Global Information Assurance Certification Paper

Rijndael – The Future of Encryption

By Sarah Merrion

Why Encryption?

What hardware platform or software application is truly secure these days? Many number of applications use cryptographic algorithms in order to provide acceptable security at a low cost. A prominent restriction being that the performance of the applications should be influenced as little as possible by the insertion of security – in this case, cryptography.

Encryption Standards

Many people wonder why we need to replace the best known and most widely used block cipher around – the DES algorithm. Simply put, it has become obsolete and is need to replacement. DES has a 64 bit data block and a 56 bit key and has been around since 1977. The competition to replace it has been ongoing for 4 years. In the meantime, Triple DES (also known as 3-DES) has been endorsed by NIST as a temporary standard to be used until the AES is finished sometime in 2001. Triple DES has never been looked on as a permanent solution. It is too expensive for many users and is slow - taking three times the computation of DES!

The Advanced Encryption Standard

The Advanced Encryption Standard will be a new Federal Information Processing Standard (FIPS) Publication that will specify the cryptographic algorithm for use by US Government organizations. The federal government has special needs to protect sensitive information. Members of the crypto community also anticipate that the new standard will be used voluntarily by commerical users outside of the Government – and outside of the US.

Talent from a number of different sources (US Government, private industry and academia) has been pulled for this four-year effort in the development of the future encryption technique. Offered as a contest with the authors receiving no royalty or future profits from the development, cryptologists from around the world have been publicly analyzing and defending their work in an attempt to prove that their algorithm is the best solution for our future. [1]

Choosing a suitable cipher

The NIST specified that proposed algorithms must implement a symmetric block cipher, with a block size of 128 bits, and key sizes of 128, 192 and 256 bits (at least). They want an algorithm whose security is at least a good as Triple-DES, but with enhancements in efficiency.

Rijndael

Of the five Round-2 finalists, Rijndael selected by the NIST as the proposed AES algorithm. It was developed and submitted by two Belgian cryptographers named Dr. Joan Daemen and Dr. Vincent Rijmen. Rijndael is a block cipher. Block ciphers are the most common form of private key algorithms. They transform a short string to a string of the same length under control of a secret key and usually involve between 8 and 32 rounds, which use half the value as input, and whose output is XOR'd with the other half.

From the authors themselves, here are the reasons that make Rijndael stand out from the other finalists:

- The symmetric and parallel structure
  - Gives implementers a lot of flexibility
  - Has not allowed effective cryptanalytic attacks
- Well adapted to modern processors
  - Pentium
  - RISC and parallel processors
- Suited for Smart cards
- Flexible in dedicated hardware[9]

In addition the algorithm can be implemented very efficiently on a wide range of processors and in hardware (smart cards, for example). Compared to the other finalists, it has the shortest encryption/decryption time, and provides the best performance of all the candidates when both hardware and software performance was taken into account.

How Rijndael works

To complete encryption, the Rijndael cipher uses 4 steps (byte substitution, row shifting, column mixing and key addition) in 10 to 14 repetitive rounds. It was derived from the previous Square cipher, also written by Daemen and Rijmen.

A 'round' takes a function from *n* bits to *n* bits and produces an inverted function from *2n* bits to *2n* bits. Not counting an extra round performed at the end of the process with one step omitted, the number of rounds in Rijndael is:

9 if both the block and the key are 128 bits long.
11 if either the block or the key is 192 bits long, and neither of them is longer than that.

13 if either the block or the key is 256 bits long.[10]

The Rounds

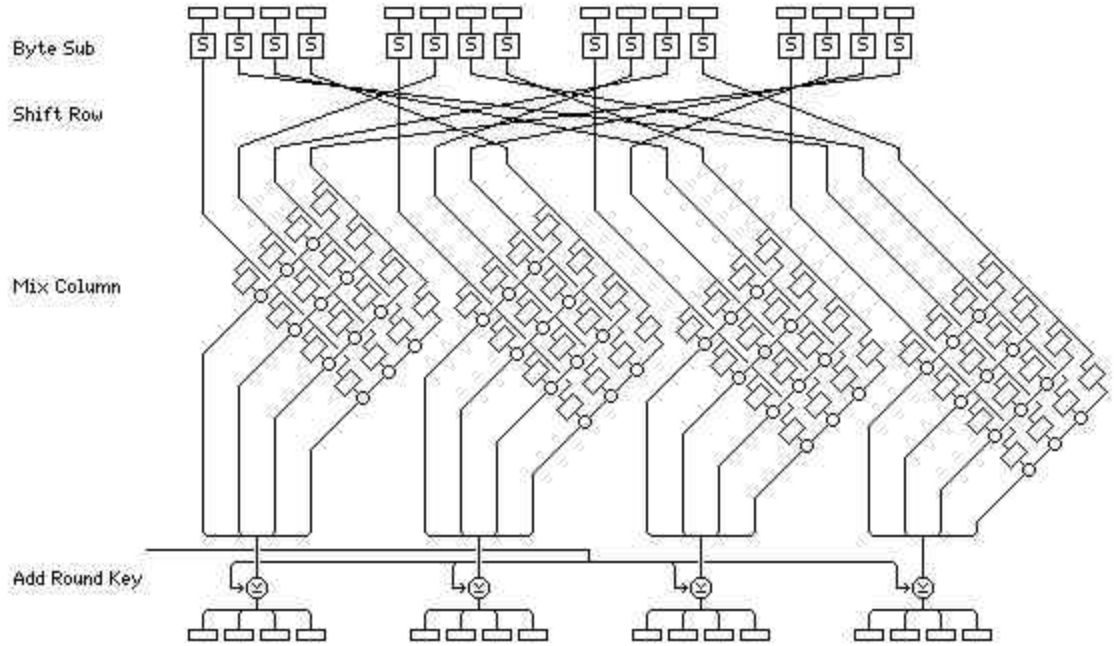
Each regular round involves four steps.

