

I. INTRODUCTION

In this report, Tom Berson details how lessons from the Advanced Encryption Standard Competition can aid the development of international NC3 components and even be mirrored in the creation of a CATALINK community.

Tom Berson is a cryptologist and founder of Anagram Laboratories. Contact: berson@anagram.com

This paper was prepared for *the Antidotes for Emerging NC3 Technical Vulnerabilities, A Scenarios-Based Workshop* held October 21-22, 2019 and convened by The Nautilus Institute for Security and Sustainability, Technology for Global Security, The Stanley Center for Peace and Security, and hosted by The Center for International Security and Cooperation (CISAC) Stanford University.

A podcast with Tom Berson and Philip Reiner can be found **here**.

It is published simultaneously **here** by Technology for Global Security and **here** by Nautilus Institute and is published under a 4.0 International Creative Commons License the terms of which are found here.

Acknowledgments: The workshop was funded by the John D. and Catherine T. MacArthur Foundation. Maureen Jerrett provided copy editing services.

Banner image is by Lauren Hostetter of Heyhoss Design

II. NAPSNet SPECIAL REPORT BY TOM BERSON

THE AES PROJECT: ANY LESSONS FOR NC3?

JUNE 23, 2020

1. THE AES PROJECT

From 1997 through 2001, the National Institute for Standards and Technology (US) (NIST) ran an open, transparent, international competition to design and select a standard block cipher called the Advanced Encryption Standard (AES)[1]. The competition proved productive, engaging, educational, surprising, and successful. AES, formally published in 2001 as FIPS 197, was quickly adopted as a basic cryptographic building block and widely deployed worldwide.

The format of the AES competition has been reused in the United States and Europe for the design and selection of other cryptographic primitives, such as hash functions and stream ciphers. As of this writing (mid 2020) NIST is in the middle of a similarly structured competition to "solicit, evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms."[2]

We believe four factors contributed to the success of the AES project:

- There was a clear VISION of the desired outcome.
- There were explicit REQUIREMENTS for the interface and evaluation criteria.
- Efforts were made to build and preserve TRUST among the people and organizations participating in the project.
- AES ran the project in the context of an existing COMMUNITY and worked to create mutual confidence among participants.

1.1 Clear Vision

NIST's vision was that AES would be "an unclassified, publicly disclosed encryption algorithm capable of protecting sensitive government information well into the next century."

As background, industry, commerce, and governments needed AES to replace the obsolescent Data

Encryption Standard (DES). DES was standardized as FIPS PUB 46 in 1977. DES had been developed starting in 1973 from a single candidate offered to the government by IBM. The National Security Agency (NSA) collaborated with IBM to modify components of the algorithm, known as S-boxes, and in shortening the key length. There were few open-community cryptographers in the 1970s, but several voiced their suspicions of NSA's involvement. Design criteria for the S-boxes were never released, leading to speculation about whether they contained some sort of trap door.

These early suspicions, along with the relative immaturity of the market, led to a slow uptake of DES. Cryptanalysis of DES trained a generation of open-community cryptographers and led to significant cryptanalytic advances. By the time the AES competition began, DES was in wide use but no longer satisfyingly secure. Moore's law[3], along with cryptanalytic advances,[4],[5] made further use of DES seem unwise. Its block length (64 bits) and key length (56 bits) were each too short. So, AES would require longer blocks and a longer key and would be chosen through a transparent process.

1.2 Explicit Requirements

The competition required AES to be a block cipher with a block length of 256 bits and key lengths of 128, 192, and 256 bits. A block cipher is an algorithm that, in a process called encryption, converts a block of plaintext into a block of ciphertext under control of a variable called the key. In a process called decryption, a block cipher must also be able to restore the block of ciphertext back into the original block of plaintext when operated with the same key.

NIST published its submission requirements and evaluation criteria for AES after public comments and a workshop held in April 1997. The evaluation addressed three criteria:

- Security (relative to other candidates, indistinguishable from random, mathematical basis of security and other factors and attacks)
- Cost (no intellectual property payments, computational cost, and memory cost)
- Algorithm and implementation characteristics (flexibility, hardware and software suitability, and simplicity)

1.3 Build and Preserve Trust

NIST issued a formal call for candidate algorithms in September 1997 after publishing the results of the Evaluation Criteria Workshop. Fifteen candidates[6] made it into Round One of the evaluation. Some were from individuals and others from teams either with or without organizational affiliation. Authors were citizens of the following nations: Armenia, Australia, Belgium, Canada, Costa Rica, France, Germany, Greece, Israel, Japan, Korea, Norway, Switzerland, United Kingdom, and the United States.

It is important to mention here that National Security Agency (NSA), the foremost cryptographic organization in the United States, if not in the world, did not have a candidate in the competition. There were those in NSA who wanted badly to compete, to show off their expertise, and to rank it against others. But, because NSA was to give technical advice to NIST in the evaluation of candidates, the real or appearance of conflict of interest would have destroyed trust in the process. NSA leadership wisely decided against allowing an NSA candidate.

Each team presented its candidate at a public AES Candidate Conference, AES1, held in August 1998. One candidate, MAGENTA, was broken during its presentation by an alert audience member, Richard Schroeppel, who was himself the author of the HPC candidate. The game was on.

What motivated fifteen distinct groups to invest time and effort into a competition with no monetary reward? In our opinion, it was the fun of the chase and the indirect benefits likely to accrue to individuals and their home organizations from winning an international cryptographic competition. The eventual winners went on to advance in their academic careers, design further algorithms, win additional honors (some with money attached), and to be principals in cyber security companies.

During a second AES Candidate Conference, AES2, held in March 1999, interested parties presented security and performance analyses of the Round One candidates. Three months later NIST announced a narrowing of the field to five Round Two candidates:

- MARS (US, Switzerland)
- RC6 (US)
- RIJNDAEL (Belgium)
- TWOFISH (US)
- SERPENT (UK, Israel, Norway)

All Round Two candidates were good block ciphers. They differed in their mathematical underpinnings, performance, and memory requirements. Much study, cryptanalysis, performance measurement, etc., followed, along with a third public AES Candidate Conference, AES3, in April 2000.

Imagine the cryptographic world's surprise when NIST announced on October 3, 2000, that AES would be RIJNDAEL, authored by two young Belgian cryptographers, and one of two Round Two candidates that had no US authors. Surprise, but not suspicion, because RIJNDAEL had been chosen in an open and transparent manner.

NIST published a draft FIPS in February 2001. AES was rapidly adopted by industry and other standards bodies responsible for payment systems, Internet security, etc. It is in widespread use today.

In June 2003, NSA announced, "The design and strength of all key lengths of the AES algorithm (i.e., 128, 192, and 256) are sufficient to protect classified information up to the SECRET level. TOP SECRET information will require use of either the 192 or 256 key lengths. The implementation of AES in products intended to protect national security systems and/or information must be reviewed and certified by NSA prior to their acquisition and use."[7] This approval of AES to protect national security information not only allows the US government to use (approved) commercial off-the-shelf equipment, but it is a powerful public endorsement of the security of AES.

1.4 Create a Community

There is a rich literature supporting the proposition that norms, including standards, are not just words, but also the communities that come together to forge and support those norms. In other words, a norm is partly a social process. It becomes a norm because a community believes in it, and it goes out into the world surrounded by a community which is invested in its success.[8]

The NIST AES project benefited greatly from the circumstance that it was embedded in a pre-existing community of cryptographers. The International Association for Cryptologic Research, Inc. (IACR)[9] is a non-profit, scientific organization founded in 1982 "to further research in cryptology and related fields." Beginning in 1982, throughout the AES competition, and continuing today, IACR has sponsored three annual scientific conferences: Crypto (held in Santa Barbara, CA); Eurocrypt

(held in various European venues); and Asiacrypt (held in various Asian and Pacific venues). These conferences typically attract 300 to 500 attendees from academic, industrial, and government circles. The conferences are organized around a program of scientific presentations and have the flavor of a collegial reunion.[10]

Almost every author of an AES candidate algorithm was a member of IACR and had been a regular attendee at IACR conferences. The same is true for the principal NIST personnel who ran the AES competition.

Further, the series of AES Candidate Conferences created a community of its own.

Roughly 200 members of the global cryptographic community attended each of AES1, AES2, and AES3. They kept in touch between conferences via a NIST-sponsored email forum and informal get-togethers at non-NIST cryptographic events.

2. POSSIBLE LESSONS FOR NC3

What lessons from the AES Competition can aid the international development of new NC3 components? We are told that a hot line is the most likely application. Allow sufficient time. Expect it to take years. Plan for a series of face-to-face conferences held on various participants' territories.

Is there a clear vision of the outcome?

Can the required technical interfaces be precisely specified? Can the evaluation criteria be stated, prioritized, and agreed upon?

Can the people who are working to create the new system learn to trust one another? This is especially difficult given that hot lines may be viewed by participants and non- participants as legitimate targets for signals intelligence and/or for offensive cyber operations.

Can governments avoid the temptation to subvert the process while it is ongoing?

Can a community be established around the new system? The answer, so far as cryptographers go, is a cautious "yes." Chances are good that the cryptographers who would work on such a system already know, or know of, one another. But the community will have to be greater than cryptographers alone. Military and policy people from different nations will have to form a community across oceans of distrust and, in some cases, rivers of blood. A difficult task indeed.

3. DO NEW HOT LINES REQUIRE NEW CRYPTOGRAPHY?

Probably not. You cannot pick up a newspaper or magazine today without reading breathless stories of blockchain (a kind of data structure) or post-quantum cryptography (because quantum computing, when practical, will threaten all currently used public-key cryptosystems).

Neither of these is required for a modern, performant, secure, authentic, usable system for communication among pre-identified parties to whom cryptographic credentials have been pre-distributed via secure physical transfer.

III. ENDNOTES

[1] Announcing Request for Candidate Algorithm Nominations for the Advanced Encryption Standard. Vol. 62, No. 177. Federal Register. (September 12, 1997). Available at https://www.govinfo.gov/content/pkg/FR-1997-09-12/pdf/97-24214.pdf

[2] Post-Quantum Cryptography Project. NIST webpage last updated June 1, 2020. Available at: https://csrc.nist.gov/Projects/post-quantum-cryptography

[3] In 1998, the Electronic Freedom Foundation built a machine called Deep Crack for less than $250,000, which was able to perform an exhaustive search of DES key space in 56 hours. Wikipedia contributors, "EFF DES cracker," *Wikipedia, The Free Encyclopedia,* https://en.wikipedia.org/w/index.php?title=EFF_DES_cracker&oldid=938377402 (accessed June 12, 2020).

[4] Biham, E. and A. Shamir. Differential Cryptanalysis of DES-like Cryptosystems. Advances in Cryptology—CRYPTO 1990.

[5] Matsui, M. Linear cryptanalysis method for DES cipher. Advances in Cryptology—EUROCRYPT 1993.

[6] The candidates were LOKI197, CAST-256, DEAL, FROG, DFC, MARS, RC6, RIJNDAEL, TWOFISH, SERPENT, MAGENTA, E2, CRYPTON, HPC, and SAFER+.

[7] CNSS Policy No. 15, Fact Sheet No. 1, National Policy on the Use of the Advanced Encryption Standard (AES) to Protect National Security Systems and National Security Information, CNSS Secretariat, National Security Agency (June 2003).

[8] For example, Finnemore, Martha and Duncan B. Hollis, Constructing Norms for Global Cybersecurity, American Journal of International Law, Vol. 110, No. 3, (July 2016), pp. 425-479. Also Raymond, Mark, *Social Practices of Rule-Making in World Politics*, Oxford (2019).

[9] International Association for Cryptologic Research. Available at: https://www.iacr.org

[10] Full disclosure: the author was President of IACR from 1988-1991 and thereafter the director of the Association. He was an editor of its *Journal of Cryptology* for 14 years and is an IACR Fellow.

IV. NAUTILUS INVITES YOUR RESPONSE

Nautilus invites your responses to this report. Please send responses to: nautilus@nautilus.org. Responses will be considered for redistribution to the network only if they include the author's name, affiliation, and explicit consent.

View this online at: https://nautilus.org/napsnet/napsnet-special-reports/the-aes-project-any-l-ssons-for-nc3/

Nautilus Institute
2342 Shattuck Ave. #300, Berkeley, CA 94704 | Phone: (510) 423-0372 | Email: nautilus@nautilus.org