1. **Byte Substitution**: Each 8-bit byte in the state is reversibly mapped into another byte. (Each byte of the block is replaced by its substitute in an S-box). An S-box is a lookup table that maps *n* bits to *m* bits. It's the only part of the cipher that is non-linear, and considered the most important part of the algorithm.[10]

2. **Shift Row**: Here, rows are shifted over four different offsets. Row 0 is unmoved, Row 1, Row 2 and Row 3 are rotated left 1, 2 and 3 bytes respectively.

3. **Mix Column:** In this step, the bytes in columns are linearly combined. Matrix multiplication is performed.

4. **Add Round Key**: This is the final step where the subkey is XORd in for the current round.



An illustration of the Rijndael round:[10]

Round Advantages/Disadvantages

Rijndael's rounds can vary from 10 to 14 and is dependent on both the block size and key length. This is a low number of rounds compared to other algorithm finalists. The low number of rounds is probably the one criticism that analysts have about Rijndael. If this ever becomes a problem, however, with a little extra money the block size and key length can be increased to eliminate this.[8]

Future

One might ask how long the AES will remain uncracked. Review of the algorithm will be ongoing, and as in the history of other algorithms we'll soon see contests offered on http://www.distributed.net in an attempt to break the code. Once the AES becomes an official standard, that standard will be formally reevaluated every five years. If needed, "certain maintenance activities for the standard will be developed whenever circumstances dictate."[1]

Recent laws have reformed export restrictions on American-made encryption products. Aware of these changes, the NIST required that all submissions conform to the new laws. The new standard will be exportable, and all current implementations in proprietary systems will just need to be reviewed prior to being exported. The Department of Commerce's Bureau of Export Administration maintains export regulations.

Commercially, companies are not required to adopt the new standard, but are welcome to. Rijndael hasn't officially been named the standard, however many technology developers and companies are committing to the new standard, as commercial use will be the largest audience.

Conclusion:

At present, it is not possible to design a block cipher which is both very fast and 'secure'. Most ciphers are secure after many rounds, however they are too slow after many rounds. Improvements have been made, although performance is the expense.

Most designs, like Rijndael, are developed in a 'trial-and-error' environment. Cryptography will be around for a long, long time. There may be changes on the horizon such as, key lengths, which will become longer as hackers continue to advance their attacks. In response, algorithms will become more highly evolved - and innovations that are not even contemplated today will emerge in the not-so-distant future.

References:

1. Advanced Encryption Standard (AES) Questions and Answers, http://csrc.nist.gov/encryption/aes/round2/aesfact.html

2. Baltimore Technologies, 'Technical Overview of RIJNDAEL - The AES', http://dev.baltimore.com/aes/tech_overview.html

3. Brown, Dr. Lawrie, 'A Current Perspective on Encryption Algorithms', http://www.adfa.edu.au/~lpb/papers/unz99.html

4. Cryptography – Digest Digest # 813, Thur, 18 May 2000, http://www.mail-archive.com/cryptography-digest%40senator-bedfellow.mit.edu/msg03002.html

5. Ellis, Kathleen, 'U.S. picks new Encryption Standard', http://www.security-focus.com/templates/article.html?id=96 [October 2, 2000]

6. Larvala, Samuli, 'AES – A New Encryption Standard', http://www.miksula.cs.hut.fi/~jpmyyry/tlark/10/, [February 1, 1999]

7. Reavis, Jim, 'Advanced Encryption Standard – crypto for the next century', NetworkWorldFusion, http://www.nwfusion.com/newsletters/sec/0927sec1.html.

8. 'Rijndael Encryption', http://www.tropsoft.com/strongenc/rijndael

9. Rijmen, Vincent, 'Rijndael' http://csrc.nist.gov/encryption/aes/rijndael/

10. Savard, John J.G., 'The Advanced Encryption Standard (Rijndael)'[Online], http://home.ecn.ab.ca/~jsavard/crypto/co040801.htm

Last Updated: July 21st, 2017

Upcoming Training

SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS